ZAP by Checkmarx Scanning Report

Generated with ZAP on Tue 18 Mar 2025, at 12:47:32

ZAP Version: 2.16.0

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=Medium (1)
  - Risk=Medium, Confidence=High (2)
  - Risk=Medium, Confidence=Medium (3)
  - Risk=Low, Confidence=Medium (3)

- Risk=Low, Confidence=Low (1)
- Risk=Informational, Confidence=Medium (9)
- 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://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
Risk	High	0 (0.0%)	0 (0.0%)	1 (5.0%)	0 (0.0%)	1 (5.0%)
	Medium	0 (0.0%)	2 (10.0%)	3 (15.0%)	0 (0.0%)	5 (25.0%)
	Low	0 (0.0%)	0 (0.0%)	3 (15.0%)	1 (5.0%)	4 (20.0%)
	Informational	0 (0.0%)	0 (0.0%)	9 (45.0%)	1 (5.0%)	10 (50.0%)
	Total	0 (0.0%)	2 (10.0%)	16 (80.0%)	2 (10.0%)	20 (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)	3 (4)
	http://localhost:3000	1 (1)	4 (5)	4 (9)	7 (16)

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
SQL Injection - SQLite	High	1 (5.0%)
Content Security Policy (CSP) Header Not Set	Medium	65 (325.0%)
Total		20

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	98 (490.0%)
Missing Anti-clickjacking Header	Medium	8 (40.0%)
Session ID in URL Rewrite	Medium	37 (185.0%)
Vulnerable JS Library	Medium	1 (5.0%)
Cross-Domain JavaScript Source File Inclusion	Low	98 (490.0%)
Private IP Disclosure	Low	1 (5.0%)
Timestamp Disclosure - Unix	Low	5 (25.0%)
X-Content-Type-Options Header Missing	Low	37 (185.0%)
Information Disclosure - Suspicious Comments	Informational	4 (20.0%)
Modern Web Application	Informational	50 (250.0%)
Retrieved from Cache	Informational	3 (15.0%)
Tech Detected - Cloudflare	Informational	1 (5.0%)
Total		20

Alert type	Risk	Count
Tech Detected - HTTP/3	Informational	1 (5.0%)
Tech Detected - Onsen UI	Informational	1 (5.0%)
Tech Detected - SoundCloud	Informational	1 (5.0%)
Tech Detected - cdnjs	Informational	1 (5.0%)
Tech Detected - jQuery	Informational	1 (5.0%)
User Agent Fuzzer	Informational	109 (545.0%)
Total		20

Alerts

Risk=High, Confidence=Medium (1)

http://localhost:3000 (1)

SQL Injection - SQLite (1)

▶ GET http://localhost:3000/rest/products/search?q=%27%28

Risk=Medium, Confidence=High (2)

http://localhost:3000 (2)

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

▶ GET http://localhost:3000

Session ID in URL Rewrite (1)

▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMfyurB&sid=ksDkJHdpd9WqyYF7AAAC

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://localhost:3000 (2)

Cross-Domain Misconfiguration (1)

▶ GET http://localhost:3000

Missing Anti-clickjacking Header (1)

▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMfyurB&sid=ksDkJHdpd9WqyYF7AAAC

Risk=Low, Confidence=Medium (3)

http://localhost:3000 (3)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://localhost:3000

Private IP Disclosure (1)

▶ GET http://localhost:3000/rest/admin/application-configuration

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

▶ GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMfyujD

Risk=Low, Confidence=Low (1)

http://localhost:3000 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://localhost:3000/main.js

Risk=Informational, Confidence=Medium (9)

http://cdnjs.cloudflare.com (3)

Retrieved from Cache (1)

▶ GET http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css

Tech Detected - Cloudflare (1)

▶ GET http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css

Tech Detected - HTTP/3 (1)

▶ GET http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js

http://localhost:3000 (6)

Modern Web Application (1)

▶ GET http://localhost:3000

Tech Detected - Onsen UI (1)

▶ GET http://localhost:3000

Tech Detected - SoundCloud (1)

▶ GET http://localhost:3000/rest/admin/application-configuration

Tech Detected - cdnjs (1)

▶ GET http://localhost:3000

Tech Detected - jQuery (1)

▶ GET http://localhost:3000

User Agent Fuzzer (1)

▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMfz2XS&sid=mtOCpNnTFH0pr2lEAAAQ

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3000/main.js

Appendix

Alert types

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

SQL Injection - SQLite

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.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

- 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

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/

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://tools.ietf.org/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)

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

Tech Detected - Cloudflare

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://www.cloudflare.com

Tech Detected - HTTP/3

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://httpwg.org/

Tech Detected - Onsen UI

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://onsen.io

Tech Detected - SoundCloud

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://developers.soundcloud.com/docs/api/html5-widget

Tech Detected - cdnjs

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)

WASC ID 13

Reference
- https://cdnjs.com

Tech Detected - jQuery

Source raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)

WASC ID 13

Reference
- https://jquery.com

User Agent Fuzzer

Source raised by an active scanner (User Agent Fuzzer)

Reference
- https://owasp.org/wstg