


ZAP by Checkmarx

Scanning Report

Generated with  ZAP on Tue 1 Jul 2025, at 12:54:14

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=Medium, Confidence=High \(5\)](#)
 - [Risk=Low, Confidence=High \(1\)](#)
 - [Risk=Low, Confidence=Medium \(4\)](#)
 - [Risk=Informational, Confidence=High \(1\)](#)
 - [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:

- <http://127.0.0.1:5173>
- <http://127.0.0.1:8000>

(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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	5 (35.7%)	0 (0.0%)	0 (0.0%)	5 (35.7%)
	Low	0 (0.0%)	1 (7.1%)	4 (28.6%)	0 (0.0%)	5 (35.7%)
	Informational	0 (0.0%)	1 (7.1%)	2 (14.3%)	1 (7.1%)	4 (28.6%)
	Total	0 (0.0%)	7 (50.0%)	6 (42.9%)	1 (7.1%)	14 (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			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site http://127.0.0.1:5173	0 (0)	0 (0)	1 (1)	1 (2)
http://127.0.0.1:8000	0 (0)	5 (5)	4 (9)	3 (12)

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
CSP: Wildcard Directive	Medium	4 (28.6%)
CSP: script-src unsafe-eval	Medium	4 (28.6%)
Total		14

Alert type	Risk	Count
CSP: script-src unsafe-inline	Medium	4 (28.6%)
CSP: style-src unsafe-inline	Medium	4 (28.6%)
Content Security Policy (CSP) Header Not Set	Medium	3 (21.4%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1 (7.1%)
CSP: Notices	Low	4 (28.6%)
Cookie No HttpOnly Flag	Low	7 (50.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	5 (35.7%)
X-Content-Type-Options Header Missing	Low	4 (28.6%)
Authentication Request Identified	Informational	1 (7.1%)
Information Disclosure - Suspicious Comments	Informational	1 (7.1%)
Modern Web Application	Informational	1 (7.1%)
Session Management Response Identified	Informational	10 (71.4%)
Total		14

Alerts

Risk=Medium, Confidence=High (5)

<http://127.0.0.1:8000> (5)

CSP: Wildcard Directive (1)

- ▶ GET <http://127.0.0.1:8000/>

CSP: script-src unsafe-eval (1)

- ▶ GET <http://127.0.0.1:8000/>

CSP: script-src unsafe-inline (1)

- ▶ GET <http://127.0.0.1:8000/>

CSP: style-src unsafe-inline (1)

- ▶ GET <http://127.0.0.1:8000/>

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

- ▶ POST <http://127.0.0.1:8000/register>

Risk=Low, Confidence=High (1)

<http://127.0.0.1:8000> (1)

CSP: Notices (1)

- ▶ GET <http://127.0.0.1:8000/>

Risk=Low, Confidence=Medium (4)

<http://127.0.0.1:5173> (1)

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

- ▶ GET <http://127.0.0.1:5173/resources/js/app.js>

<http://127.0.0.1:8000> (3)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

- ▶ GET <http://127.0.0.1:8000/dashboard>

Cookie No HttpOnly Flag (1)

- ▶ GET <http://127.0.0.1:8000/>

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

- ▶ POST <http://127.0.0.1:8000/register>

Risk=Informational, Confidence=High (1)

<http://127.0.0.1:8000> (1)

Authentication Request Identified (1)

- ▶ POST <http://127.0.0.1:8000/login>

Risk=Informational, Confidence=Medium (2)

<http://127.0.0.1:8000> (2)

Modern Web Application (1)

► GET http://127.0.0.1:8000/

Session Management Response Identified (1)

► GET http://127.0.0.1:8000/

Risk=Informational, Confidence=Low (1)

http://127.0.0.1:5173 (1)

Information Disclosure - Suspicious Comments (1)

► GET http://127.0.0.1:5173/resources/css/app.css

Appendix

Alert Types

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://www.w3.org/TR/CSP/▪ https://caniuse.com/#search=content+security+policy▪ https://content-security-policy.com/

- <https://github.com/HtmlUnit/htmlunit-csp>
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-eval

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://www.w3.org/TR/CSP/▪ https://caniuse.com/#search=content+security+policy▪ https://content-security-policy.com/▪ https://github.com/HtmlUnit/htmlunit-csp▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://www.w3.org/TR/CSP/▪ https://caniuse.com/

[#search=content+security+policy](#)

- <https://content-security-policy.com/>
- <https://github.com/HtmlUnit/htmlunit-csp>
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none">▪ https://www.w3.org/TR/CSP/▪ https://caniuse.com/#search=content+security+policy▪ https://content-security-policy.com/▪ https://github.com/HtmlUnit/htmlunit-csp▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

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

- 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/>

Big Redirect Detected (Potential Sensitive Information Leak)

Source raised by a passive scanner ([Big Redirect Detected \(Potential Sensitive Information Leak\)](#))

CWE ID [201](#)

WASC ID 13

CSP: Notices

Source raised by a passive scanner ([CSP](#))

CWE ID [693](#)

WASC ID 15

Reference

- <https://www.w3.org/TR/CSP/>
- <https://caniuse.com/#search=content+security+policy>
- <https://content-security-policy.com/>
- <https://github.com/HtmlUnit/htmlunit-csp>
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-

[Information_Gathering/08-Fingerprint_Web_Application_Framework](#)

- <https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.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

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
WASC	13

ID**Modern Web Application**

Source raised by a passive scanner ([Modern Web Application](#))

Session Management Response Identified

Source raised by a passive scanner ([Session Management Response Identified](#))

Reference

- <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id>