ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Thu 30 Oct 2025, at 11:45:06

ZAP Version: 2.16.1

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:

- http://192.168.56.103

(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%)	1 (4.3%)	1 (4.3%)	0 (0.0%)	2 (8.7%)
	Medium	0 (0.0%)	1 (4.3%)	4 (17.4%)	1 (4.3%)	6 (26.1%)
	Low	0 (0.0%)	1 (4.3%)	6 (26.1%)	1 (4.3%)	8 (34.8%)
	Informational	0 (0.0%)	1 (4.3%)	4 (17.4%)	2 (8.7%)	7 (30.4%)
	Total	0 (0.0%)	4 (17.4%)	15 (65.2%)	4 (17.4%)	23 (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://192.168.56.103**	2 (2)	6 (8)	8 (16)	7 (23)

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
Hash Disclosure - MD5 Crypt	High	1 (4.3%)
Path Traversal	High	4 (17.4%)
Absence of Anti-CSRF Tokens	Medium	1437 (6,247.8%)
Application Error Disclosure	Medium	240 (1,043.5%)
Content Security Policy (CSP) Header Not Set	Medium	5330 (23,173.9%)
Directory Browsing	Medium	9 (39.1%)
Missing Anti-clickjacking Header	Medium	5072 (22,052.2%)

Alert type	Risk	Count
Vulnerable JS Library	Medium	1 (4.3%)
Cookie No HttpOnly Flag	Low	33 (143.5%)
Cookie without SameSite Attribute	Low	48 (208.7%)
Information Disclosure - Debug Error Messages	Low	313 (1,360.9%)
Private IP Disclosure	Low	139 (604.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	164 (713.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5821 (25,308.7%)
Timestamp Disclosure - Unix	Low	3995 (17,369.6%)
X-Content-Type-Options Header Missing	Low	5155 (22,413.0%)
Authentication Request Identified	Informational	9 (39.1%)
Information Disclosure - Sensitive Information in URL	Informational	13 (56.5%)
Information Disclosure - Suspicious Comments	Informational	82 (356.5%)
Modern Web Application	Informational	5023 (21,839.1%)
Session Management Response Identified	Informational	14 (60.9%)
User Controllable Charset	Informational	2 (8.7%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	1640 (7,130.4%)
Total		23

Alerts

1. **Risk=High, Confidence=High (1)**
    1. **http://192.168.56.103 (1)**
        1. **Hash Disclosure - MD5 Crypt (1)**
            1. ▶ POST http://192.168.56.103/mutillidae/index.php?page=source-viewer.php
2. **Risk=High, Confidence=Medium (1)**
    1. **http://192.168.56.103 (1)**
        1. **Path Traversal (1)**

1. ▶ POST http://192.168.56.103/mutillidae/index.php?page=%2Fetc%2Fpasswd

3. **Risk=Medium, Confidence=High (1)**
    1. **http://192.168.56.103 (1)**
        1. **Content Security Policy (CSP) Header Not Set (1)**
            1. ▶ GET http://192.168.56.103/sitemap.xml
4. **Risk=Medium, Confidence=Medium (4)**
    1. **http://192.168.56.103 (4)**
        1. **Application Error Disclosure (1)**
            1. ▶ GET http://192.168.56.103/dav/
        2. **Directory Browsing (1)**
            1. ▶ GET http://192.168.56.103/dav/
        3. **Missing Anti-clickjacking Header (1)**
            1. ▶ GET http://192.168.56.103
        4. **Vulnerable JS Library (1)**
            1. ▶ GET http://192.168.56.103/mutillidae/javascript/ddsmoothmenu/jquery.min.js
5. **Risk=Medium, Confidence=Low (1)**
    1. **http://192.168.56.103 (1)**
        1. **Absence of Anti-CSRF Tokens (1)**
            1. ▶ GET http://192.168.56.103/dvwa/login.php
6. **Risk=Low, Confidence=High (1)**
    1. **http://192.168.56.103 (1)**
        1. **Server Leaks Version Information via "Server" HTTP Response Header Field (1)**
            1. ▶ GET http://192.168.56.103/robots.txt
7. **Risk=Low, Confidence=Medium (6)**
    1. **http://192.168.56.103 (6)**
        1. **Cookie No HttpOnly Flag (1)**

1. ▶ GET http://192.168.56.103/dvwa/

2. Cookie without SameSite Attribute **(1)**

   1. ▶ GET http://192.168.56.103/dvwa/

3. Information Disclosure - Debug Error Messages **(1)**

   1. ▶ GET http://192.168.56.103/mutillidae/

4. Private IP Disclosure **(1)**

   1. ▶ GET http://192.168.56.103/mutillidae/index.php?page=view-someones-blog.php

5. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) **(1)**

   1. ▶ GET http://192.168.56.103

6. X-Content-Type-Options Header Missing **(1)**

   1. ▶ GET http://192.168.56.103

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

   1. **http://192.168.56.103 (1)**

      1. Timestamp Disclosure - Unix **(1)**

         1. ▶ GET http://192.168.56.103/twiki/bin/view/Main/WebHome

9. **Risk=Informational, Confidence=High (1)**

   1. **http://192.168.56.103 (1)**

      1. Authentication Request Identified **(1)**

         1. ▶ POST http://192.168.56.103/dvwa/login.php

10. **Risk=Informational, Confidence=Medium (4)**

    1. **http://192.168.56.103 (4)**

       1. Information Disclosure - Sensitive Information in URL **(1)**

          1. ▶ GET http://192.168.56.103/phpMyAdmin/phpmyadmin.css.php?convcharset=utf-8&js_frame=right&lang=en-utf-8&nocache=2457687151&token=68df300a7ec8d17dd8a33d92f06caeef

       2. Information Disclosure - Suspicious Comments **(1)**

          1. ▶ GET http://192.168.56.103/mutillidae/

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

            1. ▶ GET http://192.168.56.103/twiki/TWikiHistory.html

        4. **Session Management Response Identified (1)**

            1. ▶ GET http://192.168.56.103/dvwa/

11. **Risk=Informational, Confidence=Low (2)**

    1. **http://192.168.56.103 (2)**

        1. **User Controllable Charset (1)**

            1. ▶ POST http://192.168.56.103/phpMyAdmin/index.php

        2. **User Controllable HTML Element Attribute (Potential XSS) (1)**

            1. ▶ GET http://192.168.56.103/mutillidae/index.php?page=user-info.php

Appendix

Alert types

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

1. **Hash Disclosure - MD5 Crypt**

Source	raised by a passive scanner (Hash Disclosure)
CWE ID	497
WASC ID	13
Reference	1. https://openwall.info/wiki/john/sample-hashes

2. **Path Traversal**

Source	raised by an active scanner (Path Traversal)
CWE ID	22
WASC ID	33
Reference	1. https://owasp.org/www-community/attacks/Path_Traversal 2. https://cwe.mitre.org/data/definitions/22.html

3. **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

4. **Application Error Disclosure**

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

5. **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/

6. **Directory Browsing**

Source	raised by a passive scanner (Directory Browsing)
CWE ID	548
WASC ID	16
Reference	1. https://cwe.mitre.org/data/definitions/548.html

7. **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

8. **Vulnerable JS Library**

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	1. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

9. **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

10. **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

11. **Information Disclosure - Debug Error Messages**

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	1295
WASC ID	13

12. **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

13. **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	497
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

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
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/

15. **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

16. **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

17. **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/

18. **Information Disclosure - Sensitive Information in URL**

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	598
WASC ID	13

19. **Information Disclosure - Suspicious Comments**

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

20. **Modern Web Application**

Source	raised by a passive scanner (Modern Web Application)

21. **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

22. **User Controllable Charset**

Source	raised by a passive scanner (User Controllable Charset)
CWE ID	20
WASC ID	20

23. **User Controllable HTML Element Attribute (Potential XSS)**

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html