ZAP by Checkmarx Scanning Report

Generated with ZAP on Fri 26 Dec 2025, at 11:25:37

ZAP Version: 2.17.0

ZAP by Checkmarx

Contents

- About This Report
  - Report Parameters
- Summaries
  - Alert Counts by Risk and Confidence
  - Alert Counts by Site and Risk
  - Alert Counts by Alert Type
  - Insights
- Alerts
  - Risk=Medium, Confidence=High (2)
  - Risk=Medium, Confidence=Medium (3)

  - Risk=Low, Confidence=High (2)
  - Risk=Low, Confidence=Medium (2)
  - Risk=Informational, Confidence=High (1)
  - Risk=Informational, Confidence=Medium (5)
- Appendix
  - Alert Types

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `https://192.168.29.20`
- `http://192.168.29.20`

(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 (13.3%)	3 (20.0%)	0 (0.0%)	5 (33.3%)
	Low	0 (0.0%)	2 (13.3%)	2 (13.3%)	0 (0.0%)	4 (26.7%)
	Informational	0 (0.0%)	1 (6.7%)	5 (33.3%)	0 (0.0%)	6 (40.0%)
	Total	0 (0.0%)	5 (33.3%)	10 (66.7%)	0 (0.0%)	15 (100%)

	Confidence			
User Confirmed	High	Medium	Low	Total

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://192.168.29.20	0 (0)	1 (1)	0 (1)	0 (1)
	http://192.168.29.20	0 (0)	4 (4)	4 (8)	6 (14)

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	4 (26.7%)
Directory Browsing	Medium	3 (20.0%)
HTTP Only Site	Medium	1 (6.7%)
Hidden File Found	Medium	1 (6.7%)
Missing Anti-clickjacking Header	Medium	2 (13.3%)
Cookie without SameSite Attribute	Low	1 (6.7%)
In Page Banner Information Leak	Low	2 (13.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (33.3%)
X-Content-Type-Options Header Missing	Low	4 (26.7%)
Authentication Request Identified	Informational	1 (6.7%)
Total		15

Alert type	Risk	Count
Session Management Response Identified	Informational	2 (13.3%)
Tech Detected - Apache HTTP Server	Informational	1 (6.7%)
Tech Detected - PHP	Informational	1 (6.7%)
Tech Detected - Ubuntu	Informational	1 (6.7%)
User Agent Fuzzer	Informational	5 (33.3%)
Total		15

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	4
Info	Informational	http://192.168.29.20	Percentage of responses with status code 2xx	56 %

Level	Reason	Site	Description	Statistic
Info	Informational	http://192.168.29.20	Percentage of responses with status code 3xx	37 %
Info	Exceeded Low	http://192.168.29.20	Percentage of responses with status code 4xx	5 %
Info	Informational	http://192.168.29.20	Percentage of endpoints with content type image/png	7 %
Info	Informational	http://192.168.29.20	Percentage of endpoints with content type text/css	7 %
Info	Informational	http://192.168.29.20	Percentage of endpoints with content type text/html	76 %
Info	Informational	http://192.168.29.20	Percentage of endpoints with method GET	92 %
Info	Informational	http://192.168.29.20	Percentage of endpoints with method POST	7 %
Info	Informational	http://192.168.29.2	Count of total endpoints	13

Level	Reason	Site	Description	Statistic
		0		
Info	Informational	http://192.168.29.20	Percentage of slow responses	3 %
Info	Informational	https://192.168.29.20	Percentage of endpoints with method GET	100 %
Info	Informational	https://192.168.29.20	Count of total endpoints	1

Alerts

Risk=Medium, Confidence=High (2)

http://192.168.29.20 (2)

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

▶ GET http://192.168.29.20/DVWA/

Hidden File Found (1)

▶ GET http://192.168.29.20/DVWA/.git/config

Risk=Medium, Confidence=Medium (3)

https://192.168.29.20 (1)

HTTP Only Site (1)

▶ GET http://192.168.29.20/DVWA/

http://192.168.29.20 (2)

Directory Browsing (1)

▶ GET http://192.168.29.20/DVWA/dvwa/

Missing Anti-clickjacking Header (1)

▶ GET http://192.168.29.20/DVWA/

Risk=Low, Confidence=High (2)

http://192.168.29.20 (2)

In Page Banner Information Leak (1)

▶ GET http://192.168.29.20/robots.txt

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

▶ GET http://192.168.29.20/DVWA/

Risk=Low, Confidence=Medium (2)

http://192.168.29.20 (2)

Cookie without SameSite Attribute (1)

▶ GET http://192.168.29.20/DVWA/

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

▶ GET http://192.168.29.20/DVWA/

Risk=Informational, Confidence=High (1)

http://192.168.29.20 (1)

Authentication Request Identified (1)

▶ POST http://192.168.29.20/DVWA/login.php

Risk=Informational, Confidence=Medium (5)

http://192.168.29.20 (5)

Session Management Response Identified (1)

▶ GET http://192.168.29.20/DVWA/

Tech Detected - Apache HTTP Server (1)

▶ GET http://192.168.29.20/DVWA/

Tech Detected - PHP (1)

▶ GET http://192.168.29.20/DVWA/

Tech Detected - Ubuntu (1)

▶ `GET http://192.168.29.20/DVWA/`

User Agent Fuzzer (1)

▶ `POST http://192.168.29.20/DVWA/login.php`

Appendix

Alert Types

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

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/HTTP/Guides/CSP ▪ 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/current/mod/core.html#options

HTTP Only Site

Source	raised by an active scanner (HTTP Only Site)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html ▪ https://letsencrypt.org/

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)

CWE ID	538
WASC ID	13
Reference	- https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html - https://git-scm.com/docs/git-config

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/Reference/Headers/X-Frame-Options

Cookie without SameSite Attribute

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

In Page Banner Information Leak

Source	raised by a passive scanner (In Page Banner Information Leak)
CWE ID	497
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/

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/

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/

Tech Detected - Apache HTTP Server

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://httpd.apache.org/

Tech Detected - PHP

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://php.net

Tech Detected - Ubuntu

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	▪ https://www.ubuntu.com/server

User Agent Fuzzer

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