

ZAP by Checkmarx

Scanning Report

Generated with  ZAP on Thu 10 Jul 2025, at 12:58:54

ZAP Version: 2.16.1

ZAP by [Checkmarx](#)

Contents

- [About This Report](#)
 - [Report Parameters](#)
- [Summaries](#)
 - [Alert Counts by Risk and Confidence](#)
 - [Alert Counts by Site and Risk](#)
 - [Alert Counts by Alert Type](#)
- [Alerts](#)
 - [Risk=High, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)

- [Risk=Low, Confidence=Medium \(1\)](#)
- [Risk=Low, Confidence=Low \(1\)](#)
- [Risk=Informational, Confidence=Medium \(2\)](#)
- [Risk=Informational, Confidence=Low \(1\)](#)
- [Appendix](#)
 - [Alert Types](#)

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://firefox-settings-attachments.cdn.mozilla.net`
- `http://localhost:8082`

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: [High](#), [Medium](#), [Low](#), [Informational](#)

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (11.1%)	0 (0.0%)	0 (0.0%)	1 (11.1%)
	Medium	0 (0.0%)	1 (11.1%)	1 (11.1%)	0 (0.0%)	2 (22.2%)
	Low	0 (0.0%)	1 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	2 (22.2%)	1 (11.1%)	3 (33.3%)
	Total	0 (0.0%)	3 (33.3%)	4 (44.4%)	2 (22.2%)	9 (100%)

Alert Counts by Site and Risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

		Risk			
Site		Medium		Informational	
		High (= High)	(>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://firefox-settings-attachments.cdn.mozilla.net	0 (0)	0 (0)	2 (2)	2 (4)
	http://localhost:8082	1 (1)	2 (3)	1 (4)	1 (5)

Alert Counts by Alert Type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cross Site Scripting (DOM Based)	High	2 (22.2%)
Total		9

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	1 (11.1%)
Missing Anti-clickjacking Header	Medium	1 (11.1%)
Strict-Transport-Security Header Not Set	Low	2 (22.2%)
Timestamp Disclosure - Unix	Low	2 (22.2%)
X-Content-Type-Options Header Missing	Low	4 (44.4%)
Modern Web Application	Informational	1 (11.1%)
Re-examine Cache-control Directives	Informational	2 (22.2%)
Retrieved from Cache	Informational	4 (44.4%)
Total		9

Alerts

Risk=High, Confidence=High (1)

[http://localhost:8082 \(1\)](#)

[Cross Site Scripting \(DOM Based\) \(1\)](#)

► GET http://localhost:8082/xss.html?name=abc#

Risk=Medium, Confidence=High (1)

http://localhost:8082 (1)

Content Security Policy (CSP) Header Not Set (1)

► GET http://localhost:8082/xss.html

Risk=Medium, Confidence=Medium (1)

http://localhost:8082 (1)

Missing Anti-clickjacking Header (1)

► GET http://localhost:8082/xss.html

Risk=Low, Confidence=High (1)

https://firefox-settings-attachments.cdn.mozilla.net (1)

Strict-Transport-Security Header Not Set (1)

► GET https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ffc59054-61a2-437e-aa8b-67299d879fd8

Risk=Low, Confidence=Medium (1)

<http://localhost:8082> (1)

X-Content-Type-Options Header Missing (1)

► GET <http://localhost:8082/xss.html>

Risk=Low, Confidence=Low (1)

<https://firefox-settings-attachments.cdn.mozilla.net> (1)

Timestamp Disclosure - Unix (1)

► GET <https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ffc59054-61a2-437e-aa8b-67299d879fd8>

Risk=Informational, Confidence=Medium (2)

<https://firefox-settings-attachments.cdn.mozilla.net> (1)

Retrieved from Cache (1)

► GET <https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ffc59054-61a2-437e-aa8b-67299d879fd8>

<http://localhost:8082> (1)

Modern Web Application (1)

► GET <http://localhost:8082/xss.html>

Risk=Informational, Confidence=Low (1)**<https://firefox-settings-attachments.cdn.mozilla.net> (1)****Re-examine Cache-control Directives (1)**

► GET <https://firefox-settings-attachments.cdn.mozilla.net/main-workspace/tracking-protection-lists/ffc59054-61a2-437e-aa8b-67299d879fd8>

Appendix

Alert Types

This section contains additional information on the types of alerts in the report.

Cross Site Scripting (DOM Based)

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	<ul style="list-style-type: none">▪ https://owasp.org/www-community/attacks/xss/▪ https://cwe.mitre.org/data/definitions/79.html

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html▪ https://www.w3.org/TR/CSP/▪ https://w3c.github.io/webappsec-csp/▪ https://web.dev/articles/csp▪ https://caniuse.com/#feat=contentsecuritypolicy▪ https://content-security-policy.com/

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html▪ https://owasp.org/www-community/Security-Headers▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security▪ https://caniuse.com/stricttransportsecurity▪ https://datatracker.ietf.org/doc/html/rfc6797

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	<ul style="list-style-type: none">▪ https://cwe.mitre.org/data/definitions/200.html

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)▪ https://owasp.org/www-community/Security-Headers

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)
--------	--

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	<ul style="list-style-type: none">▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

- <https://grayduck.mn/2021/09/13/cache-control-recommendations/>

Retrieved from Cache

Source

raised by a passive scanner ([Retrieved from Cache](#))

Reference

- <https://tools.ietf.org/html/rfc7234>
- <https://tools.ietf.org/html/rfc7231>
- <https://www.rfc-editor.org/rfc/rfc9110.html>