

ZAP by Checkmarx

Scanning Report

Generated with  ZAP on Sun 1 Mar 2026, at 04:51:45

ZAP Version: 2.17.0

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](#)
 - [Insights](#)
- [Alerts](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Low, Confidence=Medium \(1\)](#)
 - [Risk=Low, Confidence=Low \(1\)](#)

- [Risk=Informational, Confidence=Medium \(1\).](#)
- [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>

(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
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (16.7%)	1 (16.7%)	0 (0.0%)
	Low	0 (0.0%)	0 (0.0%)	1 (16.7%)	1 (16.7%)
	Informational	0 (0.0%)	0 (0.0%)	1 (16.7%)	1 (16.7%)
	1	0 (0.0%)	0 (0.0%)	1 (16.7%)	1 (16.7%)
Total		0 (0.0%)	1 (16.7%)	3 (50.0%)	2 (33.3%)

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

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	5 (83.3%)
Cross-Domain Misconfiguration	Medium	5 (83.3%)
Cross-Domain JavaScript Source File Inclusion	Low	5 (83.3%)
Timestamp Disclosure - Unix	Low	5 (83.3%)
Information Disclosure - Suspicious Comments	Informational	2 (33.3%)
Modern Web Application	Informational	5 (83.3%)
Total		6

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	2
Info	Informational	http://localhost:3000	Percentage of responses with status code 2xx	96 %
Info	Informational	http://localhost:3000	Percentage of responses with status code 4xx	3 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type application/javascript	5 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type application/octet-stream	6 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type image/x-icon	1 %
Info	Informational	http://localhost	Percentage of endpoints with	1 %

Level	Reason	Site	Description	Statistic
		ost:3000	content type text/css	
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text/html	79 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text/markdown	4 %
Info	Informational	http://localhost:3000	Percentage of endpoints with content type text/plain	1 %
Info	Informational	http://localhost:3000	Percentage of endpoints with method GET	100 %
Info	Informational	http://localhost:3000	Count of total endpoints	72
Info	Informational	http://localhost:3000	Percentage of slow responses	18 %

Alerts

Risk=Medium, Confidence=High (1)

<http://localhost:3000> (1)

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

► GET <http://localhost:3000/>

Risk=Medium, Confidence=Medium (1)

<http://localhost:3000> (1)

Cross-Domain Misconfiguration (1)

► GET <http://localhost:3000/runtime.js>

Risk=Low, Confidence=Medium (1)

<http://localhost:3000> (1)

Cross-Domain JavaScript Source File Inclusion (1)

► GET <http://localhost:3000/>

Risk=Low, Confidence=Low (1)

<http://localhost:3000> (1)

Timestamp Disclosure - Unix (1)

► GET <http://localhost:3000/>

Risk=Informational, Confidence=Medium (1)

<http://localhost:3000> (1)

Modern Web Application (1)

► GET http://localhost:3000/

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Information Disclosure - Suspicious Comments (1)

► GET http://localhost:3000/main.js

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	<ul style="list-style-type: none">▪ 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/>

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	<ul style="list-style-type: none">▪ https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

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>
|

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](#))