ZAP by Checkmarx Scanning Report

Generated with ZAP on Sat 21 Dec 2024, at 17:05:17

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 (33.3%)	1 (11.1%)	0 (0.0%)	4 (44.4%)
	Low	0 (0.0%)	0 (0.0%)	2 (22.2%)	0 (0.0%)	2 (22.2%)
	Informational	0 (0.0%)	1 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Total	0 (0.0%)	4 (44.4%)	4 (44.4%)	1 (11.1%)	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.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://localhost:3000	0 (0)	4 (4)	2 (6)	3 (9)

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	3 (33.3%)
Content Security Policy (CSP) Header Not Set	Medium	7 (77.8%)
Hidden File Found	Medium	1 (11.1%)
Missing Anti-clickjacking Header	Medium	7 (77.8%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	15 (166.7%)
X-Content-Type-Options Header Missing	Low	11 (122.2%)
Authentication Request Identified	Informational	1
Total		9

Alert type	Risk	Count
		(11.1%)
Information Disclosure - Sensitive Information in URL	Informational	1 (11.1%)
Information Disclosure - Suspicious Comments	Informational	1 (11.1%)
Total		9

Alerts

Risk=Medium, Confidence=High (3)

http://localhost:3000 (3)

CSP: Wildcard Directive (1)

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

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

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

Hidden File Found (1)

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

Risk=Medium, Confidence=Medium (1)

http://localhost:3000 (1)

Missing Anti-clickjacking Header (1)

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

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/images/icon1.png

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

▶ GET http://localhost:3000/images/icon1.png

Risk=Informational, Confidence=High (1)

http://localhost:3000 (1)

Authentication Request Identified (1)

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

Risk=Informational, Confidence=Medium (1)

http://localhost:3000 (1)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost:3000/welcome.html?username=ZAP

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3000/welcome.html?username=ZAP

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/

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

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://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	200
WASC ID	13

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13