ZAP Scanning Report

Generated with ⚡ZAP on Thu 8 Aug 2024, at 01:04:34

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

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:8083
- http://localhost:8085

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

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 (12.5%)
Missing Anti-clickjacking Header	Medium	1 (12.5%)
Spring Actuator Information Leak	Medium	1 (12.5%)
Timestamp Disclosure - Unix	Low	74 (925.0%)
Total		8

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Low	16 (200.0%)
Information Disclosure - Suspicious Comments	Informational	2 (25.0%)
Modern Web Application	Informational	1 (12.5%)
User Agent Fuzzer	Informational	36 (450.0%)
Total		8

Alerts

Risk=Medium**, Confidence=**High **(1)**

Risk=Medium**, Confidence=**Medium **(2)**

Risk=Low**, Confidence=**Medium **(1)**

Risk=Low**, Confidence=**Low **(1)**

Risk=Informational**, Confidence=**Medium **(2)**

Risk=Informational**, Confidence=**Low **(1)**

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/](#)

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

Spring Actuator Information Leak

Source	raised by an active scanner (plugin ID: 40042)
CWE ID	215
WASC ID	13
Reference	▪ https://docs.spring.io/spring-boot/docs/current/actuator-api/htmlsingle/#overview

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.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

Information Disclosure - Suspicious Comments

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

User Agent Fuzzer

Source	raised by an active scanner (plugin ID: 10104)
Reference	• https://owasp.org/wstg