Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by HCL AppScan Standard 10.0.8
Scan started: 9/16/2022 2:23:05 PM

Table of Contents

Introduction

Summary

Issues Sorted by Issue Type

How to Fix

- Hidden Directory Detected
- Unnecessary Http Response Headers found in the Application
- Unsafe third-party link (target="_blank")
- Missing "Content-Security-Policy" header
- Missing or Insecure "Object-Src" policy in "Content-Security-Policy" header
- Missing or Insecure "Script-Src" policy in "Content-Security-Policy" header
- Missing or Insecure "Style-Src" policy in "Content-Security-Policy"
- Missing or insecure HTTP Strict-Transport-Security Header
- Application Error
- Client-Side (JavaScript) Cookie References
- Cookie with SameSite attribute not Restrictive
- Email Address Pattern Found
- Integer Overflow
- Missing "Referrer policy" Security Header
- Possible Server Path Disclosure Pattern Found

Application Data

- Failed Requests

Introduction

This report contains the results of a web application security scan performed by HCL AppScan Standard.

Medium severity issues:	67
Low severity issues:	5
Informational severity issues:	20
Total security issues included in the report:	92
Total security issues discovered in the scan:	92

General Information

Scan file name:	2022-09-16_Engine
Scan started:	9/16/2022 2:23:05 PM
Test policy:	Default
Test optimization level:	Normal

Host	stage.rrev-engine.com
Port	443
Operating system:	Unknown
Web server:	Apache
Application server:	Any

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Enabled
In-session pattern:	`>Log out<`
Tracked or session ID cookies:	`SSESSf6189c42141c46ed558989cd4da65b9e`
Tracked or session ID parameters:	`form_build_id`

Login sequence:	`https://stage.rrev-engine.com/user/login`
	`https://stage.rrev-engine.com/user/login`
	`https://stage.rrev-engine.com/user-dashboard`

Summary

Issue Types 16

TOC

	Issue Type	Number of Issues
M	Check for SRI (Subresource Integrity) support	3
M	Hidden Directory Detected	7
M	Unnecessary Http Response Headers found in the Application	1
M	Unsafe third-party link (target="_blank")	56
L	Missing "Content-Security-Policy" header	1
L	Missing or Insecure "Object-Src" policy in "Content-Security-Policy" header	1
L	Missing or Insecure "Script-Src" policy in "Content-Security-Policy" header	1
L	Missing or Insecure "Style-Src" policy in "Content-Security-Policy"	1
L	Missing or insecure HTTP Strict-Transport-Security Header	1
I	Application Error	2
I	Client-Side (JavaScript) Cookie References	4
I	Cookie with SameSite attribute not Restrictive	1
I	Email Address Pattern Found	10
I	Integer Overflow	1
I	Missing "Referrer policy" Security Header	1
I	Possible Server Path Disclosure Pattern Found	1

Vulnerable URLs 64

TOC

	URL	Number of Issues
M	https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79	2
M	https://stage.rrev-engine.com/room/My-first-room-75	2
M	https://stage.rrev-engine.com/room/security-77	2
M	https://stage.rrev-engine.com/	14
M	https://stage.rrev-engine.com/user/	2
M	https://stage.rrev-engine.com/core/assets/vendor/once/once.min.js	1
M	https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO	1
M	https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD	2
M	https://stage.rrev-engine.com/Multiple-Learning-Pathways	1

M	https://stage.rrev-engine.com/Outdoor-Education	1	
M	https://stage.rrev-engine.com/Staged-Feedback	1	
M	https://stage.rrev-engine.com/Yet-To-Be-Imagined	1	
M	https://stage.rrev-engine.com/catesdoe_resourced/folder/add	1	
M	https://stage.rrev-engine.com/catesdoe_resourced/folder/library/749	1	
M	https://stage.rrev-engine.com/comment/336	1	
M	https://stage.rrev-engine.com/comment/364	1	
M	https://stage.rrev-engine.com/comment/372	1	
M	https://stage.rrev-engine.com/comment/392	1	
M	https://stage.rrev-engine.com/comment/395	1	
M	https://stage.rrev-engine.com/comment/reply/comment/321/field_replies/322	1	
M	https://stage.rrev-engine.com/comment/reply/comment/336/field_replies	1	
M	https://stage.rrev-engine.com/comment/reply/comment/342/field_replies/348	1	
M	https://stage.rrev-engine.com/comment/reply/group/69/field_group_comments	1	
M	https://stage.rrev-engine.com/comment/reply/group/69/field_group_comments/	1	
M	https://stage.rrev-engine.com/document-search	1	
M	https://stage.rrev-engine.com/filter/tips	1	
M	https://stage.rrev-engine.com/group/65/leave	1	
M	https://stage.rrev-engine.com/group/69	2	
M	https://stage.rrev-engine.com/group/69/filter	1	
M	https://stage.rrev-engine.com/group/80/filter	1	
M	https://stage.rrev-engine.com/group/80/join	1	
M	https://stage.rrev-engine.com/my-rooms	1	
M	https://stage.rrev-engine.com/private-message/create	2	
M	https://stage.rrev-engine.com/private-messages	1	
M	https://stage.rrev-engine.com/public-rooms	1	
M	https://stage.rrev-engine.com/resourcED	1	
M	https://stage.rrev-engine.com/resourcED/create	1	
M	https://stage.rrev-engine.com/resourcED/topic/1	1	
M	https://stage.rrev-engine.com/resourcED/topic/100	1	
M	https://stage.rrev-engine.com/resourcED/topic/7	1	
M	https://stage.rrev-engine.com/room/create	1	
M	https://stage.rrev-engine.com/search	1	
M	https://stage.rrev-engine.com/search/	1	
M	https://stage.rrev-engine.com/user	2	
M	https://stage.rrev-engine.com/user-dashboard	1	
M	https://stage.rrev-engine.com/user/163/edit	2	
M	https://stage.rrev-engine.com/user/Admin-Elaine-Bartley-156	1	
M	https://stage.rrev-engine.com/user/Dang-Tran-5	1	
M	https://stage.rrev-engine.com/user/EP-Bartley-152	1	
M	https://stage.rrev-engine.com/user/Laura-Bryant-130	1	
M	https://stage.rrev-engine.com/user/Maine-DoE-163	2	
M	https://stage.rrev-engine.com/user/Perrin-RREV-Coach-Chick-154	1	
M	https://stage.rrev-engine.com/user/Tajinder-Minhas-168	1	

M	https://stage.rrev-engine.com/user/edit	2
M	https://stage.rrev-engine.com/user/login	2
M	https://stage.rrev-engine.com/user/mainedoe-mainedoe-163	2
M	https://stage.rrev-engine.com/user/password	2
I	https://stage.rrev-engine.com/whiteboard	2
I	https://stage.rrev-engine.com/core/assets/vendor/ckeditor/ckeditor.js	1
I	https://stage.rrev-engine.com/core/assets/vendor/js-cookie/js.cookie.min.js	1
I	https://stage.rrev-engine.com/core/misc/jquery.cookie.shim.js	1
I	https://stage.rrev-engine.com/modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js	1
I	https://stage.rrev-engine.com/modules/contrib/extlink/extlink.js	1
I	https://stage.rrev-engine.com/core/modules/file/file.js	1

Fix Recommendations 12

TOC

	Remediation Task	Number of Issues
L	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"	56
L	Add to each third-party script/link element support to SRI(Subresource Integrity).	3
L	Config your server to use the "Content-Security-Policy" header with secure policies	4
L	Config your server to use the "Referrer Policy" header with secure policies	1
L	Do not allow sensitive information to leak.	1
L	Download the relevant security patch for your web server or web application.	1
L	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	1
L	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	7
L	Remove business and security logic from the client side	4
L	Remove e-mail addresses from the website	10
L	Review possible solutions for configuring SameSite Cookie attribute to recommended values	1
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	3

Security Risks 8

TOC

	Risk	Number of Issues
M	In case the third-party server is compromised, the content/behavior of the site will change	3
M	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	7
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	17
M	It is possible to persuade a naive user to supply sensitive information such as	62

	username, password, credit card number, social security number etc.		
I	It is possible to gather sensitive debugging information	3	
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	4	
I	Prevent cookie information leakage by restricting cookies to first-party or same-site context to Strict.	1	
I	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application	1	

Causes 10

TOC

	Cause	Number of Issues
M	There is no support to Subresource Integrity.	3
M	The web server or application server are configured in an insecure way	7
M	Insecure web application programming or configuration	17
M	The rel attribute in the link element is not set to "noopener noreferrer".	56
I	Proper bounds checking were not performed on incoming parameter values	2
I	No validation was done in order to make sure that user input matches the data type expected	2
I	Cookies are created at the client side	4
I	Sensitive Cookie with Unrestrictive SameSite Attributes and Flags	1
I	An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).	1
I	Latest patches or hotfixes for 3rd. party products were not installed	1

WASC Threat Classification

TOC

Threat	Number of Issues
Abuse of Functionality	56
Information Leakage	31
Integer Overflows	1
Remote File Inclusion	3
Server Misconfiguration	1

Issues Sorted by Issue Type

M Check for SRI (Subresource Integrity) support 3 TOC

Issue 1 of 3 TOC

Check for SRI (Subresource Integrity) support

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/My-first-room-75
Entity:	My-first-room-75 (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Cause:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Difference:

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Test Requests and Responses:

```
GET /room/My-first-room-75 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:36 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/My-first-room-75>; rel="canonical", <https://stage.rrev-engine.com/group/75>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
```

```
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/
...
...
...

<script src="/modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js?v=9.3.12"></script>
<script src="/core/misc/active-link.js?v=9.3.12"></script>
<script src="/modules/contrib/extlink/extlink.js?v=9.3.12"></script>
<script src="/modules/custom/whiteboard_proxy/js/jitsi_meeting.js?ri7ssq"></script>
<script src="https://8x8.vc/external_api.js"></script>
<script src="/modules/custom/catesdoe/modules/catesdoe_room/js/whiteboard.js?ri7ssq"></script>
<script src="/modules/custom/whiteboard_proxy/js/whiteboard_proxy.js?ri7ssq"></script>
<script src="/core/assets/vendor/js-cookie/js.cookie.min.js?v=3.0.1"></script>
<script src="/core/misc/jquery.cookie.shim.js?v=9.3.12"></script>
...
...
...
```

Issue 2 of 3

TOC

Check for SRI (Subresource Integrity) support

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79
Entity:	Drag-and-Drop-test-room-79 (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Cause:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Difference:

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Test Requests and Responses:

```
GET /room/Drag-and-Drop-test-room-79 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79>; rel="canonical", <https://stage.rrev-
engine.com/group/79>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http
...
...
...

<script src="/modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js?v=9.3.12"></script>
<script src="/core/misc/active-link.js?v=9.3.12"></script>
<script src="/modules/contrib/extlink/extlink.js?v=9.3.12"></script>
<script src="/modules/custom/whiteboard_proxy/js/jitsi_meeting.js?ri7ssq"></script>
<script src="https://8x8.vc/external_api.js"></script>
<script src="/modules/custom/catesdoe/modules/catesdoe_room/js/whiteboard.js?ri7ssq"></script>
<script src="/modules/custom/whiteboard_proxy/js/whiteboard_proxy.js?ri7ssq"></script>
<script src="/core/assets/vendor/js-cookie/js.cookie.min.js?v=3.0.1"></script>
<script src="/core/misc/jquery.cookie.shim.js?v=9.3.12"></script>
...
```

```
...
...
```

Issue 3 of 3

TOC

Check for SRI (Subresource Integrity) support

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/security-77
Entity:	security-77 (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Cause:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Difference:

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Test Requests and Responses:

```
GET /room/security-77 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/public-rooms
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-
06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:48:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/security-77>; rel="canonical", <https://stage.rrev-engine.com/group/77>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
```

```
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules
...
...
...

<script src="/modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js?v=9.3.12"></script>
<script src="/core/misc/active-link.js?v=9.3.12"></script>
<script src="/modules/contrib/extlink/extlink.js?v=9.3.12"></script>
<script src="/modules/custom/whiteboard_proxy/js/jitsi_meeting.js?ribj6r"></script>
<script src="https://8x8.vc/external_api.js"></script>
<script src="/modules/custom/catesdoe/modules/catesdoe_room/js/whiteboard.js?ribj6r"></script>
<script src="/modules/custom/whiteboard_proxy/js/whiteboard_proxy.js?ribj6r"></script>
<script src="/core/assets/vendor/js-cookie/js.cookie.min.js?v=3.0.1"></script>
<script src="/core/misc/jquery.cookie.shim.js?v=9.3.12"></script>
...
...
...
```

M Hidden Directory Detected 7 TOC

Issue 1 of 7 TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	sites/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/sites/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /sites/?v=1.0.1 HTTP/1.1
```

```
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:59:43 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 199
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
```

Issue 2 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	admin/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/admin/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /admin/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:52:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
X-Drupal-Cache: MISS
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent
```

Issue 3 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/
Entity:	current/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/user/login` to: `/user/current/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /user/current/ HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:52:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
X-Drupal-Cache: MISS
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent
```

Issue 4 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	modules/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/modules/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /modules/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:59:43 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 199
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
```

Issue 5 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	themes/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/themes/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /themes/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
```

```
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:59:43 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 199
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
```

Issue 6 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	libraries/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/libraries/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /libraries/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:59:43 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 199
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
```

Issue 7 of 7

TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	batch/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/core/assets/vendor/once/once.min.js` to: `/batch/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /batch/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 403 Forbidden
Date: Mon, 19 Sep 2022 16:52:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
Permissions-Policy: interest-cohort=()
```

```
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
X-Drupal-Cache: MISS
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent
```

M Unnecessary Http Response Headers found in the Application 1 TOC

Issue 1 of 1 TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/core/assets/vendor/once/once.min.js
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Difference:

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Test Requests and Responses:

```
GET /core/assets/vendor/once/once.min.js?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:28:22 GMT
Content-Type: application/javascript
Content-Length: 1357
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 20 Apr 2022 14:25:27 GMT
ETag: "54d-5dd16c3c463c0"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 19:28:22 GMT
Vary: Accept-Encoding,User-Agent

/*! @drupal/once - v1.0.1 - 2021-06-12 */
var once=function(){"use strict";var n=/[\11\12\14\15\40]+/,e="data-once",t=document;function r(n,t,r){return
```

```
n[t+"Attribute"](e,r)}function o(e){if("string"!=typeof e)throw new TypeError("once ID must be a
string");if(""===e||n.test(e))throw new RangeError("once ID must not be empty or contain spaces");return'[data-
once~="'+e+'"]'}function u(n){if(!(n instanceof Element))throw new TypeError("The element must be an instance of
Element");return!0}function i(n,e){void 0===e&&(e=t);var r=n;if(null===n)r=[];else{if(!n)throw new TypeError("Selector must
not be empty");"string"!=typeof n||e!==t&&!u(e)?n instanceof Element&&(r=[n]):r=e.querySelectorAll(n)}return
Array.prototype.slice.call(r)}function c(n,e,t){return e.filter((function(e){var r=u(e)&&e.matches(n);return
r&&t&&t(e),r}))}function f(e,t){var o=t.add,u=t.remove,i=[];r(e,"has")&&r(e,"get").trim().split(n).forEach((function(n)
{i.indexOf(n)<0&&n!==u&&i.push(n)})),o&&i.push(o);var c=i.join(" ");r(e,""===c?"remove":"set",c)}function a(n,e,t){return
c(":not("+o(n)+")",i(e,t),(function(e){return f(e,{add:n})}))}return a.remove=function(n,e,t){return c(o(n),i(e,t),
(function(e){return f(e,{remove:n})}))},a.filter=function(n,e,t){return c(o(n),i(e,t))},a.find=function(n,e){return i(n?
o(n):"[data-once]",e)},a}();
//# sourceMappingURL=once.min.js.map
```

M Unsafe third-party link (target="_blank") 56

TOC

Issue 1 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO
Entity:	Extended-Learning-Opportunities-ELO (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Extended-Learning-Opportunities-ELO HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/group/66/join
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:52 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO>; rel="canonical", <https://stage.rrev-
engine.com/group/66>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
...
...
...d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 2 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/document-search
Entity:	document-search (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /document-search?search_api_fulltext=1234 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/login
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 18:59:54 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: HIT
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs:
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 3 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/search
Entity:	search (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /search?search_api_fulltext=1234 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:22:29 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: stri
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 4 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET / HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/search?search_api_fulltext=25&last-edited-date=All&last-edited%5Bmin%5D=1234&last-
edited%5Bmax%5D=1234
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:54 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/node/1>; rel="canonical", <https://stage.rrev-engine.com/node/1>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rr
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 5 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Outdoor-Education
Entity:	Outdoor-Education (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Outdoor-Education HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/group/64/join
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:53 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Outdoor-Education>; rel="canonical", <https://stage.rrev-engine.com/group/64>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
```

```
Surrogate-Control: no-store, conte
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 6 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Yet-To-Be-Imagined
Entity:	Yet-To-Be-Imagined (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Yet-To-Be-Imagined HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/group/68/join
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Yet-To-Be-Imagined>; rel="canonical", <https://stage.rrev-engine.com/group/68>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
```

```
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, con
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 7 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/reply/comment/321/field_replies/322
Entity:	322 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/reply/comment/321/field_replies/322 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user-dashboard
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:58 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/reply/comment/342/field_replies/348
Entity:	348 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/reply/comment/342/field_replies/348 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user-dashboard
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:58 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 9 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Multiple-Learning-Pathways
Entity:	Multiple-Learning-Pathways (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Multiple-Learning-Pathways HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/comment/393
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr
```

```
HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:40 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Multiple-Learning-Pathways>; rel="canonical", <https://stage.rrev-
engine.com/group/65>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; repor
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 10 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user-dashboard
Entity:	user-dashboard (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user-dashboard HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user-dashboard
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
```

```
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXie
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 11 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Staged-Feedback
Entity:	Staged-Feedback (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Staged-Feedback HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/Online-Education
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:20:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
```

```
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Staged-Feedback>; rel="canonical", <https://stage.rrev-engine.com/group/80>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 12 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD
Entity:	Innovative-Mindset-Pilot-development-IMPD (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /Innovative-Mindset-Pilot-development-IMPD HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:21:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.main
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 13 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/private-messages
Entity:	private-messages (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /private-messages HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:23:52 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin

...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 14 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/group/69/filter
Entity:	filter (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /group/69/filter?destination=group/69&topics HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
```

```
Date: Fri, 16 Sep 2022 19:23:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 15 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/group/65/leave
Entity:	leave (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /group/65/leave HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Multiple-Learning-Pathways
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:25:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
```

```
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 16 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/reply/group/69/field_group_comments/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/reply/group/69/field_group_comments/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:24:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
```

```
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 17 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/reply/comment/336/field_replies
Entity:	field_replies (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/reply/comment/336/field_replies HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:24:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cook
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
```

```
...
```

Issue 18 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/group/69
Entity:	69 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /group/69 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/group/69/filter?destination=group/69&topics=
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:23:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
```

```
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 19 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/372
Entity:	372 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/372 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

```
Referer: https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD?sort_by=created&sort_order=DESC
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:24:07 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink", <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>;
rel="canonical", <https://stage.rrev-engine.com/group/69>; rel="shortlink"
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 20 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/395
Entity:	395 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/395 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/Outdoor-Education?sort_by=created&sort_order=DESC
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:24:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Outdoor-Education>; rel="canonical", <https://stage.rrev-engine.com/group/64>;
rel="shortlink", <https://stage.rrev-engine.com/Outdoor-Education>; rel="canonical", <https://stage.rrev-
engine.com/group/64>; rel="shortlink"
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security:
...
```

```
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 21 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/392
Entity:	392 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/392 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/Staged-Feedback?sort_by=created&sort_order=DESC
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:25:34 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Staged-Feedback>; rel="canonical", <https://stage.rrev-engine.com/group/80>;
```

```
rel="shortlink", <https://stage.rrev-engine.com/Staged-Feedback>; rel="canonical", <https://stage.rrev-
engine.com/group/80>; rel="shortlink"
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-ag
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 22 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/364
Entity:	364 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/364 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO?sort_by=created&sort_order=DESC
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:24:11 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO>; rel="canonical", <https://stage.rrev-
engine.com/group/66>; rel="shortlink", <https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO>;
rel="canonical", <https://stage.rrev-engine.com/group/66>; rel="shortlink"
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-viola
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user
Entity:	user (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/comment/383
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; Drupal-quicktabs-active-
tab-id-my_engine_landing_page=1


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 20:04:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
```

```
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-orig
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 24 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Maine-DoE-163
Entity:	Maine-DoE-163 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Maine-DoE-163 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; Drupal-quicktabs-active-
tab-id-my_engine_landing_page=1


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:25:59 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cooki
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 25 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/group/80/join
Entity:	join (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /group/80/join HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Staged-Feedback
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:25:27 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
```

```
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXie
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 26 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/163/edit
Entity:	edit (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/163/edit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/edit
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:26:35 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
```

```
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cooki
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 27 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/edit
Entity:	edit (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/edit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/Maine-DoE-163
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 19:26:30 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Location: https://stage.rrev-engine.com/user/163/edit
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html>
    <head>
        <meta charset=
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
```

```
</div>
...
...
...
```

Issue 28 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/my-rooms
Entity:	my-rooms (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /my-rooms HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user/%5Bcurrent-user%3Auid%5D/settings
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:28:17 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
```

```
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security:
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 29 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/resourcED
Entity:	resourcED (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /resourcED HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/catesdoe_resourced/folder/library/749?destination=/resourcED&ajax=1
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
```

```
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:28:19 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov
...
...
...

<div  class="field-name visibility">
      <a href="https://medium.com/analytics-vidhya/build-deploy-a-natural-language-processing-nlp-app-with-spacy-streamlit-
and-heroku-54e78468f" target="_blank">NLP project</a>
          <div class="field field--name-field-resourced-visibility field--type-boolean field--label-hidden field__item">
</div>

  </div>
...
...
...d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/EP-Bartley-152
Entity:	EP-Bartley-152 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/EP-Bartley-152 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:37:30 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
```

```
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 31 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/private-message/create
Entity:	create (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /private-message/create?recipient=152&direct-message=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/EP-Bartley-152
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:38:07 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
```

```
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 32 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/resourcED/create
Entity:	create (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /resourcED/create?destination=/resourcED HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Enco
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
```

```
...
```

Issue 33 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/resourcED/topic/7
Entity:	7 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /resourcED/topic/7 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:30 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: HIT
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
```

```
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine
...
...
...

<div  class="field-name visibility">
      <a href="https://www.edutopia.org/article/promoting-student-led-learning-elementary-school" target="_blank">Student-
led learning</a>
          <div class="field field--name-field-resourced-visibility field--type-boolean field--label-hidden field__item">
</div>

  </div>
...
...
...d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 34 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/create
Entity:	create (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /room/create?destination=/my-rooms HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/my-rooms
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr
```

```
HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:38:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Upgrade: h2,h2c
Vary: A
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/catesdoe_resourced/folder/library/749
Entity:	749 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /catesdoe_resourced/folder/library/749?destination=/resourcED&ajax=1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:02 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
```

```
X-Accel-Buff
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 36 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/resourcED/topic/100
Entity:	100 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /resourcED/topic/100 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: HIT
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
```

```
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie:
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 37 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/My-first-room-75
Entity:	My-first-room-75 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /room/My-first-room-75 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:31 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/My-first-room-75>; rel="canonical", <https://stage.rrev-engine.com/group/75>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/public-rooms
Entity:	public-rooms (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /public-rooms HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/my-rooms
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:38:07 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
```

```
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie:
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 39 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/resourcED/topic/1
Entity:	1 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /resourcED/topic/1 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:30 GMT
Content-Type: text/html; charset=UTF-8
```

```
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: HIT
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: S
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/catesdoe_resourced/folder/add
Entity:	add (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /catesdoe_resourced/folder/add HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/catesdoe_resourced/folder/add
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:25 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
```

```
X-Accel-Buffering: no
Vary: A
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 41 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79
Entity:	Drag-and-Drop-test-room-79 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /room/Drag-and-Drop-test-room-79 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/resourcED
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:39:13 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79>; rel="canonical", <https://stage.rrev-
engine.com/group/79>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origi
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 42 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/password
Entity:	password (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/password HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user/163/edit
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:52:20 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/filter/tips
Entity:	tips (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /filter/tips HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/Extended-Learning-Opportunities-ELO
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:59:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: HIT
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
```

```
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-cs
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 44 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Perrin-RREV-Coach-Chick-154
Entity:	Perrin-RREV-Coach-Chick-154 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Perrin-RREV-Coach-Chick-154 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
```

```
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:53:44 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
...
...
...
```

Issue 45 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Tajinder-Minhas-168
Entity:	Tajinder-Minhas-168 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Tajinder-Minhas-168 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/comment/323
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:53:44 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-v
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 46 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Dang-Tran-5
Entity:	Dang-Tran-5 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Dang-Tran-5 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/comment/363
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:53:46 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

```
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
...
...
...d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 47 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Admin-Elaine-Bartley-156
Entity:	Admin-Elaine-Bartley-156 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Admin-Elaine-Bartley-156 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:53:47 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 48 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/login
Entity:	login (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/login HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 20:04:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Upgrade: h2,h2c
Location: https://stage.rrev-engine.com/user/mainedoe-mainedoe-163
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="0;url='https://stage.rrev-engi
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 49 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/room/security-77
Entity:	security-77 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /room/security-77 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/public-rooms
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-
06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv
```

```
HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:48:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/room/security-77>; rel="canonical", <https://stage.rrev-engine.com/group/77>;
rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 50 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/Laura-Bryant-130
Entity:	Laura-Bryant-130 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/Laura-Bryant-130 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:53:49 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
```

```
uri /report-csp-violation
X-XSS-Prot
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 51 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/mainedoe-mainedoe-163
Entity:	mainedoe-mainedoe-163 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/mainedoe-mainedoe-163 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/login
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:04:11 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
```

```
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJ
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 52 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/reply/group/69/field_group_comments
Entity:	field_group_comments (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
POST /comment/reply/group/69/field_group_comments HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/comment/reply/group/69/field_group_comments/
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv
Content-Length: 524

field_comment_body%5B0%5D%5Bvalue%5D=1234&form_build_id=form-cENU9vLpcICP1Ty-NC-8-
Xie4brdIlSvstnebIHmMjU&form_token=2_imicWKOVWN920aJ76hNSvgtBkZOxAjyymU_69IF2k&form_id=comment_group_comments_form&value=%25
AutoEntityLabel%25&field_topics%5B%5D=90&field_suggest_a_new_topic%5B0%5D%5Bstatus%5D=0&field_suggest_a_new_topic%5B0%5D%5B
last_edited_uid%5D=0&field_suggest_a_new_topic%5B0%5D%5Bvalue%5D=1234&field_suggest_a_new_topic%5B0%5D%5B_weight%5D=0&field
_is_deleted%5Bvalue%5D=1&ief-field_media_attachment-form-add=Add+new+file

HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:38:16 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/group/80/filter
Entity:	filter (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /group/80/filter?destination=group/80&topics%5B98%5D=98&topics%5B99%5D=99 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/Staged-Feedback?topics%5B98%5D=98&topics%5B99%5D=99&sort_by=created&sort_order=DESC
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:38:07 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
```

```
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigP
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 54 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/comment/336
Entity:	336 (Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /comment/336 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/flag/unflag/comment_cheer/336?
destination&token=RgwHBT_rbTeiLnytkq9tpsDu8_mJIxTGRdECxfhwq3s
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:48:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink", <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>;
```

```
rel="canonical", <https://stage.rrev-engine.com/group/69>; rel="shortlink"
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Frame-Options: SAMEORIG
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 55 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/user/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /user/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 302 Found
Date: Mon, 19 Sep 2022 16:52:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: MISS
Location: https://stage.rrev-engine.com/user/login
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />

...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
```

```
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 56 of 56

TOC

Unsafe third-party link (target="_blank")

Severity:	Medium
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/search/
Entity:	(Page)
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Difference:

Reasoning: The third-party links with target="_blank" attribute and no rel="noopener noreferrer" attribute allows linked page partial access to the linking page window object

Test Requests and Responses:

```
GET /search/?v=1.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 200 OK
Date: Mon, 19 Sep 2022 17:00:05 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: HIT
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modu
...
...
...
d="9ffcad81-157e-45d7-8da8-80a458f4cff6" src="/sites/default/files/inline-images/Maine-DOE-Logo-White.png" width="356"
height="122" loading="lazy" /></p><div class="social-wrapper">Follow the Maine DOE
<div class="social-icons-container"><a aria-label="Link to DOE Facebook page" class="footer-icon"
href="https://www.facebook.com/MaineDepartmentofEducation1" target="_blank"><img alt="Facebook icon"
src="/themes/custom/cates/img/facebook-icon.svg" /></a> <a aria-label="Link to DOE Twitter page" class="footer-icon"
href="https://twitter.com/mdoeNews" target="_blank"> <img alt="Twitter icon" src="/themes/custom/cates/img/twitter-
icon.svg" /></a> <a aria-label="Link to DOE YouTube page" class="footer-icon"
href="https://www.youtube.com/user/MaineDOEComm" target="_blank"> <img alt="Youtube Icon"
src="/themes/custom/cates/img/youtube-icon.svg" /></a> <a aria-label="Link to DOE Instagram page" class="footer-icon"
href="https://www.instagram.com/mainedepted/" target="_blank"> <img alt="Instagram Icon"
src="/themes/custom/cates/img/instagram-icon.svg" /></a></div>
</div>
</div>
...
...
...
```

Issue 1 of 1

TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /modules/contrib/seckit/js/seckit.document_write.js HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:27:57 GMT
Content-Type: application/javascript
Content-Length: 221
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 14 Sep 2022 19:22:54 GMT
ETag: "dd-5e8a80e341f80"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 19:27:57 GMT
Vary: Accept-Encoding,User-Agent

/**
 * If site is not being framed or being framed within the same host,
 * start commenting out seckit.no_body.css.
 */
```

```
if (top === self || top.location.hostname === self.location.hostname) {
  document.write('<!--');
}
```

L Missing or Insecure "Object-Src" policy in "Content-Security-Policy" header 1 TOC

Issue 1 of 1 TOC

Missing or Insecure "Object-Src" policy in "Content-Security-Policy" header

Severity:	Low
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /user/login HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 18:57:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
```

```
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: HIT
Vary: Accept-Encoding,User-Agent
Content-Length: 33097

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<link rel="icon" href="/themes/custom/cates/favicon.ico" type="image/vnd.microsoft.icon" />
<script src="/sites/default/files/google_tag/production/google_tag.script.js?ri7ssq" defer></script>
<script src="/sites/default/files/google_tag/dev/google_tag.script.js?ri7ssq" defer></script>

    <title>Sign In | RREV</title>
    <link rel="stylesheet" media="all" href="/modules/custom/catesdoe/modules/catesdoe_resourced/css/catesdoe_r
...
...
...
```

L Missing or Insecure "Script-Src" policy in "Content-Security-Policy" header 1 TOC

Issue 1 of 1 TOC

Missing or Insecure "Script-Src" policy in "Content-Security-Policy" header

Severity:	Low
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /user/login HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 18:57:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
```

```
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: HIT
Vary: Accept-Encoding,User-Agent
Content-Length: 33097

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<link rel="icon" href="/themes/custom/cates/favicon.ico" type="image/vnd.microsoft.icon" />
<script src="/sites/default/files/google_tag/production/google_tag.script.js?ri7ssq" defer></script>
<script src="/sites/default/files/google_tag/dev/google_tag.script.js?ri7ssq" defer></script>

    <title>Sign In | RREV</title>
    <link rel="stylesheet" media="all" href="/modules/custom/catesdoe/modules/catesdoe_resourced/css/catesdoe_r
...
...
...
```

L Missing or Insecure "Style-Src" policy in "Content-Security-Policy" 1 TOC

Issue 1 of 1 TOC

Missing or Insecure "Style-Src" policy in "Content-Security-Policy"

Severity:	Low
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /user/login HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
```

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:01:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: MISS
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
X-Drupal-Cache: HIT
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />
<link rel="icon" href="/themes/custom/cates/favicon.ico" type="image/vnd.microsoft.icon" />
<script src="/sites/default/files/google_tag/production/google_tag.script.js?ri7ssq" defer></script>
<script src="/sites/default/files/google_tag/dev/google_tag.script.js?ri7ssq" defer></script>

    <title>Sign In | RREV</title>
    <link rel="stylesheet" media="all"
href="/modules/custom/catesdoe/modules/catesdoe_resourced/css/catesdoe_resourced.css?r
...
...
...
```

Issue 1 of 1

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity:	Low
CVSS Score:	6.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Test Requests and Responses:

```
GET /modules/contrib/blazy/js/polyfill/blazy.polyfill.min.js?ri7ssq HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 21:18:40 GMT
Content-Type: application/javascript
Content-Length: 1151
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Fri, 16 Sep 2022 19:44:32 GMT
ETag: "47f-5e8d09740c800"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 21:18:40 GMT
Vary: Accept-Encoding,User-Agent

!function(t){"use strict";var n=Element.prototype,e=NodeList.prototype,r=String.prototype;function o(t,e){e=e||
{bubbles:!1,cancelable:!1,detail:null};var n=document.createEvent("CustomEvent");return
n.initCustomEvent(t,e.bubbles,e.cancelable,e.detail),n}n.matches||
(n.matches=n.msMatchesSelector||n.webkitMatchesSelector),n.closest||(n.closest=function(t){var
e=this;do{if(n.matches.call(e,t))return e}while(null!==(e=e.parentElement||e.parentNode)&&1===e.nodeType);return
null}),t.NodeList&&!e.forEach&&(e.forEach=Array.prototype.forEach),"function"!=typeof
Object.assign&&Object.defineProperty(Object,"assign",{value:function(t,e){if(null===t||"undefined"===t)throw new
TypeError("Cannot convert undefined or null to object");for(var n=Object(t),r=1;r<arguments.length;r++){var
o=arguments[r];if(null!==o&&"undefined"!==o)for(var c in o)Object.prototype.hasOwnProperty.call(o,c)&&(n[c]=o[c])}return
n},writable:!0,configurable:!0}),r.startsWith||Object.defineProperty(r,"startsWith",{value:function(t,e){e=0<e?0|e:0;return
this.substring(e,e+t.length)===t}}),"function"!=typeof t.CustomEvent&&(o.prototype=t.Event.prototype,t.CustomEvent=o)}
(this);
```

Issue 1 of 2

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/private-message/create
Entity:	ajax_page_state[theme] (Parameter)
Risk:	It is possible to gather sensitive debugging information
Cause:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Difference: **Parameter** `ajax_page_state[theme]` manipulated from: `ajax_page_state[theme]` to: `__ORIG_VAL__[]`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /private-message/create?recipient=155&direct-message=1&_wrapper_format=drupal_modal HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://stage.rrev-engine.com/user/Helene-RREV-Coach-Adams-155
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv
Content-Length: 352

js=true&dialogOptions%5BminWidth%5D=800&_drupal_ajax=1&ajax_page_state%5Btheme%5D%5B%5D=cates&ajax_page_state%5Btheme_token
%5D=&ajax_page_state%5Blibraries%5D=blazy%2Fbio.ajax%2Ccates%2Fcates-user-profile-
strengths%2Ccatesdoe%2Fcatesdoe.ajax%2Clayout_discovery%2Fonecol%2Cviews%2Fviews.ajax%2Cviews%2Fviews.module%2Cviews_entity
_form_field%2Fviews_form

HTTP/1.1 500 500 Service unavailable (with message)
Date: Mon, 19 Sep 2022 12:49:52 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Vary: Accept-Encoding,User-Agent

The website encountered an unexpected error. Please try again later.
```

Issue 2 of 2

TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/whiteboard
Entity:	whiteboardid (Parameter)
Risk:	It is possible to gather sensitive debugging information
Cause:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Difference: **Parameter** `whiteboardid` manipulated from: `79` to: `%27`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
GET /whiteboard?whiteboardid=%27&username=mainedoe_mainedoe HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79?sort_by=title&sort_order=DESC
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-
06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv
```

```
HTTP/1.1 500 500 Service unavailable (with message)
Date: Mon, 19 Sep 2022 16:59:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: no-cache, private
X-Content-Type-Options: nosniff
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent

The website encountered an unexpected error. Please try again later.<br />
```

I Client-Side (JavaScript) Cookie References 4

TOC

Issue 1 of 4

TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js
Entity:	(function ($, Drupal) { (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Difference:

Reasoning: AppScan found a reference to cookies in the JavaScript.

Test Requests and Responses:

```
GET /modules/contrib/simple_popup_blocks/js/simple_popup_blocks.js?v=9.3.12 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:36:47 GMT
Content-Type: application/javascript
Content-Length: 11554
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 14 Sep 2022 19:22:54 GMT
ETag: "2d22-5e8a80e341f80"
Accept-Ranges: bytes
```

```
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 19:36:47 GMT
Vary: Accept-Encoding,User-Agent

(function ($, Drupal) {

  'use strict'

  Drupal.behaviors.simplePopupBlocks = {
    attach: function (context, settings) {
      // Global variables
      var popup_settings = drupalSettings.simple_popup_blocks.settings,
        _html = document.documentElement, windowWidth = $(window).width();

      $.each(popup_settings, function (index, values) {

        // No popup when the window width is less than the trigger width.
      if (windowWidth < values.trigger_width) {return null;};

        // Declaring variable inside foreach - so it will not global.
        var modal_class = '',
          block_id = values.identifier,
          visit_counts_arr = values.visit_counts.split(','),
          allow_cookie = true,
          read_cookie = '',
          cookie_val = 1,
          cookie_days = values.cookie_expiry || 100,
          match = 0,
          css_identity = '',
          spb_popup_id = '',
          modal_close_class = '',
          modal_minimize_class = '',
          modal_minimized_class = '',
          layout_class = '',
          class_exists = false,
          delays = '',
          browser_close_trigger = true,
          use_time_frequency = values.use_time_frequency,
          time_frequency = values.time_frequency,
          time_frequency_cookie = 0,
          next_popup = 0,
          current_timestamp = 0,
          show_minimized_button = values.show_minimized_button,
          show_model = true
        // Always show popup, so prevent from creating cookie
        if (visit_counts_arr.length == 1 && visit_counts_arr[0] == 0 && use_time_frequency == 0) {
          allow_cookie = false
        }
        // Check to see if the block exists in the current page.
        var element = document.getElementById(block_id);
        if (typeof(element) != 'undefined' && element != null) {
        // Creating cookie
        if (allow_cookie == true) {
        if (use_time_frequency == 0) {
          read_cookie = readCookie('spb_' + block_id)
          if (read_cookie) {
          cookie_val = + read_cookie + 1
          createCookie('spb_' + block_id, cookie_val, 100)
          }
          else {
          createCookie('spb_' + block_id, cookie_val, 100)
          }
          // Match cookie
          cookie_val = cookie_val.toString()
          match = $.inArray(cookie_val, visit_counts_arr)

          if (match === -1) {
          show_model = false
          }
          }
          else {
          time_frequency_cookie = readCookie('spb_time' + block_id)
          current_timestamp = Math.floor(Date.now() / 1000)
          next_popup = current_timestamp + parseInt(time_frequency, 10)

          if (time_frequency_cookie) {
          // If current_timestamp is greater than cookie time show the popup.
          if (current_timestamp >= time_frequency_cookie) {
          match = 1
          }
          // This should allow the time frequency to be adjusted down after
          // the cookie has been set.
          else if (next_popup <= time_frequency_cookie) {
          match = 1
```

```
            }
            else {
            match = -1
            show_model = false
            }

            // Create new cookie for popup.
            if (match === 1) {
            createCookie('spb_time' + block_id, next_popup, 100)
            }
            }
            else {
            createCookie('spb_time' + block_id, next_popup, 100)
            }
            }
          }

          }
          // Set css selector
          css_identity = '.'
          if (values.css_selector == 1) {
            css_identity = '#'
          }

          // Assign dynamic css classes
          spb_popup_id = 'spb-' + block_id
          modal_class = block_id + '-modal'
          modal_close_class = block_id + '-modal-close'
          modal_minimize_class = block_id + '-modal-minimize'
          modal_minimized_class = block_id + '-modal-minimize
...
...
...

      }
      else {
        var expires = ''
      }
      document.cookie = name + '=' + value + expires + '; path=/'
    }
...
...
...
```

Issue 2 of 4

TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/core/misc/jquery.cookie.shim.js
Entity:	/** (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Difference:

Reasoning: AppScan found a reference to cookies in the JavaScript.

Test Requests and Responses:

```
GET /core/misc/jquery.cookie.shim.js?v=9.3.12 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
```

```
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 21:14:58 GMT
Content-Type: application/javascript
Content-Length: 4111
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 20 Apr 2022 14:25:27 GMT
ETag: "100f-5dd16c3c463c0"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 21:14:58 GMT
Vary: Accept-Encoding,User-Agent

/**
* DO NOT EDIT THIS FILE.
* See the following change record for more information,
* https://www.drupal.org/node/2815083
* @preserve
**/

function ownKeys(object, enumerableOnly) { var keys = Object.keys(object); if (Object.getOwnPropertySymbols) { var symbols
= Object.getOwnPropertySymbols(object); enumerableOnly && (symbols = symbols.filter(function (sym) { return
Object.getOwnPropertyDescriptor(object, sym).enumerable; })), keys.push.apply(keys, symbols); } return keys; }

function _objectSpread(target) { for (var i = 1; i < arguments.length; i++) { var source = null != arguments[i] ?
arguments[i] : {}; i % 2 ? ownKeys(Object(source), !0).forEach(function (key) { _defineProperty(target, key, source[key]);
}) : Object.getOwnPropertyDescriptors ? Object.defineProperties(target, Object.getOwnPropertyDescriptors(source)) :
ownKeys(Object(source)).forEach(function (key) { Object.defineProperty(target, key, Object.getOwnPropertyDescriptor(source,
key)); }); } return target; }

function _defineProperty(obj, key, value) { if (key in obj) { Object.defineProperty(obj, key, { value: value, enumerable:
true, configurable: true, writable: true }); } else { obj[key] = value; } return obj; }

(function ($, Drupal, cookies) {
  var deprecatedMessageSuffix = "is deprecated in Drupal 9.0.0 and will be removed in Drupal 10.0.0. Use the core/js-cookie
library instead. See https://www.drupal.org/node/3104677";

  var isFunction = function isFunction(obj) {
    return Object.prototype.toString.call(obj) === '[object Function]';
  };

  var parseCookieValue = function parseCookieValue(value, parseJson) {
    if (value.indexOf('"') === 0) {
      value = value.slice(1, -1).replace(/\\"/g, '"').replace(/\\\\/g, '\\');
    }

    try {
      value = decodeURIComponent(value.replace(/\+/g, ' '));
      return parseJson ? JSON.parse(value) : value;
    } catch (e) {}
  };

  var reader = function reader(cookieValue, cookieName, converter, readUnsanitized, parseJson) {
    var value = readUnsanitized ? cookieValue : parseCookieValue(cookieValue, parseJson);

    if (converter !== undefined && isFunction(converter)) {
      return converter(value, cookieName);
    }

    return value;
  };

  $.cookie = function (key) {
    var value = arguments.length > 1 && arguments[1] !== undefined ? arguments[1] : undefined;
    var options = arguments.length > 2 && arguments[2] !== undefined ? arguments[2] : undefined;
    Drupal.deprecationError({
      message: "jQuery.cookie() ".concat(deprecatedMessageSuffix)
    });

    if (value !== undefined && !isFunction(value)) {
      var attributes = _objectSpread(_objectSpread({}, $.cookie.defaults), options);
```

```
      if (typeof attributes.expires === 'string' && attributes.expires !== '') {
        attributes.expires = new Date(attributes.expires);
      }

      var cookieSetter = cookies.withConverter({
        write: function write(cookieValue) {
          return encodeURIComponent(cookieValue);
        }
      });
      value = $.cookie.json && !$.cookie.raw ? JSON.stringify(value) : String(value);
      return cookieSetter.set(key, value, attributes);
    }

    var userProvidedConverter = value;
    var cookiesShim = cookies.withConverter({
      read: function read(cookieValue, cookieName) {
        return reader(cookieValue, cookieName, userProvidedConverter, $.cookie.raw, $.cookie.json);
      }
    });

    if (key !== undefined) {
      return cookiesShim.get(key);
    }

    var results = cookiesShim.get();
    Object.keys(results).forEach(function (resultKey) {
      if (results[resultKey] === undefined) {
        delete results[resultKey];
      }
    });
    return results;
  };

  $.cookie.defaults = _objectSpread({
    path: ''
  }, cookies.defaults);
  $.cookie.json = false;
  $.cookie.raw = false;

  $.removeCookie = function (key, options) {
    Drupal.deprecationError({
      message: "jQuery.removeCookie() ".concat(deprecatedMessageSuffix)

...
...
...
```

Issue 3 of 4

TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/core/assets/vendor/ckeditor/ckeditor.js
Entity:	/* (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Difference:

Reasoning: AppScan found a reference to cookies in the JavaScript.

Test Requests and Responses:

```
GET /core/assets/vendor/ckeditor/ckeditor.js?v=4.18.0 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://stage.rrev-engine.com/user/EP-Bartley-152
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 21:50:10 GMT
Content-Type: application/javascript
Content-Length: 640106
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 20 Apr 2022 14:25:27 GMT
ETag: "9c46a-5dd16c3c463c0"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 21:50:10 GMT
Vary: Accept-Encoding,User-Agent

/*
Copyright (c) 2003-2022, CKSource Holding sp. z o.o. All rights reserved.
For licensing, see LICENSE.md or https://ckeditor.com/legal/ckeditor-oss-license/
*/
(function(){window.CKEDITOR&&window.CKEDITOR.dom||(window.CKEDITOR||(window.CKEDITOR=function(){var b=/(^|.*
[\\\/])ckeditor\.js(?:\?.*|;.*)?$/i,h=
{timestamp:"M2GD",version:"4.18.0",revision:"5fe059002f",rnd:Math.floor(900*Math.random())+100,_:{pending:
[],basePathSrcPattern:b},status:"unloaded",basePath:function(){var a=window.CKEDITOR_BASEPATH||"";if(!a)for(var
e=document.getElementsByTagName("script"),f=0;f<e.length;f++){var m=e[f].src.match(b);if(m){a=m[1];break}}-
1==a.indexOf(":/")&&"//"!=a.slice(0,
2)&&(a=0===a.indexOf("/")?location.href.match(/^.*?:\/\/[^\/]*/)[0]+a:location.href.match(/^[^\?]*\/(?:)/)
[0]+a);if(!a)throw'The CKEditor installation path could not be automatically detected. Please set the global variable
"CKEDITOR_BASEPATH" before creating editor instances.';return a},getUrl:function(a){-
1==a.indexOf(":/")&&0!==a.indexOf("/")&&(a=this.basePath+a);return a=this.appendTimestamp(a)},appendTimestamp:function(a)
{if(!this.timestamp||"/"===a.charAt(a.length-1)||/[&?]t=/.test(a))return a;
var b=0<=a.indexOf("?")?"\x26":"?";return a+b+"t\x3d"+this.timestamp},domReady:function(){function a()
{try{document.addEventListener?
(document.removeEventListener("DOMContentLoaded",a,!1),window.removeEventListener("load",a,!1),b()):document.attachEvent&&"
complete"===document.readyState&&(document.detachEvent("onreadystatechange",a),window.detachEvent("onload",a),b())}catch(e)
{}}function b(){for(var a;a=e.shift();)a()}var e=[];return function(b){function c()
{try{document.documentElement.doScroll("left")}catch(g){setTimeout(c,
1);return}a()}e.push(b);"complete"===document.readyState&&setTimeout(a,1);if(1==e.length)if(document.addEventListener)docum
ent.addEventListener("DOMContentLoaded",a,!1),window.addEventListener("load",a,!1);else if(document.attachEvent)
{document.attachEvent("onreadystatechange",a);window.attachEvent("onload",a);b=!1;try{b=!window.frameElement}catch(d)
{}document.documentElement.doScroll&&b&&c()}}()},f=window.CKEDITOR_GETURL;if(f){var e=h.getUrl;h.getUrl=function(a){return
f.call(h,a)||e.call(h,a)}}return h}()),
function(){var b={};CKEDITOR.event||(CKEDITOR.event=function(){},CKEDITOR.event.implementOn=function(b){var
f=CKEDITOR.event.prototype,e;for(e in f)null==b[e]&&(b[e]=f[e])},CKEDITOR.event.prototype=function(){function h(a){var
b=f(this);return b[a]||(b[a]=new e(a))}var f=function(a){a=a.getPrivate&&a.getPrivate()||a._||(a._={});return a.events||
(a.events={})},e=function(a){this.name=a;this.listeners=[]};e.prototype={getListenerIndex:function(a){for(var
b=0,e=this.listeners;b<e.length;b++)if(e[b].fn==
a)return b;return-1}};return{define:function(a,b){var
e=h.call(this,a);CKEDITOR.tools.extend(e,b,!0)},on:function(a,e,f,m,c){function d(n,c,d,v){n=
{name:a,sender:this,editor:n,data:c,listenerData:m,stop:d,cancel:v,removeListener:g};return!1===e.call(f,n)?
b:n.data}function g(){n.removeListener(a,e)}var n=this,v=h.call(this,a);if(0>v.getListenerIndex(e)){v=v.listeners;f||
(f=this);isNaN(c)&&(c=10);d.fn=e;d.priority=c;for(var x=v.length-1;0<=x;x--)if(v[x].priority<=c)return v.splice(x+1,0,d),
{removeListener:g};
v.unshift(d)}return{removeListener:g}},once:function(){var a=Array.prototype.slice.call(arguments),b=a[1];a[1]=function(a)
{a.removeListener();return b.apply(this,arguments)};return this.on.apply(this,a)},capture:function()
{CKEDITOR.event.useCapture=1;var a=this.on.apply(this,arguments);CKEDITOR.event.useCapture=0;return a},fire:function(){var
a=0,e=function(){a=1},h=0,m=function(){h=1};return function(c,d,g){var n=f(this)[c];c=a;var v=h;a=h=0;if(n){var
x=n.listeners;if(x.length)for(var x=x.
...
...
...
```

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/core/assets/vendor/js-cookie/js.cookie.min.js
Entity:	/*! js-cookie v3.0.1 | MIT */ (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Difference:

Reasoning: AppScan found a reference to cookies in the JavaScript.

Test Requests and Responses:

```
GET /core/assets/vendor/js-cookie/js.cookie.min.js?v=3.0.1 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user-dashboard
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 21:13:56 GMT
Content-Type: application/javascript
Content-Length: 1681
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 20 Apr 2022 14:25:27 GMT
ETag: "691-5dd16c3c463c0"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 21:13:56 GMT
Vary: Accept-Encoding,User-Agent

/*! js-cookie v3.0.1 | MIT */
!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof
define&&define.amd?define(t):(e=e||self,function(){var n=e.Cookies,o=e.Cookies=t();o.noConflict=function(){return
e.Cookies=n,o}}())}(this,(function(){"use strict";function e(e){for(var t=1;t<arguments.length;t++){var
n=arguments[t];for(var o in n)e[o]=n[o]}return e}return function t(n,o){function r(t,r,i){if("undefined"!=typeof document)
{"number"==typeof(i=e({},o,i)).expires&&(i.expires=new Date(Date.now()+864e5*i.expires)),i.expires&&
(i.expires=i.expires.toUTCString()),t=encodeURIComponent(t).replace(/%
(2[346B]|5E|60|7C)/g,decodeURIComponent).replace(/[()]/g,escape);var c="";for(var u in i)i[u]&&(c+="; "+u,!0!==i[u]&&
(c+="="+i[u].split(";")[0]));return document.cookie=t+"="+n.write(r,t)+c}return Object.create({set:r,get:function(e)
{if("undefined"!=typeof document&&(!arguments.length||e)){for(var t=document.cookie?document.cookie.split("; "):[],o=
{},r=0;r<t.length;r++){var i=t[r].split("="),c=i.slice(1).join("=");try{var
u=decodeURIComponent(i[0]);if(o[u]=n.read(c,u),e===u)break}catch(e){}}return e?o[e]:o}},remove:function(t,n){r(t,"",e({},n,
{expires:-1}))},withAttributes:function(n){return t(this.converter,e({},this.attributes,n))},withConverter:function(n)
{return t(e({},this.converter,n),this.attributes)}},{attributes:{value:Object.freeze(o)},converter:
{value:Object.freeze(n)}})}({read:function(e){return'"'===e[0]&&(e=e.slice(1,-1)),e.replace(/(%[\dA-F]
{2})+/gi,decodeURIComponent)},write:function(e){return encodeURIComponent(e).replace(/%(2[346BF]|3[AC-
F]|40|5[BDE]|60|7[BCD])/g,decodeURIComponent)}},{path:"/"})));
```

Issue 1 of 1

TOC

Cookie with SameSite attribute not Restrictive

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/
Entity:	SSESSf6189c42141c46ed558989cd4da65b9e (Cookie)
Risk:	Prevent cookie information leakage by restricting cookies to first-party or same-site context to Strict.
Cause:	Sensitive Cookie with Unrestrictive SameSite Attributes and Flags
Fix:	Review possible solutions for configuring SameSite Cookie attribute to recommended values

Difference:

Reasoning: The response contains sensitive Cookie with unrestrictive SameSite attribute. If possible, it is advisable to configure the SameSite attribute to Strict. If not, the value "Lax" will suffice if you avoid using GET requests, and a good session management mechanism is in place to mitigate the risk of CSRF completely.

Test Requests and Responses:

```
GET /user-dashboard HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user/login
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:28:51 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
```

```
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<noscript><meta http-equiv="Refresh" content="0; URL=/big_pipe/no-js?destination=/user-dashboard" />
</noscript><meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" conten
...
...
...
```

I Email Address Pattern Found 10

TOC

Issue 1 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD
Entity:	Innovative-Mindset-Pilot-development-IMPD (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /Innovative-Mindset-Pilot-development-IMPD HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:21:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite
...
...
...

  <footer
    class="comment__meta">
          <p class="parent visually-hidden">In reply to <a href="/comment/360#comment-360" class="permalink" rel="bookmark"
hreflang="en">Laura I attended a great conference put on by JMG</a> by <a title="View user profile." href="/user/Perrin-
RREV-Coach-Chick-154" lang="" about="/user/Perrin-RREV-Coach-Chick-154" typeof="schema:Person" property="schema:name"
datatype="" content="pchick@mmsa.org" class="username">Perrin (RREV C…</a></p>
      </footer>
  <div class="user-comment-wrap">
    <div class="user-wrapper">
<div class="user-profile-picture">
...
```

```
...
...
```

Issue 2 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/Maine-DoE-163
Entity:	Maine-DoE-163 (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/Maine-DoE-163 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; Drupal-quicktabs-active-
tab-id-my_engine_landing_page=1


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:25:59 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
```

```
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<noscript><meta http-equiv="Refresh" content="0; URL=/big_pipe/no-js?destination=/user/mainedoe-mainedoe-163" />
</noscript><meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="Mobil
...
...
...

          <strong>Username:</strong>
          mainedoe mainedoe
          |
          <strong>Email:</strong>
          test@altoromutual.com
          </div>
          <p>Your
          <strong>name, role, school,</strong>
          and
...
...
...
```

Issue 3 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/group/69
Entity:	69 (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /group/69 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/group/69/filter?destination=group/69&topics=
```

```
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:23:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
Link: <https://stage.rrev-engine.com/Innovative-Mindset-Pilot-development-IMPD>; rel="canonical", <https://stage.rrev-
engine.com/group/69>; rel="shortlink"
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#
...
...
...

  <footer
    class="comment__meta">
          <p class="parent visually-hidden">In reply to <a href="/comment/360#comment-360" class="permalink" rel="bookmark"
hreflang="en">Laura I attended a great conference put on by JMG</a> by <a title="View user profile." href="/user/Perrin-
RREV-Coach-Chick-154" lang="" about="/user/Perrin-RREV-Coach-Chick-154" typeof="schema:Person" property="schema:name"
datatype="" content="pchick@mmsa.org" class="username">Perrin (RREV C…</a></p>
      </footer>
  <div class="user-comment-wrap">
    <div class="user-wrapper">
<div class="user-profile-picture">
...
...
...
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user
Entity:	user (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/comment/383
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; Drupal-quicktabs-active-
tab-id-my_engine_landing_page=1


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 20:04:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
```

```
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Upgrade: h2,h2c
Location: https://stage.rrev-engine.com/user/mainedoe-mainedoe-163
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="0;url='https://stage.rrev-engine.com/user/mainedoe-mainedoe-163'" />

        <title>Redirecting to https://stage.rrev-engine.com/user/mainedoe-mainedoe-163</title>
          <script type="text/javascript" src="/modules/contrib/seckit/js/seckit.document_write.js"></script>
        <link type="text/css" rel="stylesheet" id="seckit-clickjacking-no-body" media="all"
href="/modules/contrib/seckit/css/seckit.no_body.css" />
        <!-- stop SecKit protection -->
        <noscript>
        <link type="text/css" rel="stylesheet" id="seckit-clickjack
...
...
...

          <strong>Username:</strong>
          mainedoe mainedoe
          |
          <strong>Email:</strong>
          test@altoromutual.com
          </div>
          <p>Your
          <strong>name, role, school,</strong>
          and
...
...
...
```

Issue 5 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/163/edit
Entity:	edit (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/163/edit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/edit
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
```

```
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:26:35 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<noscript><meta http-equiv="Refresh" content="0; URL=/big_pipe/no-js?destination=/user/163/edit" />
</noscript><meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta
...
...
...

        <input autocomplete="off" data-drupal-selector="edit-mail" aria-describedby="edit-mail--description" type="email"
id="edit-mail" name="mail" value="test@altoromutual.com" size="60" maxlength="254" class="form-email required"
required="required" aria-required="true" />
...
...
...
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/edit
Entity:	edit (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/edit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/Maine-DoE-163
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 19:26:30 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Location: https://stage.rrev-engine.com/user/163/edit
Vary: Accept-Encoding,User-Agent
```

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="0;url='https://stage.rrev-engine.com/user/163/edit'" />

        <title>Redirecting to https://stage.rrev-engine.com/user/163/edit</title>
          <script type="text/javascript" src="/modules/contrib/seckit/js/seckit.document_write.js"></script>
        <link type="text/css" rel="stylesheet" id="seckit-clickjacking-no-body" media="all"
href="/modules/contrib/seckit/css/seckit.no_body.css" />
        <!-- stop SecKit protection -->
        <noscript>
        <link type="text/css" rel="stylesheet" id="seckit-clickjacking-noscript-tag" media="all"
href="/modules/contrib/seckit/css/seckit.noscript_tag.css" />
        <div id="seckit-noscript-tag">
          Sorry, you need to enable JavaScript to visit this website.
        </div>
        </n
...
...
...

        <input autocomplete="off" data-drupal-selector="edit-mail" aria-describedby="edit-mail--description" type="email"
id="edit-mail" name="mail" value="test@altoromutual.com" size="60" maxlength="254" class="form-email required"
required="required" aria-required="true" />
...
...
...
```

Issue 7 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/modules/contrib/extlink/extlink.js
Entity:	extlink.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /modules/contrib/extlink/extlink.js?v=9.3.12 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/Maine-DoE-163
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:36:47 GMT
Content-Type: application/javascript
Content-Length: 12177
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 14 Sep 2022 19:22:54 GMT
```

```
ETag: "2f91-5e8a80e341f80"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 19:36:47 GMT
Vary: Accept-Encoding,User-Agent

/**
 * @file
 * External links js file.
 */

(function ($, Drupal, drupalSettings) {

  'use strict';

  Drupal.extlink = Drupal.extlink || {};

  Drupal.extlink.attach = function (context, drupalSettings) {
    if (typeof drupalSettings.data === 'undefined' || !drupalSettings.data.hasOwnProperty('extlink')) {
      return;
    }

    // Define the jQuery method (either 'append' or 'prepend') of placing the
    // icon, defaults to 'append'.
    var extIconPlacement = 'append';
    if (drupalSettings.data.extlink.extIconPlacement && drupalSettings.data.extlink.extIconPlacement != '0') {
          extIconPlacement = drupalSettings.data.extlink.extIconPlacement;
        }

    // Strip the host name down, removing ports, subdomains, or www.
    var pattern = /^(([^\/:]+?\.)*)([^\.:]{1,})((\.[a-z0-9]{1,253})*)(:[0-9]{1,5})?$/;
    var host = window.location.host.replace(pattern, '$2$3$6');
    var subdomain = window.location.host.replace(host, '');

    // Determine what subdomains are considered internal.
    var subdomains;
    if (drupalSettings.data.extlink.extSubdomains) {
      subdomains = '([^/]*\\.)?';
    }
    else if (subdomain === 'www.' || subdomain === '') {
      subdomains = '(www\\.)?';
    }
    else {
      subdomains = subdomain.replace('.', '\\.');
    }

    // Whitelisted domains.
    var whitelistedDomains = false;
    if (drupalSettings.data.extlink.whitelistedDomains) {
      whitelistedDomains = [];
      for (var i = 0; i < drupalSettings.data.extlink.whitelistedDomains.length; i++) {
        whitelistedDomains.push(new RegExp('^https?:\\/\\/' +
drupalSettings.data.extlink.whitelistedDomains[i].replace(/(\r\n|\n|\r)/gm,'') + '.*$', 'i'));
      }
    }

    // Build regular expressions that define an internal link.
    var internal_link = new RegExp('^https?://([^@]*@)?' + subdomains + host, 'i');

    // Extra internal link matching.
    var extInclude = false;
    if (drupalSettings.data.extlink.extInclude) {
      extInclude = new RegExp(drupalSettings.data.extlink.extInclude.replace(/\\/, '\\'), 'i');
    }

    // Extra external link matching.
    var extExclude = false;
    if (drupalSettings.data.extlink.extExclude) {
      extExclude = new RegExp(drupalSettings.data.extlink.extExclude.replace(/\\/, '\\'), 'i');
    }

    // Extra external link CSS selector exclusion.
    var extCssExclude = false;
    if (drupalSettings.data.extlink.extCssExclude) {
      extCssExclude = drupalSettings.data.extlink.extCssExclude;
    }

    // Extra external link CSS selector explicit.
    var extCssExplicit = false;
    if (drupalSettings.data.extlink.extCssExplicit) {
      extCssExplicit = drupalSettings.data.extlink.extCssExplicit;
    }

    // Find all links which are NOT internal and begin with http as opposed
```

```
    // to ftp://, javascript:, etc. other kinds of links.
    // When operating on the 'this' variable, the host has been appended to
    // all links by the browser, even local ones.
    // In jQuery 1.1 and higher, we'd use a filter method here, but it is not
    // available in jQuery 1.0 (Drupal 5 default).
    var external_links = [];
    var mailto_links = [];
    $('a:not([data-extlink]), area:not([data-extlink])', context).each(function (el) {
      try {
        var url = '';
        if (typeof this.href == 'string') {
          url = this.href.toLowerCase();
        }
        // Handle SVG links (xlink:href).
        else if (typeof this.href == 'object') {
          url = this.href.baseVal;
        }
        if (url.indexOf('http') === 0
          && ((!internal_link.test(url) && !(extExclude && extExclude.test(url))) || (extInclude && extInclude.test(url)))
          && !(extCssExclude && $(this).is(extCssExclude))

...
...
...

        }
      }
      // IE7 throws errors often when dealing with irregular links, such as:
      // <a href="node/10"></a> Empty tags.
      // <a href="http://user:pass@example.com">example</a> User:pass syntax.
      catch (error) {
        return false;
      }
    });
...
...
...
```

Issue 8 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/password
Entity:	password (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/password HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://stage.rrev-engine.com/user/163/edit
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 19:52:20 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.ma
...
...
...

    <div id="block-cates-content" class="block block-system block-system-main-block">


      <form class="user-pass" data-drupal-selector="user-pass" action="/user/password" method="post" id="user-pass" accept-
charset="UTF-8">
  <p>Password reset instructions will be mailed to <em class="placeholder">test@altoromutual.com</em>. You must log out to
use the password reset link in the email.</p><input autocomplete="off" data-twig-suggestion="user-pass" data-drupal-
selector="form-47jz8co8r6iuymx-fsptdtesdaaduw9xul5dy2ccyuo" type="hidden" name="form_build_id" value="form-47JZ8CO8r6iuyMX-
FspTDTesDaAduw9XuL5dy2CcYuo" />
<input data-twig-suggestion="user-pass" data-drupal-selector="edit-user-pass-form-token" type="hidden" name="form_token"
value="aHdD2XF72ByGPt3C7irloi1c5NIH-7gaqGA-lAGp_Tw" />
<input data-twig-suggestion="user-pass" data-drupal-selector="edit-user-pass" type="hidden" name="form_id"
value="user_pass" />
<div data-twig-suggestion="user-pass" data-drupal-selector="edit-actions" class="form-actions js-form-wrapper form-wrapper"
id="edit-actions"><input data-twig-suggestion="user-pass" data-drupal-select
...
...
...
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/login
Entity:	login (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/login HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 302 Found
Date: Fri, 16 Sep 2022 20:04:09 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Upgrade: h2,h2c
Location: https://stage.rrev-engine.com/user/mainedoe-mainedoe-163
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html>
```

```
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh" content="0;url='https://stage.rrev-engine.com/user/mainedoe-mainedoe-163'" />

        <title>Redirecting to https://stage.rrev-engine.com/user/mainedoe-mainedoe-163</title>
          <script type="text/javascript" src="/modules/contrib/seckit/js/seckit.document_write.js"></script>
        <link type="text/css" rel="stylesheet" id="seckit-clickjacking-no-body" media="all"
href="/modules/contrib/seckit/css/seckit.no_body.css" />
        <!-- stop SecKit protection -->
        <noscript>
        <link type="text/css" rel="stylesheet" id="seckit-clickjacking-noscript-tag" media="all"
href="/modules/contrib/seckit/css/seckit.noscript_tag.css" />
        <div id="seckit-noscript-tag">
          Sorry, you need to enable JavaScript to visit this website.
        </div>
        </noscript></head>
    <body>
        Redirecting to <a href="https://stage.rrev-engin
...
...
...

          <strong>Username:</strong>
          mainedoe mainedoe
          |
          <strong>Email:</strong>
          test@altoromutual.com
          </div>
          <p>Your
          <strong>name, role, school,</strong>
          and
...
...
...
```

Issue 10 of 10

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/user/mainedoe-mainedoe-163
Entity:	mainedoe-mainedoe-163 (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /user/mainedoe-mainedoe-163 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/user/login
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 20:04:11 GMT
```

```
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: must-revalidate, no-cache, private
X-Drupal-Dynamic-Cache: UNCACHEABLE
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
Expires: Sun, 19 Nov 1978 05:00:00 GMT
X-Generator: Drupal 9 (https://www.drupal.org)
Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-Content-Security-Policy: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-WebKit-CSP: default-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com *.google-
analytics.com *.googletagmanager.com *.rrev-engine.com 8x8.vc; script-src 'self'  'unsafe-inline' *.gstatic.com
*.googleapis.com *.googletagmanager.com 8x8.vc *.google-analytics.com *.google.com *.rrev-engine.com *.maine.gov; style-src
'self' 'unsafe-inline' *.googleapis.com *.rrev-engine.com *.maine.gov 8x8.vc; img-src *; media-src  'self'; frame-src
'self' *.googletagmanager.com *.google.com 8x8.vc; child-src 'self' *.googleapis.com *.gstatic.com; font-src 'self'
*.googleapis.com *.gstatic.com; connect-src 'self' 'unsafe-inline' *.google.com *.maine.gov *.googleapis.com *.gstatic.com
*.google-analytics.com *.googletagmanager.com wss://*.rrev-engine.com *.rrev-engine.com wss://*.maine.gov 8x8.vc; report-
uri /report-csp-violation
X-XSS-Protection: 1
Strict-Transport-Security: max-age=2592000
From-Origin: same
Referrer-Policy: strict-origin-when-cross-origin
Expect-CT: max-age=86400
Surrogate-Control: no-store, content="BigPipe/1.0"
X-Accel-Buffering: no
Vary: Accept-Encoding,User-Agent
Set-Cookie: SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv; path=/;
domain=.stage.rrev-engine.com; secure; HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<noscript><meta http-equiv="Refresh" content="0; URL=/big_pipe/no-js?destination=/user/mainedoe-mainedoe-163" />
</noscript><meta name="Generator" content="Drupal 9 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="
...
...
...

          <strong>Username:</strong>
          mainedoe mainedoe
          |
          <strong>Email:</strong>
          test@altoromutual.com
          </div>
          <p>Your
          <strong>name, role, school,</strong>
          and
...
...
...
```

I Integer Overflow 1 TOC

Issue 1 of 1 TOC

Integer Overflow

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/whiteboard
Entity:	whiteboardid (Parameter)
Risk:	It is possible to gather sensitive debugging information
Cause:	An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Difference: **Parameter** `whiteboardid` manipulated from: `79` to: `99999999999999999999`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
GET /whiteboard?whiteboardid=99999999999999999999&username=mainedoe_mainedoe HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://stage.rrev-engine.com/room/Drag-and-Drop-test-room-79?sort_by=title&sort_order=DESC
Host: stage.rrev-engine.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; SSESSf6189c42141c46ed558989cd4da65b9e=oJdAInR-
06djhaL601gjtG%2CXzohpt7gpbcYF4fOK0ARb6hXv


HTTP/1.1 500 500 Service unavailable (with message)
Date: Mon, 19 Sep 2022 16:59:55 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
Cache-Control: no-cache, private
X-Content-Type-Options: nosniff
Upgrade: h2,h2c
Vary: Accept-Encoding,User-Agent

The website encountered an unexpected error. Please try again later.<br />
```

I Missing "Referrer policy" Security Header 1 TOC

Issue 1 of 1 TOC

Missing "Referrer policy" Security Header

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/
Entity:	stage.rrev-engine.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Referrer Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Referrer Policy Response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /modules/contrib/seckit/js/seckit.document_write.js HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/login
Content-Length: 0


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 18:55:10 GMT
Content-Type: application/javascript
Content-Length: 221
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 14 Sep 2022 19:22:54 GMT
ETag: "dd-5e8a80e341f80"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 18:55:10 GMT
Vary: Accept-Encoding,User-Agent

/**
 * If site is not being framed or being framed within the same host,
 * start commenting out seckit.no_body.css.
 */
if (top === self || top.location.hostname === self.location.hostname) {
  document.write('<!--');
}
```

I Possible Server Path Disclosure Pattern Found 1

TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://stage.rrev-engine.com/core/modules/file/file.js
Entity:	file.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Difference:

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Test Requests and Responses:

```
GET /core/modules/file/file.js?v=9.3.12 HTTP/1.1
Host: stage.rrev-engine.com
Connection: keep-alive
sec-ch-ua: "Chromium";v="100"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://stage.rrev-engine.com/user/163/edit
Cookie: Drupal-quicktabs-active-tab-id-my_engine_landing_page=1; Drupal-quicktabs-active-tab-id-resourced_tab=1;
SSESSf6189c42141c46ed558989cd4da65b9e=78rRmarXieanPQZqOFDiVYh2vSefuxC6RsWgNwbV0N%2CLyKRr


HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 21:48:22 GMT
Content-Type: application/javascript
Content-Length: 5437
Connection: keep-alive
Server: Apache/2.4.54 () OpenSSL/1.0.2k-fips
X-Content-Type-Options: nosniff
Last-Modified: Wed, 20 Apr 2022 14:25:27 GMT
ETag: "153d-5dd16c3c463c0"
Accept-Ranges: bytes
Cache-Control: max-age=1209600
Expires: Fri, 30 Sep 2022 21:48:22 GMT
Vary: Accept-Encoding,User-Agent

/**
* DO NOT EDIT THIS FILE.
* See the following change record for more information,
* https://www.drupal.org/node/2815083
* @preserve
**/

(function ($, Drupal) {
  Drupal.behaviors.fileValidateAutoAttach = {
    attach: function attach(context, settings) {
      var $context = $(context);
      var elements;

      function initFileValidation(selector) {
        $(once('fileValidate', $context.find(selector))).on('change.fileValidate', {
          extensions: elements[selector]
        }, Drupal.file.validateExtension);
      }

      if (settings.file && settings.file.elements) {
        elements = settings.file.elements;
```

```
        Object.keys(elements).forEach(initFileValidation);
      }
    },
    detach: function detach(context, settings, trigger) {
      var $context = $(context);
      var elements;

      function removeFileValidation(selector) {
        $(once.remove('fileValidate', $context.find(selector))).off('change.fileValidate', Drupal.file.validateExtension);
      }

      if (trigger === 'unload' && settings.file && settings.file.elements) {
        elements = settings.file.elements;
        Object.keys(elements).forEach(removeFileValidation);
      }
    }
  };
  Drupal.behaviors.fileAutoUpload = {
    attach: function attach(context) {
      $(once('auto-file-upload', 'input[type="file"]', context)).on('change.autoFileUpload',
Drupal.file.triggerUploadButton);
    },
    detach: function detach(context, settings, trigger) {
      if (trigger === 'unload') {
        $(once.remove('auto-file-upload', 'input[type="file"]', context)).off('.autoFileUpload');
      }
    }
  };
  Drupal.behaviors.fileButtons = {
    attach: function attach(context) {
      var $context = $(context);
      $context.find('.js-form-submit').on('mousedown', Drupal.file.disableFields);
      $context.find('.js-form-managed-file .js-form-submit').on('mousedown', Drupal.file.progressBar);
    },
    detach: function detach(context, settings, trigger) {
      if (trigger === 'unload') {
        var $context = $(context);
        $context.find('.js-form-submit').off('mousedown', Drupal.file.disableFields);
        $context.find('.js-form-managed-file .js-form-submit').off('mousedown', Drupal.file.progressBar);
      }
    }
  };
  Drupal.behaviors.filePreviewLinks = {
    attach: function attach(context) {
      $(context).find('div.js-form-managed-file .file a').on('click', Drupal.file.openInNewWindow);
    },
    detach: function detach(context) {
      $(context).find('div.js-form-managed-file .file a').off('click', Drupal.file.openInNewWindow);
    }
  };
  Drupal.file = Drupal.file || {
    validateExtension: function validateExtension(event) {
      event.preventDefault();
      $('.file-upload-js-error').remove();
      var extensionPattern = event.data.extensions.replace(/,\s*/g, '|');

      if (extensionPattern.length > 1 && this.value.length > 0) {
        var acceptableMatch = new RegExp("\\.(".concat(extensionPattern, ")$"), 'gi');

        if (!acceptableMatch.test(this.value)) {
          var error = Drupal.t('The selected file %filename cannot be uploaded. Only files with the following extensions
are allowed: %extensions.', {
          '%filename': this.value.replace('C:\\fakepath\\', ''),
          '%extensions': extensionPattern.replace(/\|/g, ', ')
          });
          $(this).closest('div.js-form-managed-file').prepend("<div class=\"messages messages--error file-upload-js-error\"
aria-live=\"polite\">".concat(error, "</div>"));
          this.value = '';
          event.stopImmediatePropagation();
        }
      }
    },
    triggerUploadButton: function triggerUploadButton(event) {
      $(event.target).closest('.js-form-managed-file').find('.js-form-submit[data-drupal-selector$="upload-
button"]').trigger('mousedown');
    },
    disableFields: function disableF
...
...
...
```

How to Fix

Check for SRI (Subresource Integrity) support

TOC

Cause:

There is no support to Subresource Integrity.

Risk:

The user-agent can't verify scripts from third-party services. In case of compromise of the third-party service, the user is not protected.
script and link tags with src from another domain are not supporting integrity check.
This can be exploited if the service that have the script is compromise.
Sample Script Element Not Supporting SRI:
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
Sample Script Element Supporting SRI:
<script src="https://example.com/example-framework.js" integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7" crossorigin="anonymous"></script>

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Add Subresource Integrity to every script/link with source not in your domain
W3C Subresource Integrity:
https://www.w3.org/TR/SRI/
SRI Hash Generator:
https://srihash.org
Sample Script Element Not Supporting SRI:
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
Sample Script Element Supporting SRI:
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

CWE:

829

External References:

Vendor site
Explanation

Hidden Directory Detected

TOC

Cause:

The web server or application server are configured in an insecure way

Risk:

It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
The web application has exposed the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it, or sub directories under it, and try to access them.
The more sensitive the content is, the more severe this issue may be.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

If the forbidden resource is not required, remove it from the site.
If possible, issue a "404 - Not Found" response status code instead of "403 - Forbidden". This change will obfuscate the presence of the directory in the site, and will prevent the site structure from being exposed.

CWE:

200

Unnecessary Http Response Headers found in the Application

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web server type, version, OS and more.
AppScan detected a Http response header that is unnecessary.
For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.
The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.
The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.
These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Configure your server to remove the default "Server" header from being sent to all outgoing requests.
For IIS, see:
Set IIS response headers
For nginx, see:
Set nginx response headers
For Weblogic, see:
Set Weblogic response headers
For Apache, see:
Set Apache response headers

CWE:

200

External References:

Fingerprinting
Preventing Information Leakage

Unsafe third-party link (target="_blank")

TOC

Cause:

The rel attribute in the link element is not set to "noopener noreferrer".

Risk:

The linked page gains partial access to the opening page window object.
The target="_blank" attribute is added to link elements to make the link open in a new window.
link tags of this kind(i.e. with target="_blank" attribute) expose parts of the window object of the original page to the linked page via window.opener object.
This can be exploited for phishing attacks if the linked page is malicious.
Attention: if links can be added by users and propogate to pages visable by other users this threat should be treated as HIGH severity

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Add rel="noopener noreferrer" to every link tag with source not in your domain
More detailed fix recomendation can be found in the Advisory's References and Relevant Links

External References:

The most underestimated vulnerability ever - Explanation, example and fix recomendation

Missing "Content-Security-Policy" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of CSP can cause the web application being vulnerable to XSS, clickjacking, etc.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:
Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.
For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header.
It is recommended to configure Content-Security-Policy header with secure values for its directives as below:
For 'default-src', 'script-src' and 'object-src', secure values such as 'none', 'self', https://any.example.com.
For 'frame-ancestors', secure values such as 'self', 'none' or https://any.example.com were expected.
"unsafe-inline" and "unsafe-eval" must not be used in any circumstance. Using nonce / hash would be only considered for short-term workaround.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

1032

External References:

List of some secure Headers
An Introduction to Content Security Policy
MDN web docs - Content-Security-Policy

Missing or Insecure "Object-Src" policy in "Content-Security-Policy" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of object-src directive(CSP) can cause the web application being vulnerable to cross-site scripting, cross-site framing and more.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site.
The object-src directive restricts the URLs from which plugin content may be loaded. To protect against cross-site-scripting(XSS), it is important to set the policies with proper values as shown below:
For 'object-src', insecure values such as '*', 'data:', 'http:', 'https:', 'ws:', 'wss:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
If object-src directive is not set explicitly, Consider having default-src which acts as a fallback for many directives including object-src.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header with proper values for "object-src" directive
It is recommended to configure object-src directive with secure values such as 'self' or 'none' and if needed, you should use 'unsafe-inline' or 'unsafe-eval' with nonce or hash-algorithm
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

External References:

List of some useful secure Headers
An Introduction to Content Security Policy
MDN web docs - CSP: object-src

Missing or Insecure "Script-Src" policy in "Content-Security-Policy" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of script-src directive(CSP) can cause the web application being vulnerable to cross-site scripting, cross-site framing and more.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
The script-src directive restricts the locations from which scripts may be executed. This includes not only URLs loaded directly into script elements, but also things like inline script blocks and XSLT stylesheets [XSLT] which can trigger script execution.
To protect against cross-site-scripting(XSS), it is important to set the policies with proper values:
For 'script-src', insecure values such as '*', 'data:', 'http:', 'https:', 'ws:', 'wss:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
If script-src directive is not set explicitly, Consider having default-src which acts as a fallback for many directives including script-src.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header with proper values for "script-src" directive
It is recommended to configure script-src directive with secure values such as 'self' or 'none' and if needed, you should use 'unsafe-inline' or 'unsafe-eval' with nonce or hash-algorithm
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

External References:

List of some useful secure Headers
An Introduction to Content Security Policy
MDN web docs - CSP: script-src

Missing or Insecure "Style-Src" policy in "Content-Security-Policy"

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of style-src directive(CSP) can cause the web application to be vulnerable to cross-site scripting more.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
The "style-src" Content Security Policy (CSP) directive guards the loading and execution of CSS styles and stylesheets.
To protect against cross-site-scripting(XSS), it is important to set the policies with proper values:
For 'style-src', insecure values such as '*', 'data:', 'http:', 'https:', 'ws:', 'wss:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
If style-src directive is not set explicitly, Consider having default-src which acts as a fallback for many directives including script-src.
Please refer the following links for more information.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header with proper values for "style-src" directive
It is recommended to configure style-src directive with secure values such as 'self' or 'none' and if needed, you should use 'unsafe-inline' or 'unsafe-eval' with nonce or hash-algorithm
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

External References:

List of some useful secure Headers
An Introduction to Content Security Policy
MDN web docs - CSP: style-src

Missing or insecure HTTP Strict-Transport-Security Header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.
It is important to set the 'max-age' to a high enough value to prevent falling back to an insecure connection prematurely.
The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.
For more information please see
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

CWE:

200

External References:

OWASP "HTTP Strict Transport Security"
HSTS Spec

Application Error

TOC

Cause:

- Proper bounds checking were not performed on incoming parameter values
- No validation was done in order to make sure that user input matches the data type expected

Risk:

It is possible to gather sensitive debugging information
If an attacker probes the application by forging a request that contains parameters or parameter values other than the ones expected by the application (examples are listed below), the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request, which information may be exploited to locate application weaknesses.
For example, if the parameter field should be an apostrophe-quoted string (e.g. in an ASP script or SQL query), the injected apostrophe symbol will prematurely terminate the string stream, thus changing the normal flow/syntax of the script.
Another cause of vital information being revealed in error messages, is when the scripting engine, web server, or database are misconfigured.
Here are some different variants:
[1] Remove parameter
[2] Remove parameter value
[3] Set parameter value to null
[4] Set parameter value to a numeric overflow (+/- 99999999)
[5] Set parameter value to hazardous characters, such as ' " \' \") ;
[6] Append some string to a numeric parameter value
[7] Append "." (dot) or "[]" (angle brackets) to the parameter name

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

[1] Check incoming requests for the presence of all expected parameters and values. When a parameter is missing, issue a proper error message or use default values.
[2] The application should verify that its input consists of valid characters (after decoding). For example, an input value containing the null byte (encoded as %00), apostrophe, quotes, etc. should be rejected.
[3] Enforce values in their expected ranges and types. If your application expects a certain parameter to have a value from a certain set, then the application should ensure that the value it receives indeed belongs to the set. For example, if your application expects a value in the range 10..99, then it should make sure that the value is indeed numeric, and that its value is in 10..99.
[4] Verify that the data belongs to the set offered to the client.
[5] Do not output debugging error messages and exceptions in a production environment.
In order to disable debugging in ASP.NET, edit your web.config file to contain the following:
<compilation
debug="false"
/>
For more information, see "HOW TO: Disable Debugging for ASP.NET Applications" in:
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157
You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, testing for valid dates or values within a range), plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.
To make sure that all the required parameters exist in a request, use the "RequiredFieldValidator" validation control. This control ensures that the user does not skip an entry in the web form.
To make sure user input contains only valid values, you can use one of the following validation controls:
[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.
[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.
Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions. There are two ways to check for user input validity:
1. Test for a general error state:
In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.
2. Test for the error state of individual controls:
Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.
** Input Data Validation:
While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.
A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response
A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.
[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.
Example of how to validate required fields:
// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }
[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.
Example of how to validate a numeric field (type int):

// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }

A good practice is to convert all HTTP request parameters to their respective data types. For example, store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...

The primary Java data types that the application should handle:

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength) { String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength && validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if (Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >= min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if (Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) { // numberOfChoices is valid, continue processing request ... } } }

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options, Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch (Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"); // Verify that the user selection is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) { // valid user selection, continue processing request ... }

[6] Field pattern

Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support.

Example to perform regular expression validation:

// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); } return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import java.util.regex.Pattern; import java.util.regexe.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }

[7] Cookie value

Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies = request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { //

validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }
[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +
Example to filter a specified string by converting sensitive characters to their corresponding character entities:
// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null) { return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<': result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case '\'': result.append("'"); break; case '%': result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&': result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } ... // Filter the HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response)); out.close();
The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.
Example of using a Servlet Filter to sanitize the response using Validator.filter:
// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter(); ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw = new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html"); response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){ return new PrintWriter(output); } } } }
[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.
Example to secure the "user" cookie:
// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user", "sensitive"); cookie.setSecure(true); response.addCookie(cookie);
RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.
Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.
Example to validate the userName field of a loginForm using Struts Validator:
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.
The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component
The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance

output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message
Example to validate the userName field of a loginForm using JavaServer Faces:
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /><p> </h:form> </f:use_faces>
REFERENCES
Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/
** Error Handling:
Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.
While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:
[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping
[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:
(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;
A good practice is to define the following framework Java classes which are used to store and report application errors:
- ErrorKeys: defines all error keys
// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // - ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }
- Error: encapsulates an individual error

// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private Object[] values = null; }
- Errors: encapsulates a Collection of errors
// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors = (ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); } propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new HashMap(); }
Using the above framework classes, here is an example to process validation errors of the "user_name" field:
// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName = request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE); } } // set the errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...
[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism
[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception
It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):
// Example to forward to the userInput.jsp following user validation errors RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }
If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.
Example to return a HTTP error:
// Example to return a HTTP error code RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) { // messages is a resource bundle with all message keys and values response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR, messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }
As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException
[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:
<%@ page errorPage="/errors/userValidation.jsp" %>
Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:
<%@ page isErrorPage="true" %>
The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.
[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:
(a) Resource Bundles
(b) Message Formatting
[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.
It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:
ErrorMessages.properties

required user name error message error.username.required=User name field is required # invalid user name format error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message error.username.duplicate=User name {0} already exists, please choose another one ...
Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.
[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:
// Example to show how to format a message using placeholder parameters String pattern = "User name {0} already exists, please choose another one"; String userName = request.getParameter("user_name"); Object[] args = new Object[1]; args[0] = userName; String message = MessageFormat.format(pattern, args);
Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:
// Example to render an error message from a localized ErrorMessages resource (properties file) // Utility class to retrieve locale-specific error messages public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale Locale userLocale = request.getLocale(); // Check if there were any validation errors Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage + "\r\n"); } }
It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.
[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:
<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-code>500</exception-type> <location>/errors/internalError.html</error-page> </error-page> <error-page> ... </error-page> ...
RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.
Example to validate the userName field of a loginForm using Struts Validator:
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:
<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right"> <html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username" size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right"> <html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>
[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.
The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.
Example to validate the userName field of a loginForm using JavaServer Faces:
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20"

modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /><p> </h:form> </f:use_faces>
REFERENCES
Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/
** Input Data Validation:
While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.
A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response
A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.
[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.
Example of how to validate required fields:
// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0){ $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }
[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.
[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.
[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.
[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.
[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$
[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.
[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +
PHP includes some automatic sanitization utility functions, such as htmlentities():
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:
<?php header('Content-Type: text/html; charset=UTF-8'); ?>
[8-2] Secure the cookie
When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP

response. This will instruct the browser to only use that cookie over SSL connections.
You can use the following code example, for securing the cookie:
<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>
In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).
The HttpOnly flag was Added in PHP 5.2.0.
REFERENCES
[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

CWE:

550

External References:

An example for using apostrophe to hack a site can be found in "How I hacked PacketStorm (by Rain Forest Puppy), RFP's site"
"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
CERT Advisory (CA-1997-25): Sanitizing user-supplied data in CGI scripts

Client-Side (JavaScript) Cookie References

TOC

Cause:

Cookies are created at the client side

Risk:

The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
A cookie is a piece of information usually created by the Web server and stored in the Web browser.
The cookie contains information used by web applications mainly (but not only) to identify users and maintain their state.
AppScan detected that the JavaScript code at the client side is used to manipulate (either create or modify) the site's cookies.
It is possible for an attacker to view this code, understand its logic, and use it to compose his own cookies, or modify existing ones, based on this knowledge.
The damage an attacker may cause depends on how the application uses its cookies, or what information it stores in them.
Among other things, cookie manipulation may lead to session hijacking or privilege escalation.
Other vulnerabilities caused by cookie poisoning contain SQL injection and Cross-Site scripting.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

[1] Avoid placing business/security logic at the client side.
[2] Find and remove insecure client-side Javascript code which may pose a security threat to the site.

CWE:

602

External References:

WASC Threat Classification: Information Leakage

Cookie with SameSite attribute not Restrictive

TOC

Cause:

Sensitive Cookie with Unrestrictive SameSite Attributes and Flags

Risk:

Prevent Cookie information leakage by restricting cookies to first-party or same-site context as Strict
Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
The SameSite attribute controls how cookies are sent for cross-domain requests.
* Strict mode is recommended, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.
* Setting SameSite attribute to 'Strict' will only be sent in a first-party context and not be sent along with requests initiated by third party websites.
* Example - Set-Cookie: key=value; SameSite=Strict

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

[1] Restrict Cookies to a first-party context.
[2] Verify and set the SameSite attribute of the cookie to Strict, to ensure that the cookie will only be sent in a first-party context.
[3] The value "Lax" will suffice if you avoid using GET requests, and a good session management mechanism is in place to mitigate the risk of CSRF completely.

CWE:

1275

External References:

WASC Threat Classification: Information Leakage
SameSite Cookies

Email Address Pattern Found

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).
AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail
Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

CWE:

359

External References:

Definition of Spambot (Wikipedia)

Integer Overflow

TOC

Cause:

An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).

Risk:

When an integer overflow occurs, the interpreted value will appear to have 'wrapped around' past the maximum value and reset back to the minimum value.
The value can unexpectedly become zero or negative. This can have security implications if the value is used to control looping, manage resources (such as memory allocation), or make business logic decisions.
For example, an integer overflow can give money to the customer in addition to their purchases, when the transaction is completed.
In particular, if a mathematical operation results in a number larger than the maximum possible for the integer type, the value wraps around and the variable is set to zero, or negative.
i=UINT_MAX+1; // Maximum value for a variable of type unsigned int - 4294967295 (0xffffffff). The result is: i=0

Fix Recommendation:

General

Validate all inputs are within an expected range and the sign before relying on their values or using them in arithmetic calculations.
Be sure to check both upper bounds and lower bounds, including negative lower bounds for signed integers (integer overflow is also possible with very large negative numbers).
Use unsigned integers where possible.
Consider using a safe integer-handling library (such as C/C++ SafeInt or IntegerLib).
Consider enabling compiler extensions that prevent some classes of buffer overflows.

CWE:

190

External References:

SafeInt Library

Missing "Referrer policy" Security Header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of Referrer Policy can cause URL leak itself, and even sensitive information contained in the URL will be leaked to the cross-site.
This is a part of ruleset to check if Referrer Policy is present and if so to test its configuration. The "Referer Policy" header defines what data is made available in the Referer header, and for navigation and iframes in the destination's (document.referrer). This header is designed to modify the way browsers render pages, and thus to prevent cross-domain Referer leakage. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site.
Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.
"no-referrer-when-downgrade" and "unsafe-url" are the policies which leaks the Full Url for the ThirdParty Sites. The remaining policies are"no-referrer", "origin", "origin-when-cross-origin","same-origin", "strict-origin", "strict-origin-when-cross-origin.
Please refer the following links for more information.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Referrer Policy" header.
It is recommended to configure Referrer Policy header with secure values for its directives as below:
"strict-origin-when-cross-origin" offers more privacy. With this policy, only the origin is sent in the Referer header of cross-origin requests.
For Google Chrome, see:
https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
For Firefox , see:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.

CWE:

200

External References:

MDN web docs - Referrer-Policy

Possible Server Path Disclosure Pattern Found

TOC

Cause:

Latest patches or hotfixes for 3rd. party products were not installed

Risk:

It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
AppScan detected a response containing a file's absolute path (e.g. c:\dir\file in Windows, or /dir/file in Unix).
An attacker may be able to exploit this information to access sensitive information on the directory structure of the server machine which could be used for further attacks against the site.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

There are several mitigation techniques:
[1] In case the vulnerability is in the application itself, fix the server code so it doesn't include file locations in any output.
[2] Otherwise, if the application is in a 3rd party product, download the relevant security patch depending on the 3rd party product you are using on your web server or web application.

CWE:

200

Application Data

Failed Requests 18

TOC

URL	Reason
https://stage.rrev-engine.com/user/%5Bcurrent-user%3Auid%5D/settings	Response Status '404' - Not Found
https://stage.rrev-engine.com/user/register	Response Status '403' - Forbidden
https://stage.rrev-engine.com/user/%5Bcurrent-user%3Auid%5D/settings	Response Status '404' - Not Found
https://stage.rrev-engine.com/user/%5Bcurrent-user%3Auid%5D/settings	Response Status '404' - Not Found
https://stage.rrev-engine.com/group/64/join	Response Status '403' - Forbidden
https://stage.rrev-engine.com/group/66/join	Response Status '403' - Forbidden
https://stage.rrev-engine.com/user/register	Response Status '403' - Forbidden
https://stage.rrev-engine.com/group/69/join	Response Status '403' - Forbidden
https://stage.rrev-engine.com/group/68/join	Response Status '403' - Forbidden
https://stage.rrev-engine.com/core/modules/views/js/Drupal.Views.pathPortion(href);	Response Status '404' - Not Found
https://stage.rrev-engine.com/core/assets/vendor/ckeditor/styles.js	Response Status '404' - Not Found
https://stage.rrev-engine.com/user/current/	Response Status '403' - Forbidden
https://stage.rrev-engine.com/batch/?v=1.0.1	Response Status '403' - Forbidden
https://stage.rrev-engine.com/modules/?v=1.0.1	Response Status '403' - Forbidden
https://stage.rrev-engine.com/sites/?v=1.0.1	Response Status '403' - Forbidden
https://stage.rrev-engine.com/admin/?v=1.0.1	Response Status '403' - Forbidden
https://stage.rrev-engine.com/themes/?v=1.0.1	Response Status '403' - Forbidden
https://stage.rrev-engine.com/libraries/?v=1.0.1	Response Status '403' - Forbidden