ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Fri 22 Nov 2024, at 21:37:33

ZAP Version: 2.15.0

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://sec.cse.csusb.edu

(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%)	4 (25.0%)	1 (6.2%)	0 (0.0%)	5 (31.2%)
	Low	0 (0.0%)	3 (18.8%)	3 (18.8%)	1 (6.2%)	7 (43.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	2 (12.5%)	4 (25.0%)
	Total	0 (0.0%)	7 (43.8%)	6 (37.5%)	3 (18.8%)	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)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://sec.cse.csusb.edu	0 (0)	5 (5)	7 (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
CSP: Wildcard Directive	Medium	28 (175.0%)
CSP: script-src unsafe-inline	Medium	28 (175.0%)
CSP: style-src unsafe-inline	Medium	28 (175.0%)
Content Security Policy (CSP) Header Not Set	Medium	2 (12.5%)
Vulnerable JS Library	Medium	4 (25.0%)
CSP: Notices	Low	28 (175.0%)
Cookie No HttpOnly Flag	Low	11 (68.8%)
Cookie Without Secure Flag	Low	11 (68.8%)
Cookie without SameSite Attribute	Low	11 (68.8%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	252 (1,575.0%)
Strict-Transport-Security Header Not Set	Low	1 (6.2%)
Timestamp Disclosure - Unix	Low	22 (137.5%)
Information Disclosure - Suspicious Comments	Informational	104 (650.0%)
Modern Web Application	Informational	28 (175.0%)
Re-examine Cache-control Directives	Informational	192 (1,200.0%)
Session Management Response Identified	Informational	28 (175.0%)
Total		16

Alerts

1. **Risk=Medium, Confidence=High (4)**
    1. **https://sec.cse.csusb.edu (4)**
        1. CSP: Wildcard Directive **(1)**
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        2. CSP: script-src unsafe-inline **(1)**
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        3. CSP: style-src unsafe-inline **(1)**
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        4. Content Security Policy (CSP) Header Not Set **(1)**
            1. ▶ GET https://sec.cse.csusb.edu/robots.txt
2. **Risk=Medium, Confidence=Medium (1)**
    1. **https://sec.cse.csusb.edu (1)**

1. Vulnerable JS Library (1)
    1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/static/components/react/react-dom.production.min.js?v=6fc58c1c4736868ff84f57bd8b85f2bdb985993a9392718f3b4af4bfa10fb4efba2b4ddd68644bd2a8daf0619a3844944c9c43f8528364a1aa6fc0

3. **Risk=Low, Confidence=High (3)**
    1. **https://sec.cse.csusb.edu (3)**
        1. CSP: Notices (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        2. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/_stcore/stream
        3. Strict-Transport-Security Header Not Set (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/_stcore/stream
4. **Risk=Low, Confidence=Medium (3)**
    1. **https://sec.cse.csusb.edu (3)**
        1. Cookie No HttpOnly Flag (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        2. Cookie Without Secure Flag (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        3. Cookie without SameSite Attribute (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
5. **Risk=Low, Confidence=Low (1)**
    1. **https://sec.cse.csusb.edu (1)**
        1. Timestamp Disclosure - Unix (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
6. **Risk=Informational, Confidence=Medium (2)**
    1. **https://sec.cse.csusb.edu (2)**
        1. Modern Web Application (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        2. Session Management Response Identified (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
7. **Risk=Informational, Confidence=Low (2)**
    1. **https://sec.cse.csusb.edu (2)**
        1. Information Disclosure - Suspicious Comments (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree
        2. Re-examine Cache-control Directives (1)
            1. ▶ GET https://sec.cse.csusb.edu/team2/jupyter/tree

Appendix

Alert types

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

1. **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

2. **CSP: script-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

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. **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. **Vulnerable JS Library**

   Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
   CWE ID 829
   Reference
   1. https://reactjs.org/blog/2018/08/01/react-v-16-4-2.html
   2. https://github.com/advisories/GHSA-myjj-gqq2-p4hw
   3. https://nvd.nist.gov/vuln/detail/CVE-2018-6341

6. **CSP: Notices**

   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

7. **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

8. **Cookie Without Secure Flag**

Source raised by a passive scanner (Cookie Without Secure Flag)
CWE ID 614
WASC ID 13
Reference
1. https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

9. **Cookie without SameSite Attribute**

Source raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID 1275
WASC ID 13
Reference
1. https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

10. **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/

11. **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

12. **Timestamp Disclosure - Unix**

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

13. **Information Disclosure - Suspicious Comments**

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

14. **Modern Web Application**

Source raised by a passive scanner (Modern Web Application)

15. **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/

16. **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