

ZAP Scanning Report

Generated with  ZAP on Sun 29 Sept 2024, at 22:54:48

ZAP Version: 2.15.0

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 \(1\)](#)
 - [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://juice-shop.herokuapp.com>

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

		Informational		
		High (= High)	Medium (>= Medium)	Low (>= Informational)
Site	http://juice-shop.herokuapp.com	0	2	2
		(0)	(2)	(4)

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	2 (33.3%)
Cross-Domain Misconfiguration	Medium	9 (150.0%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (66.7%)
Timestamp Disclosure - Unix	Low	10 (166.7%)
Information Disclosure - Suspicious Comments	Informational	2 (33.3%)
Modern Web Application	Informational	2 (33.3%)
Total		6

Alerts

Risk=Medium, Confidence=High (1)

<http://juice-shop.herokuapp.com> (1)

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

► GET <http://juice-shop.herokuapp.com/>

Risk=Medium, Confidence=Medium (1)

<http://juice-shop.herokuapp.com> (1)

Cross-Domain Misconfiguration (1)

► GET <http://juice-shop.herokuapp.com/robots.txt>

Risk=Low, Confidence=Medium (1)

<http://juice-shop.herokuapp.com> (1)

Cross-Domain JavaScript Source File Inclusion (1)

► GET <http://juice-shop.herokuapp.com/>

Risk=Low, Confidence=Low (1)

<http://juice-shop.herokuapp.com> (1)

Timestamp Disclosure - Unix (1)

► GET <http://juice-shop.herokuapp.com/robots.txt>

Risk=Informational, Confidence=Medium (1)

<http://juice-shop.herokuapp.com> (1)

Modern Web Application (1)

► GET <http://juice-shop.herokuapp.com/>

Risk=Informational, Confidence=Low (1)

<http://juice-shop.herokuapp.com> (1)

Information Disclosure - Suspicious Comments (1)

► GET <http://juice-shop.herokuapp.com/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	▪ 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/>

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	■ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

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	200
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	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)
--------	--