Automated Scan on JuiceShop -Active Scan

Generated with ZAP on Wed 13 Aug 2025, at 19:33:49

ZAP Version: 2.16.1

ZAP by Checkmarx

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 (2)
  - Risk=Medium, Confidence=Medium (2)
  - Risk=Medium, Confidence=Low (1)
  - Risk=Low, Confidence=Medium (3)

    - 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://localhost:3000`

(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%)	2 (18.2%)	2 (18.2%)	1 (9.1%)	5 (45.5%)
	Low	0 (0.0%)	0 (0.0%)	3 (27.3%)	1 (9.1%)	4 (36.4%)
	Informational	0 (0.0%)	0 (0.0%)	1 (9.1%)	1 (9.1%)	2 (18.2%)
	Total	0 (0.0%)	2 (18.2%)	6 (54.5%)	3 (27.3%)	11 (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:3000	0 (0)	5 (5)	4 (9)	2 (11)

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	22 (200.0%)
Cross-Domain Misconfiguration	Medium	51 (463.6%)
Hidden File Found	Medium	4 (36.4%)
Total		11

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	10 (90.9%)
Session ID in URL Rewrite	Medium	34 (309.1%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (36.4%)
Private IP Disclosure	Low	1 (9.1%)
Timestamp Disclosure - Unix	Low	21 (190.9%)
X-Content-Type-Options Header Missing	Low	34 (309.1%)
Information Disclosure - Suspicious Comments	Informational	3 (27.3%)
Modern Web Application	Informational	3 (27.3%)
Total		11

Alerts

Risk=Medium, Confidence=High (2)

http://localhost:3000 (2)

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

▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PYcPi_Q&sid=3zNn55Mkk0kR3zLHAAAR

Session ID in URL Rewrite (1)

▶ GET http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=3zNn55Mkk0kR3zLHAAAR

Risk=Medium, Confidence=Medium (2)

http://localhost:3000 (2)

Cross-Domain Misconfiguration (1)

▶ GET http://localhost:3000/runtime.js

Missing Anti-clickjacking Header (1)

▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PYcPi_Q&sid=3zNn55Mkk0kR3zLHAAAR

Risk=Medium, Confidence=Low (1)

http://localhost:3000 (1)

Hidden File Found (1)

▶ GET http://localhost:3000/.hg

Risk=Low, Confidence=Medium (3)

http://localhost:3000 (3)

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://localhost:3000/

Private IP Disclosure (1)

▶ GET http://localhost:3000/rest/admin/application-configuration

X-Content-Type-Options Header Missing (1)

▶ GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PYcPi_5

Risk=Low, Confidence=Low (1)

http://localhost:3000 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://localhost:3000/

Risk=Informational, Confidence=Medium (1)

http://localhost:3000 (1)

Modern Web Application (1)

▶ GET http://localhost:3000/

Risk=Informational, Confidence=Low (1)

http://localhost:3000 (1)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost:3000/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

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

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

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	598
WASC ID	13
Reference	https://seclists.org/webappsec/2002/q4/111

Cross-Domain JavaScript Source File Inclusion

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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	497
WASC ID	13
Reference	https://tools.ietf.org/html/rfc1918

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

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	615
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)