ZAP by Checkmarx Scanning Report(DVWA)

Generated with ZAP on Tue 16 Sept 2025, at 14:21:32

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://127.0.0.1

(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%)	4 (18.2%)	0 (0.0%)	4 (18.2%)
	Medium	0 (0.0%)	1 (4.5%)	3 (13.6%)	2 (9.1%)	6 (27.3%)
	Low	0 (0.0%)	1 (4.5%)	5 (22.7%)	0 (0.0%)	6 (27.3%)
	Informational	0 (0.0%)	1 (4.5%)	4 (18.2%)	1 (4.5%)	6 (27.3%)
	Total	0 (0.0%)	3 (13.6%)	16 (72.7%)	3 (13.6%)	22 (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://127.0.0.1	4 (4)	6 (10)	6 (16)	6 (22)

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
Cross Site Scripting (Persistent)	High	2 (9.1%)
Cross Site Scripting (Reflected)	High	1 (4.5%)
Total		22

Alert type	Risk	Count
SQL Injection - MySQL	High	1 (4.5%)
SQL Injection - SQLite (Time Based)	High	1 (4.5%)
Absence of Anti-CSRF Tokens	Medium	3 (13.6%)
Application Error Disclosure	Medium	1 (4.5%)
Content Security Policy (CSP) Header Not Set	Medium	13 (59.1%)
Directory Browsing	Medium	1 (4.5%)
Missing Anti-clickjacking Header	Medium	13 (59.1%)
Parameter Tampering	Medium	4 (18.2%)
Cookie No HttpOnly Flag	Low	3 (13.6%)
Cookie without SameSite Attribute	Low	3 (13.6%)
Private IP Disclosure	Low	1 (4.5%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	14 (63.6%)
Total		22

Alert type	Risk	Count
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	18 (81.8%)
X-Content-Type-Options Header Missing	Low	17 (77.3%)
Authentication Request Identified	Informational	1 (4.5%)
Information Disclosure - Sensitive Information in URL	Informational	4 (18.2%)
Modern Web Application	Informational	11 (50.0%)
Session Management Response Identified	Informational	2 (9.1%)
User Agent Fuzzer	Informational	72 (327.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	10 (45.5%)
Total		22

Alerts

Risk=High, Confidence=Medium (4)

http://127.0.0.1 (4)

Cross Site Scripting (Persistent) (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/xss_s/

Cross Site Scripting (Reflected) (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=%3C%2Fpre%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Cpre%3E

SQL Injection - MySQL (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit

SQL Injection - SQLite (Time Based) (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=%27+OR+%271%27%3D%271&Submit=Submit

Risk=Medium, Confidence=High (1)

http://127.0.0.1 (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://127.0.0.1/dvwa/login.php

Risk=Medium, Confidence=Medium (3)

http://127.0.0.1 (3)

Application Error Disclosure (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271%27+--&Submit=Submit

Directory Browsing (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/

Missing Anti-clickjacking Header (1)

▶ GET http://127.0.0.1/dvwa/login.php

Risk=Medium, Confidence=Low (2)

http://127.0.0.1 (2)

Absence of Anti-CSRF Tokens (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/exec/

Parameter Tampering (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/csrf/?
=&password_conf=newpassword&Change=Change

Risk=Low, Confidence=High (1)

http://127.0.0.1 (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://127.0.0.1/dvwa/dvwa/css/login.css

Risk=Low, Confidence=Medium (5)

http://127.0.0.1 (5)

Cookie No HttpOnly Flag (1)

▶ GET http://127.0.0.1/dvwa/login.php

Cookie without SameSite Attribute (1)

▶ GET http://127.0.0.1/dvwa/login.php

Private IP Disclosure (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/xss_s/

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

▶ GET http://127.0.0.1/dvwa/login.php

X-Content-Type-Options Header Missing (1)

▶ GET http://127.0.0.1/dvwa/dvwa/css/login.css

Risk=Informational, Confidence=High (1)

http://127.0.0.1 (1)

Authentication Request Identified (1)

▶ POST http://127.0.0.1/dvwa/login.php

Risk=Informational, Confidence=Medium (4)

http://127.0.0.1 (4)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=newpassword&password_conf=newpassword&Change=Change

Modern Web Application (1)

▶ GET http://127.0.0.1/dvwa/index.php

Session Management Response Identified (1)

▶ GET http://127.0.0.1/dvwa/login.php

User Agent Fuzzer (1)

▶ GET http://127.0.0.1/dvwa/vulnerabilities

Risk=Informational, Confidence=Low (1)

http://127.0.0.1 (1)

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ POST http://127.0.0.1/dvwa/vulnerabilities/exec/

Appendix

Alert Types

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

Cross Site Scripting (Persistent)

Source	raised by an active scanner (Cross Site Scripting (Persistent))
CWE ID	79

WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ https://owasp.org/www-community/attacks/xss/ ▪ https://cwe.mitre.org/data/definitions/79.html

SQL Injection - MySQL

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

SQL Injection - SQLite (Time Based)

Source	raised by an active scanner (SQL Injection - SQLite (Time Based))

CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Absence of Anti-CSRF Tokens

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

Application Error Disclosure

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

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

Directory Browsing

Source	raised by an active scanner (Directory Browsing)
CWE ID	548
WASC ID	48
Reference	▪ https://httpd.apache.org/docs/mod/core.html#options

Missing Anti-clickjacking Header

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

Parameter Tampering

Source	raised by an active scanner (Parameter Tampering)
CWE ID	472
WASC ID	20

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)

CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Private IP Disclosure

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

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	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework ▪ https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

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

Authentication Request Identified

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

Information Disclosure - Sensitive Information in URL

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Session Management Response Identified

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

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg

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	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html