ZAP by Checkmarx Scanning Report

Generated with ZAP on Sun 7 Sept 2025, at 12:56:42

ZAP Version: 2.16.1

ZAP by Checkmarx

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://127.0.0.1:3000`
- `http://example.com`

(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`, `False Positive`

Excluded: None

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	False Positive	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (9.1%)	0 (0.0%)	1 (9.1%)
	Medium	0 (0.0%)	2 (18.2%)	2 (18.2%)	0 (0.0%)	0 (0.0%)	4 (36.4%)
	Low	0 (0.0%)	0 (0.0%)	2 (18.2%)	1 (9.1%)	0 (0.0%)	3 (27.3%)
	Informational	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	0 (0.0%)	3 (27.3%)
	Total	0 (0.0%)	3 (27.3%)	5 (45.5%)	3 (27.3%)	0 (0.0%)	11 (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://127.0.0.1:3000	1 (1)	2 (3)	2 (5)	3 (8)
	http://example.com	0 (0)	2 (2)	1 (3)	0 (3)

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

Alert type	Risk	Count
SQL Injection	High	3 (27.3%)
Content Security Policy (CSP) Header Not Set	Medium	3 (27.3%)
Cross-Domain Misconfiguration	Medium	27 (245.5%)
Missing Anti-clickjacking Header	Medium	3 (27.3%)
Session ID in URL Rewrite	Medium	7 (63.6%)
Private IP Disclosure	Low	1 (9.1%)
Timestamp Disclosure - Unix	Low	2 (18.2%)
X-Content-Type-Options Header Missing	Low	8 (72.7%)
Authentication Request Identified	Informational	2 (18.2%)
Session Management Response Identified	Informational	3 (27.3%)

Alert type	Risk	Count
User Agent Fuzzer	Informational	320 (2,909.1%)
Total		11

Alerts

Risk=High, Confidence=Low (1)

http://127.0.0.1:3000 (1)

SQL Injection (1)

▶ GET http://127.0.0.1:3000/rest/products/search?q=%27%28

Risk=Medium, Confidence=High (2)

http://127.0.0.1:3000 (1)

Session ID in URL Rewrite (1)

▶ GET http://127.0.0.1:3000/socket.io/?EIO=4&transport=polling&t=PaYrYmk&sid=HIjWKXXhTRnmC7QIAAAW

http://example.com (1)

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

▶ GET http://example.com/

Risk=Medium, Confidence=Medium (2)

http://127.0.0.1:3000 (1)

Cross-Domain Misconfiguration (1)

▶ GET http://127.0.0.1:3000/runtime.js

http://example.com (1)

Missing Anti-clickjacking Header (1)

▶ GET http://example.com/

Risk=Low, Confidence=Medium (2)

http://127.0.0.1:3000 (1)

Private IP Disclosure (1)

▶ GET http://127.0.0.1:3000/rest/admin/application-configuration

http://example.com (1)

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

▶ GET http://example.com/

Risk=Low, Confidence=Low (1)

http://127.0.0.1:3000 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://127.0.0.1:3000/rest/admin/application-configuration

Risk=Informational, Confidence=High (1)

http://127.0.0.1:3000 (1)

Session Management Response Identified (1)

▶ GET http://127.0.0.1:3000/rest/user/login

Risk=Informational, Confidence=Medium (1)

http://127.0.0.1:3000 (1)

User Agent Fuzzer (1)

▶ POST http://127.0.0.1:3000/socket.io/?EIO=4&transport=polling&t=PaYwnxO&sid=djT6CUBVV3Hp14g7AAAY

Risk=Informational, Confidence=Low (1)

http://127.0.0.1:3000 (1)

Authentication Request Identified (1)

▶ POST http://127.0.0.1:3000/api/Users/

Appendix

Alert Types

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

SQL Injection

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/webappse

	c/2002/q4/111

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

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/

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

User Agent Fuzzer

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