ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Tue 21 Jan 2025, at 00:20:39

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://admin.securepass.shdigitallab.lk
- https://cdnjs.cloudflare.com
- https://securepass.shdigitallab.lk

(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 (7.7%)	2 (15.4%)	0 (0.0%)	3 (23.1%)
	Low	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Informational	0 (0.0%)	1 (7.7%)	3 (23.1%)	2 (15.4%)	6 (46.2%)
	Total	0 (0.0%)	3 (23.1%)	7 (53.8%)	3 (23.1%)	13 (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://admin.securepass.shdigitallab.lk	0 (0)	0 (0)	1 (1)	1 (2)
	https://cdnjs.cloudflare.com	0 (0)	1 (1)	0 (1)	2 (3)
	https://securepass.shdigitallab.lk	0 (0)	2 (2)	3 (5)	3 (8)

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	8 (61.5%)
Cross-Domain Misconfiguration	Medium	1 (7.7%)
Missing Anti-clickjacking Header	Medium	8 (61.5%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	1 (7.7%)
Strict-Transport-Security Header Not Set	Low	18 (138.5%)
Timestamp Disclosure - Unix	Low	1 (7.7%)
X-Content-Type-Options Header Missing	Low	17 (130.8%)
Authentication Request Identified	Informational	1 (7.7%)
Information Disclosure - Sensitive Information in HTTP Referrer Header	Informational	1 (7.7%)
Information Disclosure - Suspicious Comments	Informational	12 (92.3%)
Modern Web Application	Informational	8 (61.5%)
Re-examine Cache-control Directives	Informational	7 (53.8%)
Retrieved from Cache	Informational	23 (176.9%)
Total		13

Alerts

1. **Risk=Medium, Confidence=High (1)**
    1. **https://securepass.shdigitallab.lk (1)**
        1. Content Security Policy (CSP) Header Not Set (1)
            1. ▶ GET https://securepass.shdigitallab.lk/
2. **Risk=Medium, Confidence=Medium (2)**
    1. **https://cdnjs.cloudflare.com (1)**
        1. Cross-Domain Misconfiguration (1)
            1. ▶ GET https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css
    2. **https://securepass.shdigitallab.lk (1)**
        1. Missing Anti-clickjacking Header (1)
            1. ▶ GET https://securepass.shdigitallab.lk/
3. **Risk=Low, Confidence=High (1)**
    1. **https://securepass.shdigitallab.lk (1)**
        1. Strict-Transport-Security Header Not Set (1)
            1. ▶ GET https://securepass.shdigitallab.lk/
4. **Risk=Low, Confidence=Medium (2)**
    1. **https://admin.securepass.shdigitallab.lk (1)**
        1. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)
            1. ▶ POST https://admin.securepass.shdigitallab.lk/api/admin/login
    2. **https://securepass.shdigitallab.lk (1)**
        1. X-Content-Type-Options Header Missing (1)
            1. ▶ GET https://securepass.shdigitallab.lk/
5. **Risk=Low, Confidence=Low (1)**
    1. **https://securepass.shdigitallab.lk (1)**
        1. Timestamp Disclosure - Unix (1)
            1. ▶ GET https://securepass.shdigitallab.lk/assets/index-DdBvI_-fj.js
6. **Risk=Informational, Confidence=High (1)**
    1. **https://admin.securepass.shdigitallab.lk (1)**
        1. Authentication Request Identified (1)
            1. ▶ POST https://admin.securepass.shdigitallab.lk/api/admin/login
7. **Risk=Informational, Confidence=Medium (3)**
    1. **https://cdnjs.cloudflare.com (2)**
        1. Information Disclosure - Sensitive Information in HTTP Referrer Header (1)
            1. ▶ GET https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css
        2. Retrieved from Cache (1)
            1. ▶ GET https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.0.0-beta3/css/all.min.css
    2. **https://securepass.shdigitallab.lk (1)**
        1. Modern Web Application (1)
            1. ▶ GET https://securepass.shdigitallab.lk/
8. **Risk=Informational, Confidence=Low (2)**
    1. **https://securepass.shdigitallab.lk (2)**
        1. Information Disclosure - Suspicious Comments (1)
            1. ▶ GET https://securepass.shdigitallab.lk/assets/index-DdBvI_-fj.js
        2. Re-examine Cache-control Directives (1)
            1. ▶ GET https://securepass.shdigitallab.lk/

Appendix

Alert types

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

1. **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/

2. **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

3. **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

4. **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**

    Source raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
    CWE ID 200
    WASC ID 13
    Reference
    1. https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
    2. https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

5. **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

6. **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

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. **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/

9. **Information Disclosure - Sensitive Information in HTTP Referrer Header**

    Source raised by a passive scanner (Information Disclosure - Sensitive Information in HTTP Referrer Header)
    CWE ID 200
    WASC ID 13

10. **Information Disclosure - Suspicious Comments**

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

11. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)

12. **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/

13. **Retrieved from Cache**

    Source raised by a passive scanner (Retrieved from Cache)
    Reference
    1. https://tools.ietf.org/html/rfc7234
    2. https://tools.ietf.org/html/rfc7231
    3. https://www.rfc-editor.org/rfc/rfc9110.html