ZAP by Checkmarx Scanning Report

Generated with ZAP on Sat 3 Jan 2026, at 22:03:32

ZAP Version: 2.17.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- `http://cdnjs.cloudflare.com`
- `http://127.0.0.1:42000`

(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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	3 (23.1%)	3 (23.1%)	0 (0.0%)	6 (46.2%)
	Low	0 (0.0%)	0 (0.0%)	4 (30.8%)	1 (7.7%)	5 (38.5%)
	Informational	0 (0.0%)	0 (0.0%)	1 (7.7%)	1 (7.7%)	2 (15.4%)
	Total	0 (0.0%)	3 (23.1%)	8 (61.5%)	2 (15.4%)	13 (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://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	0 (1)
	http://127.0.0.1:42000	0 (0)	5 (5)	5 (10)	2 (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: Failure to Define Directive with No Fallback	Medium	5 (38.5%)
Content Security Policy (CSP) Header Not Set	Medium	5 (38.5%)
Cross-Domain Misconfiguration	Medium	8 (61.5%)
Missing Anti-clickjacking Header	Medium	1 (7.7%)
Session ID in URL Rewrite	Medium	3 (23.1%)
Vulnerable JS Library	Medium	1 (7.7%)
Total		13

Alert type	Risk	Count
Application Error Disclosure	Low	4 (30.8%)
Cross-Domain JavaScript Source File Inclusion	Low	5 (38.5%)
Private IP Disclosure	Low	1 (7.7%)
Timestamp Disclosure - Unix	Low	5 (38.5%)
X-Content-Type-Options Header Missing	Low	3 (23.1%)
Information Disclosure - Suspicious Comments	Informational	3 (23.1%)
Modern Web Application	Informational	5 (38.5%)
Total		13

Alerts

Risk=Medium, Confidence=High (3)

http://127.0.0.1:42000 (3)

CSP: Failure to Define Directive with No Fallback (1)

▶ GET http://127.0.0.1:42000/assets

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

▶ GET http://127.0.0.1:42000/

Session ID in URL Rewrite (1)

▶ POST http://127.0.0.1:42000/socket.io/?EIO=4&transport=polling&t=Pk5so3L&sid=1vDi4dZP8URnq6dIAAAC

Risk=Medium, Confidence=Medium (3)

http://cdnjs.cloudflare.com (1)

Vulnerable JS Library (1)

▶ GET http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js

http://127.0.0.1:42000 (2)

Cross-Domain Misconfiguration (1)

▶ GET http://127.0.0.1:42000/runtime.js

Missing Anti-clickjacking Header (1)

▶ POST http://127.0.0.1:42000/socket.io/?EIO=4&transport=polling&t=Pk5so3L&sid=1vDi4dZP8URnq6dIAAAC

Risk=Low, Confidence=Medium (4)

http://127.0.0.1:42000 (4)

Application Error Disclosure (1)

▶ GET http://127.0.0.1:42000/api

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET `http://127.0.0.1:42000/`

Private IP Disclosure (1)

▶ GET `http://127.0.0.1:42000/rest/admin/application-configuration`

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

▶ GET `http://127.0.0.1:42000/socket.io/?EIO=4&transport=polling&t=Pk5snGb`

Risk=Low, Confidence=Low (1)

`http://127.0.0.1:42000` (1)

Timestamp Disclosure - Unix (1)

▶ GET `http://127.0.0.1:42000/`

Risk=Informational, Confidence=Medium (1)

`http://127.0.0.1:42000` (1)

Modern Web Application (1)

▶ GET `http://127.0.0.1:42000/`

Risk=Informational, Confidence=Low (1)

`http://127.0.0.1:42000` (1)

Information Disclosure - Suspicious Comments (1)

▶ GET `http://127.0.0.1:42000/main.js`

Appendix

Alert types

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

CSP: Failure to Define Directive with No Fallback

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://web.dev/articles/csp#resource-options

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/HTTP/Guides/CSP ▪ 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/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	598

WASC ID	13
Reference	- https://seclists.org/webappsec/2002/q4/111

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	550
WASC ID	13

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	497
WASC ID	13

Reference	▪ https://datatracker.ietf.org/doc/html/rfc1918

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	▪ 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	▪ 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

Information Disclosure - Suspicious Comments

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)