ZAP Scanning Report

Generated with ZAP on Sun 17 Mar 2024, at 14:40:28

ZAP Version: 2.14.0

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:8081`

- `http://localhost:8083`
- `http://localhost:8084`

(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 (16.7%)	3 (50.0%)	0 (0.0%)	4 (66.7%)
	Low	0 (0.0%)	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)
	Informational	0 (0.0%)	0 (0.0%)	1 (16.7%)	0 (0.0%)	1 (16.7%)
	Total	0 (0.0%)	1 (16.7%)	5 (83.3%)	0 (0.0%)	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)**	**Low (>= Low)**	**Informational (>= Informational)**
Site	**http://localhost:8081**	0 (0)	1 (1)	1 (2)	0 (2)
	http://localhost:8083	0 (0)	2 (2)	0 (2)	0 (2)
	http://localhost:8084	0 (0)	1 (1)	0 (1)	1 (2)

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
Buffer Overflow	Medium	3 (50.0%)
Content Security Policy (CSP) Header Not Set	Medium	4 (66.7%)
Format String Error	Medium	1 (16.7%)
Spring Actuator Information Leak	Medium	1 (16.7%)
Application Error Disclosure	Low	2 (33.3%)
User Agent Fuzzer	Informational	36 (600.0%)
Total		6

Alerts

Risk=Medium, Confidence=High (1)

http://localhost:8084 (1)

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

▶ GET http://localhost:8084/robots.txt

Risk=Medium, Confidence=Medium (3)

http://localhost:8081 (1)

Spring Actuator Information Leak (1)

▶ GET http://localhost:8081/lanchonete/actuator/health

http://localhost:8083 (2)

Buffer Overflow (1)

▶ POST http://localhost:8083/pedidos

Format String Error (1)

▶ POST http://localhost:8083/pedidos

Risk=Low, Confidence=Medium (1)

http://localhost:8081 (1)

Application Error Disclosure (1)

▶ POST http://localhost:8081/lanchonete/pagamentos?pagamentoId=30b11e78-8d51-4f29-b4b1-dec8747d5a76

Risk=Informational, Confidence=Medium (1)

http://localhost:8084 (1)

User Agent Fuzzer (1)

▶ GET http://localhost:8084/lanchonete

Appendix

Alert types

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

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

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/

Format String Error

Source	raised by an active scanner (Format String Error)
CWE ID	134
WASC ID	6
Reference	- https://owasp.org/www-community/attacks/Format_string_attack

Spring Actuator Information Leak

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

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

User Agent Fuzzer

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