ZAP by Checkmarx Scanning Report

Generated with ZAP on Thu 20 Mar 2025, at 20:20:46

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

- Risk=Informational, Confidence=Medium (3)
- 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://localhost:3000
- http://localhost:5173

(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 (16.7%)	1 (8.3%)	0 (0.0%)	3 (25.0%)
	Low	0 (0.0%)	0 (0.0%)	3 (25.0%)	0 (0.0%)	3 (25.0%)
	Informational	0 (0.0%)	2 (16.7%)	3 (25.0%)	1 (8.3%)	6 (50.0%)
	Total	0 (0.0%)	4 (33.3%)	7 (58.3%)	1 (8.3%)	12 (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.)

Site	Risk: High (= High)	Risk: Medium (>= Medium)	Risk: Low (>= Low)	Risk: Informational (>= Informational)
http://localhost:3000	0 (0)	0 (0)	1 (1)	2 (3)
http://localhost:5173	0 (0)	3 (3)	2 (5)	4 (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
Content Security Policy (CSP) Header Not Set	Medium	1 (8.3%)
Information Disclosure - JWT in Browser localStorage	Medium	2 (16.7%)
Total		12

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	1 (8.3%)
Private IP Disclosure	Low	1 (8.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	63 (525.0%)
X-Content-Type-Options Header Missing	Low	106 (883.3%)
Authentication Request Identified	Informational	2 (16.7%)
Information Disclosure - Information in Browser localStorage	Informational	4 (33.3%)
Information Disclosure - Sensitive Information in URL	Informational	3 (25.0%)
Information Disclosure - Suspicious Comments	Informational	6 (50.0%)
Modern Web Application	Informational	1 (8.3%)
Session Management Response Identified	Informational	2 (16.7%)
Total		12

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:5173 (2)

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

▶ GET http://localhost:5173/

Information Disclosure - JWT in Browser localStorage (1)

▶ GET http://localhost:5173/

Risk=Medium, Confidence=Medium (1)

http://localhost:5173 (1)

Missing Anti-clickjacking Header (1)

▶ GET http://localhost:5173/

Risk=Low, Confidence=Medium (3)

http://localhost:3000 (1)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET http://localhost:3000/api/meals/rating?mealId=633167

http://localhost:5173 (2)

Private IP Disclosure (1)

▶ GET http://localhost:5173/node_modules/.vite/deps/react-icons_fa.js?v=acb8032b

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

▶ GET http://localhost:5173/src/main.jsx

Risk=Informational, Confidence=High (2)

http://localhost:3000 (1)

Authentication Request Identified (1)

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

http://localhost:5173 (1)

Information Disclosure - Information in Browser localStorage (1)

▶ GET http://localhost:5173/

Risk=Informational, Confidence=Medium (3)

http://localhost:3000 (1)

Session Management Response Identified (1)

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

http://localhost:5173 (2)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost:5173/?token=pC1QcWz4OEa1

Modern Web Application (1)

▶ GET http://localhost:5173/

Risk=Informational, Confidence=Low (1)

http://localhost:5173 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:5173/node_modules/.vite/deps/chunk-RLJ2RCJQ.js?v=acb8032b

Appendix

Alert types

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

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/

Information Disclosure - JWT in Browser localStorage

Source	raised by a passive scanner (plugin ID: 120002)
CWE ID	922
WASC ID	13
Reference	▪ https://www.zaproxy.org/blog/2020-09-03-zap-jwt-scanner/

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

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

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/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 - Information in Browser localStorage

Source	raised by a passive scanner (plugin ID: 120000)
CWE ID	359
WASC ID	13

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)

CWE ID	598
WASC ID	13

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)

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