ZAP by Checkmarx Scanning Report

Generated with ⚡ZAP on Fri 6 Dec 2024, at 18:05:18

ZAP Version: 2.15.0

ZAP by Checkmarx

Contents

- **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://cdnjs.cloudflare.com`
- `http://localhost:3000`

(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**
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (22.2%)	2 (22.2%)	0 (0.0%)	4 (44.4%)
Risk	**Low**	0 (0.0%)	0 (0.0%)	2 (22.2%)	0 (0.0%)	2 (22.2%)
	Informational	0 (0.0%)	0 (0.0%)	3 (33.3%)	0 (0.0%)	3 (33.3%)
	Total	0 (0.0%)	2 (22.2%)	7 (77.8%)	0 (0.0%)	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.)

		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
					Risk
Site	https://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	1 (2)
	http://localhost:3000	0 (0)	3 (3)	2 (5)	2 (7)

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	7 (77.8%)
Content Security Policy (CSP) Header Not Set	Medium	4 (44.4%)
Cross-Domain Misconfiguration	Medium	1 (11.1%)
Missing Anti-clickjacking Header	Medium	4 (44.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	15 (166.7%)
X-Content-Type-Options Header Missing	Low	8 (88.9%)
Total		9

Alert type	Risk	Count
Modern Web Application	Informational	3 (33.3%)
Retrieved from Cache	Informational	2 (22.2%)
User Agent Fuzzer	Informational	12 (133.3%)
Total		9

Alerts

Risk=`Medium`**, Confidence=**`High` **(2)**

`http://localhost:3000` **(2)**

CSP: Wildcard Directive (1)

▶ GET `http://localhost:3000/sitemap.xml`

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

▶ POST `http://localhost:3000/api/register`

Risk=`Medium`**, Confidence=**`Medium` **(2)**

`https://cdnjs.cloudflare.com` **(1)**

Cross-Domain Misconfiguration (1)

▶ GET `https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css`

---

http://localhost:3000 **(1)**

Missing Anti-clickjacking Header **(1)**

▶ POST http://localhost:3000/api/register

Risk=Low, Confidence=Medium **(2)**

http://localhost:3000 **(2)**

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

▶ GET http://localhost:3000/scripts.js

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

▶ GET http://localhost:3000/scripts.js

Risk=Informational, Confidence=Medium **(3)**

https://cdnjs.cloudflare.com **(1)**

Retrieved from Cache **(1)**

▶ GET https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css

http://localhost:3000 **(2)**

Modern Web Application **(1)**

▶ GET http://localhost:3000/regestration.html

User Agent Fuzzer **(1)**

▶ GET http://localhost:3000/images

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	• 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/](#)

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?id=desc.config.dotnet.html5_overly_permissive_cors_policy](#)

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/Headers/X-Frame-Options

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	[200](#)
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	■ [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941)

- https://owasp.org/www-community/Security_Headers

Modern Web Application

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

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

User Agent Fuzzer

Source	raised by an active scanner ([User Agent Fuzzer](#))
Reference	- https://owasp.org/wstg