ZAP by Checkmarx Scanning Report

Generated with ZAP on Sun 22 Dec 2024, at 13:09:59

ZAP Version: 2.15.0

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://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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	3 (75.0%)	0 (0.0%)	0 (0.0%)	3 (75.0%)
	Low	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Informational	0 (0.0%)	1 (25.0%)	0 (0.0%)	0 (0.0%)	1 (25.0%)
	Total	0 (0.0%)	4 (100.0%)	0 (0.0%)	0 (0.0%)	4 (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://localhost:3000	0 (0)	3 (3)	0 (3)	1 (4)

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	9 (225.0%)
CSP: style-src unsafe-inline	Medium	6 (150.0%)
Hidden File Found	Medium	1 (25.0%)
Authentication Request Identified	Informational	1 (25.0%)
Total		4

Alerts

Risk=Medium, Confidence=High (3)

http://localhost:3000 (3)

CSP: Wildcard Directive (1)

▶ GET http://localhost:3000/

CSP: style-src unsafe-inline (1)

▶ GET http://localhost:3000/

Hidden File Found (1)

▶ GET http://localhost:3000/.git/config

Risk=Informational, Confidence=High (1)

http://localhost:3000 (1)

Authentication Request Identified (1)

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

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

CSP: style-src unsafe-inline

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

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://git-scm.com/docs/git-config

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/