

ZAP Scanning Report

Generated with  ZAP on Sat 15 Jun 2024, at 22:07:09

ZAP Version: 2.15.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

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=High, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Low, Confidence=Medium \(2\)](#)
 - [Risk=Low, Confidence=Low \(1\)](#)
 - [Risk=Informational, Confidence=Medium \(1\)](#)
- [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:8003>

(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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)
	Medium	0 (0.0%)	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)
	Low	0 (0.0%)	0 (0.0%)	2 (33.3%)	1 (16.7%)	3 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)
	Total	0 (0.0%)	0 (0.0%)	5 (83.3%)	1 (16.7%)	6 (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) 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
SQL Injection	High	1 (16.7%)
Buffer Overflow	Medium	1 (16.7%)
Application Error Disclosure	Low	1 (16.7%)
Cross Site Scripting Weakness (Persistent in JSON Response)	Low	1 (16.7%)
Information Disclosure - Debug Error Messages	Low	1 (16.7%)
User Agent Fuzzer	Informational	60 (1,000.0%)
Total		6

Alerts

Risk=High, Confidence=Medium (1)

Risk=Medium, Confidence=Medium (1)

Risk=Low, Confidence=Medium (2)

Risk=Low, Confidence=Low (1)

Risk=Informational, Confidence=Medium (1)

Appendix

Alert types

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

SQL Injection

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	■ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Buffer Overflow

Source	raised by an active scanner (Buffer Overflow)
CWE ID	120
WASC ID	7

Reference

- https://owasp.org/www-community/attacks/Buffer_overflow_attack

Application Error Disclosure**Source**

raised by a passive scanner ([Application Error Disclosure](#))

CWE ID

[200](#)

WASC ID

13

Cross Site Scripting Weakness (Persistent in JSON Response)**Source**

raised by an active scanner ([Cross Site Scripting_\(Persistent\)](#))

CWE ID

[79](#)

WASC ID

8

Reference

- <https://owasp.org/www-community/attacks/xss/>
- <https://cwe.mitre.org/data/definitions/79.html>

Information Disclosure - Debug Error Messages**Source**

raised by a passive scanner ([Information Disclosure - Debug Error Messages](#))

CWE ID

[200](#)

WASC ID

13

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg