Juice Shop - Automated Scan by ZAP Report

Generated with ZAP on Tue 12 Aug 2025, at 18:16:08

ZAP Version: 2.16.1

ZAP by Checkmarx

Contents

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://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				
		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 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Low	0 (0.0%)	1 (11.1%)	1 (11.1%)	1 (11.1%)	3 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (11.1%)	2 (22.2%)	3 (33.3%)
	Total	0 (0.0%)	2 (22.2%)	3 (33.3%)	4 (44.4%)	9 (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	https://juice-shop.herokuapp.com	0 (0)	3 (3)	3 (6)	3 (9)

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	57 (633.3%)
Cross-Domain Misconfiguration	Medium	75 (833.3%)
Total		9

Alert type	Risk	Count
Hidden File Found	Medium	4 (44.4%)
Cross-Domain JavaScript Source File Inclusion	Low	96 (1,066.7%)
Strict-Transport-Security Header Not Set	Low	75 (833.3%)
Timestamp Disclosure - Unix	Low	231 (2,566.7%)
Information Disclosure - Suspicious Comments	Informational	2 (22.2%)
Modern Web Application	Informational	49 (544.4%)
Re-examine Cache-control Directives	Informational	19 (211.1%)
Total		9

Alerts

Risk=Medium, Confidence=High (1)

https://juice-shop.herokuapp.com (1)

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

▶ GET https://juice-shop.herokuapp.com/

Risk=Medium, Confidence=Medium (1)

https://juice-shop.herokuapp.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://juice-shop.herokuapp.com/robots.txt

Risk=Medium, Confidence=Low (1)

https://juice-shop.herokuapp.com (1)

Hidden File Found (1)

▶ GET https://juice-shop.herokuapp.com/.hg

Risk=Low, Confidence=High (1)

https://juice-shop.herokuapp.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://juice-shop.herokuapp.com/assets/public/favicon_js.ico

Risk=Low, Confidence=Medium (1)

https://juice-shop.herokuapp.com (1)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://juice-shop.herokuapp.com/

Risk=Low, Confidence=Low (1)

https://juice-shop.herokuapp.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://juice-shop.herokuapp.com/robots.txt

Risk=Informational, Confidence=Medium (1)

https://juice-shop.herokuapp.com (1)

Modern Web Application (1)

▶ GET https://juice-shop.herokuapp.com/

Risk=Informational, Confidence=Low (2)

https://juice-shop.herokuapp.com (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://juice-shop.herokuapp.com/main.js

Re-examine Cache-control Directives (1)

▶ GET https://juice-shop.herokuapp.com/robots.txt

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

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

Cross-Domain JavaScript Source File Inclusion

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

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/

HTTP_Strict_Transport_Security_Cheat_Sheet.html

- https://owasp.org/www-community/Security_Headers
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- https://caniuse.com/stricttransportsecurity
- https://datatracker.ietf.org/doc/html/rfc6797

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)

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/