ZAP by Checkmarx Scanning Report

Generated with ZAP on Wed 3 Dec 2025, at 14:19:31

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://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%)	2 (25.0%)	1 (12.5%)	0 (0.0%)	3 (37.5%)
	Low	0 (0.0%)	0 (0.0%)	2 (25.0%)	0 (0.0%)	2 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	2 (25.0%)	1 (12.5%)	3 (37.5%)
	Total	0 (0.0%)	2 (25.0%)	5 (62.5%)	1 (12.5%)	8 (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)	2 (5)	3 (8)

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	2 (25.0%)
Content Security Policy (CSP) Header Not Set	Medium	2 (25.0%)
Missing Anti-clickjacking Header	Medium	2 (25.0%)
Total		8

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	4 (50.0%)
X-Content-Type-Options Header Missing	Low	2 (25.0%)
Authentication Request Identified	Informational	1 (12.5%)
Information Disclosure - Sensitive Information in URL	Informational	2 (25.0%)
Modern Web Application	Informational	2 (25.0%)
Total		8

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:3000 (2)

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

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

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

▶ GET http://localhost:3000

Risk=Medium, Confidence=Medium (1)

http://localhost:3000 (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:3000

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/sitemap.xml

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

▶ GET http://localhost:3000

Risk=Informational, Confidence=Medium (2)

http://localhost:3000 (2)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost:3000/?password=ZAP&username=ZAP

Modern Web Application (1)

▶ GET http://localhost:3000

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Authentication Request Identified (1)

▶ GET http://localhost:3000/?password=ZAP&username=ZAP

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/

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

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	497
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/shhh-dont-let-your-response-headers/

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/

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	598
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)