ZAP by Checkmarx Scanning Report

Generated with ZAP on Fri 14 Mar 2025, at 19:30:55

ZAP Version: 2.16.0

ZAP by Checkmarx

Contents

About this report

Report description

OWASP JUICE SHOP 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%)	2 (12.5%)	0 (0.0%)	2 (12.5%)
	Medium	0 (0.0%)	3 (18.8%)	2 (12.5%)	0 (0.0%)	5 (31.2%)
	Low	0 (0.0%)	0 (0.0%)	4 (25.0%)	1 (6.2%)	5 (31.2%)
	Informational	0 (0.0%)	1 (6.2%)	2 (12.5%)	1 (6.2%)	4 (25.0%)
	Total	0 (0.0%)	4 (25.0%)	10 (62.5%)	2 (12.5%)	16 (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**	2 (2)	5 (7)	5 (12)	4 (16)

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**
Open Redirect	High	1 (6.2%)
SQL Injection - SQLite	High	3 (18.8%)
CSP: Wildcard Directive	Medium	5 (31.2%)
Content Security Policy (CSP) Header Not Set	Medium	326 (2,037.5%)
Cross-Domain Misconfiguration	Medium	361 (2,256.2%)
Missing Anti-clickjacking Header	Medium	80 (500.0%)
Session ID in URL Rewrite	Medium	373 (2,331.2%)
Application Error Disclosure	Low	7 (43.8%)
Cross-Domain JavaScript Source File Inclusion	Low	460 (2,875.0%)
Private IP Disclosure	Low	1 (6.2%)
Timestamp Disclosure - Unix	Low	5 (31.2%)
X-Content-Type-Options Header Missing	Low	372 (2,325.0%)
Authentication Request Identified	Informational	2 (12.5%)
Information Disclosure - Suspicious Comments	Informational	2 (12.5%)
Modern Web Application	Informational	231 (1,443.8%)
User Agent Fuzzer	Informational	108 (675.0%)
Total		16

Alerts

1. **Risk=High, Confidence=Medium (2)**

1. **http://localhost:3000 (2)**
    1. **Open Redirect (1)**
        - GET http://localhost:3000/redirect?to=https://github.com/juice-shop/juice-shop
    2. **SQL Injection - SQLite (1)**
        - GET http://localhost:3000/rest/products/search?q=%27%28
2. **Risk=Medium, Confidence=High (3)**
    1. **http://localhost:3000 (3)**
        1. **CSP: Wildcard Directive (1)**
            - GET http://localhost:3000/assets
        2. **Content Security Policy (CSP) Header Not Set (1)**
            - GET http://localhost:3000/
        3. **Session ID in URL Rewrite (1)**
            - POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMLNpi0&sid=JRhUHDUo60e2ORz7AAAC
3. **Risk=Medium, Confidence=Medium (2)**
    1. **http://localhost:3000 (2)**
        1. **Cross-Domain Misconfiguration (1)**
            - GET http://localhost:3000/
        2. **Missing Anti-clickjacking Header (1)**
            - POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMLNpi0&sid=JRhUHDUo60e2ORz7AAAC
4. **Risk=Low, Confidence=Medium (4)**
    1. **http://localhost:3000 (4)**
        1. **Application Error Disclosure (1)**
            - GET http://localhost:3000/api
        2. **Cross-Domain JavaScript Source File Inclusion (1)**
            - GET http://localhost:3000/
        3. **Private IP Disclosure (1)**
            - GET http://localhost:3000/rest/admin/application-configuration
        4. **X-Content-Type-Options Header Missing (1)**
            - GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMLNpX7
5. **Risk=Low, Confidence=Low (1)**
    1. **http://localhost:3000 (1)**
        1. **Timestamp Disclosure - Unix (1)**
            - GET http://localhost:3000/main.js
6. **Risk=Informational, Confidence=High (1)**
    1. **http://localhost:3000 (1)**
        1. **Authentication Request Identified (1)**
            - POST http://localhost:3000/rest/user/login

7. **Risk=Informational, Confidence=Medium (2)**

    1. **http://localhost:3000 (2)**

        1. **Modern Web Application (1)**

            ▶ GET http://localhost:3000/

        2. **User Agent Fuzzer (1)**

            ▶ POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PMLNqTM&sid=uv_TUdtuKpIebnQVAAAD

8. **Risk=Informational, Confidence=Low (1)**

    1. **http://localhost:3000 (1)**

        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.

1. **Open Redirect**

    Source raised by a passive scanner (Open Redirect)
    CWE ID 601
    WASC ID 38
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html
    2. https://cwe.mitre.org/data/definitions/601.html

2. **SQL Injection - SQLite**

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

3. **CSP: Wildcard Directive**

    Source raised by a passive scanner (CSP)
    CWE ID 693
    WASC ID 15
    Reference
    1. https://www.w3.org/TR/CSP/
    2. https://caniuse.com/#search=content+security+policy
    3. https://content-security-policy.com/
    4. https://github.com/HtmlUnit/htmlunit-csp
    5. https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

4. **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
    1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
    2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
    3. https://www.w3.org/TR/CSP/
    4. https://w3c.github.io/webappsec-csp/
    5. https://web.dev/articles/csp
    6. https://caniuse.com/#feat=contentsecuritypolicy
    7. https://content-security-policy.com/

5. **Cross-Domain Misconfiguration**

    Source raised by a passive scanner (Cross-Domain Misconfiguration)
    CWE ID 264
    WASC ID 14

Reference 1. https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

6. **Missing Anti-clickjacking Header**

   Source raised by a passive scanner (Anti-clickjacking Header)
   CWE ID 1021
   WASC ID 15
   Reference 1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

7. **Session ID in URL Rewrite**

   Source raised by a passive scanner (Session ID in URL Rewrite)
   CWE ID 598
   WASC ID 13
   Reference 1. https://seclists.org/webappsec/2002/q4/111

8. **Application Error Disclosure**

   Source raised by a passive scanner (Application Error Disclosure)
   CWE ID 550
   WASC ID 13

9. **Cross-Domain JavaScript Source File Inclusion**

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

10. **Private IP Disclosure**

    Source raised by a passive scanner (Private IP Disclosure)
    CWE ID 497
    WASC ID 13
    Reference 1. https://tools.ietf.org/html/rfc1918

11. **Timestamp Disclosure - Unix**

    Source raised by a passive scanner (Timestamp Disclosure)
    CWE ID 497
    WASC ID 13
    Reference 1. https://cwe.mitre.org/data/definitions/200.html

12. **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
    1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
    2. https://owasp.org/www-community/Security_Headers

13. **Authentication Request Identified**

    Source raised by a passive scanner (Authentication Request Identified)
    Reference 1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

14. **Information Disclosure - Suspicious Comments**

    Source raised by a passive scanner (Information Disclosure - Suspicious Comments)
    CWE ID 615
    WASC ID 13

15. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)

16. **User Agent Fuzzer**

Source raised by an active scanner (plugin ID: 10104)

Reference 1. https://owasp.org/wstg