ZAP Scanning Report

Generated with The ZAP logoZAP on Thu 18 Apr 2024, at 11:25:28

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:

- https://bookstack.domain.tld

(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%)	0 (0.0%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	2 (18.2%)	2 (18.2%)	0 (0.0%)	4 (36.4%)
	Informational	0 (0.0%)	1 (9.1%)	1 (9.1%)	2 (18.2%)	4 (36.4%)
	Total	0 (0.0%)	5 (45.5%)	3 (27.3%)	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	**https://bookstack.domain.tld**	0 (0)	3 (3)	4 (7)	4 (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
Absence of Anti-CSRF Tokens	Medium	1 (9.1%)
CSP: Wildcard Directive	Medium	1 (9.1%)
CSP: style-src unsafe-inline	Medium	1 (9.1%)
Cookie No HttpOnly Flag	Low	1 (9.1%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3 (27.3%)
Strict-Transport-Security Header Not Set	Low	3 (27.3%)
X-Content-Type-Options Header Missing	Low	3 (27.3%)
Information Disclosure - Suspicious Comments	Informational	4 (36.4%)
Modern Web Application	Informational	1 (9.1%)
Re-examine Cache-control Directives	Informational	1 (9.1%)
Session Management Response Identified	Informational	3 (27.3%)
Total		11

Alerts

1. **Risk=Medium, Confidence=High (2)**
    1. **https://bookstack.domain.tld (2)**
        1. CSP: Wildcard Directive **(1)**
            1. ▶ GET https://bookstack.domain.tld/
        2. CSP: style-src unsafe-inline **(1)**
            1. ▶ GET https://bookstack.domain.tld/
2. **Risk=Medium, Confidence=Low (1)**
    1. **https://bookstack.domain.tld (1)**

1. Absence of Anti-CSRF Tokens (1)
    1. ▶ GET https://bookstack.domain.tld/

3. **Risk=Low, Confidence=High (2)**
    1. **https://bookstack.domain.tld (2)**
        1. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
            1. ▶ GET https://bookstack.domain.tld/dist/styles.css?version=v24.02.2
        2. Strict-Transport-Security Header Not Set (1)
            1. ▶ GET https://bookstack.domain.tld/dist/styles.css?version=v24.02.2
4. **Risk=Low, Confidence=Medium (2)**
    1. **https://bookstack.domain.tld (2)**
        1. Cookie No HttpOnly Flag (1)
            1. ▶ GET https://bookstack.domain.tld/
        2. X-Content-Type-Options Header Missing (1)
            1. ▶ GET https://bookstack.domain.tld/dist/styles.css?version=v24.02.2
5. **Risk=Informational, Confidence=High (1)**
    1. **https://bookstack.domain.tld (1)**
        1. Session Management Response Identified (1)
            1. ▶ GET https://bookstack.domain.tld/uploads/images/cover_bookshelf/2024-03/thumbs-440-250
6. **Risk=Informational, Confidence=Medium (1)**
    1. **https://bookstack.domain.tld (1)**
        1. Modern Web Application (1)
            1. ▶ GET https://bookstack.domain.tld/
7. **Risk=Informational, Confidence=Low (2)**
    1. **https://bookstack.domain.tld (2)**
        1. Information Disclosure - Suspicious Comments (1)

1. ▶ GET https://bookstack.domain.tld/dist/app.js?version=v24.02.2

2. **Re-examine Cache-control Directives** **(1)**

    1. ▶ GET https://bookstack.domain.tld/

Appendix

Alert types

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

1. **Absence of Anti-CSRF Tokens**

    Source raised by a passive scanner (Absence of Anti-CSRF Tokens)
    CWE ID 352
    WASC ID 9
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
    2. https://cwe.mitre.org/data/definitions/352.html

2. **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

3. **CSP: style-src unsafe-inline**

    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. **Cookie No HttpOnly Flag**

    Source raised by a passive scanner (Cookie No HttpOnly Flag)
    CWE ID 1004
    WASC ID 13

Reference
1. https://owasp.org/www-community/HttpOnly

5. **Server Leaks Version Information via "Server" HTTP Response Header Field**

Source raised by a passive scanner (HTTP Server Response Header)
CWE ID 200
WASC ID 13
Reference
1. https://httpd.apache.org/docs/current/mod/core.html#servertokens
2. https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
3. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

6. **Strict-Transport-Security Header Not Set**

Source raised by a passive scanner (Strict-Transport-Security Header)
CWE ID 319
WASC ID 15
Reference
1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
2. https://owasp.org/www-community/Security_Headers
3. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
4. https://caniuse.com/stricttransportsecurity
5. https://datatracker.ietf.org/doc/html/rfc6797

7. **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

8. **Information Disclosure - Suspicious Comments**

Source raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID 200
WASC ID 13

9. **Modern Web Application**

Source raised by a passive scanner (Modern Web Application)

10. **Re-examine Cache-control Directives**

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

3. https://grayduck.mn/2021/09/13/cache-control-recommendations/

11. **Session Management Response Identified**

Source raised by a passive scanner (Session Management Response Identified)
Reference 1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id