

# ZAP by Checkmarx

# Scanning Report

Generated with  ZAP on Fri 26 Dec 2025, at 15:06:17

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 \(1\)](#)
  - [Risk=Medium, Confidence=Medium \(2\)](#)

- [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%)	1 (7.7%)	2 (15.4%)	0 (0.0%)	3 (23.1%)
	Low	0 (0.0%)	2 (15.4%)	2 (15.4%)	0 (0.0%)	4 (30.8%)
	Informational	0 (0.0%)	1 (7.7%)	5 (38.5%)	0 (0.0%)	6 (46.2%)
	Total	0 (0.0%)	4 (30.8%)	9 (69.2%)	0 (0.0%)	13 (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				
Site		High	Medium	Informational
		(= High)	(>= Medium)	(>= Informational)
https://192.168.2.9.20		0	1	0
		(0)	(1)	(1)
http://192.168.2.9.20		0	2	4
		(0)	(2)	(6)

### 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
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	4 (30.8%)
<a href="#">HTTP Only Site</a>	Medium	1 (7.7%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	2 (15.4%)
<a href="#">Cookie without SameSite Attribute</a>	Low	1 (7.7%)
<a href="#">In Page Banner Information Leak</a>	Low	2 (15.4%)
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	5 (38.5%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	4 (30.8%)
<a href="#">Authentication Request Identified</a>	Informational	1 (7.7%)
<a href="#">Session Management Response Identified</a>	Informational	2 (15.4%)
<a href="#">Tech Detected - Apache HTTP Server</a>	Informational	1 (7.7%)
Total		13

Alert type	Risk	Count
<a href="#">Tech Detected - PHP</a>	Informational	1 (7.7%)
<a href="#">Tech Detected - Ubuntu</a>	Informational	1 (7.7%)
<a href="#">User Agent Fuzzer</a>	Informational	5 (38.5%)
Total		13

## 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	48 %
Info	Informational	http://192.168.29.20	Percentage of responses with status code 3xx	17 %
Info	Exceeded	http://	Percentage of	33 %

Level	Reason	Site	Description	Statistic
	d Low	192.16 8.29.2 0	responses with status code 4xx	
Info	Informati onal	http:// 192.16 8.29.2 0	Percentage of endpoints with content type image/png	11 %
Info	Informati onal	http:// 192.16 8.29.2 0	Percentage of endpoints with content type text/ css	11 %
Info	Informati onal	http:// 192.16 8.29.2 0	Percentage of endpoints with content type text/ html	77 %
Info	Informati onal	http:// 192.16 8.29.2 0	Percentage of endpoints with method GET	88 %
Info	Informati onal	http:// 192.16 8.29.2 0	Percentage of endpoints with method POST	11 %
Info	Informati onal	http:// 192.16 8.29.2 0	Count of total endpoints	9
Info	Informati onal	https:// 192.16 8.29.2 0	Percentage of endpoints with method GET	100 %

Level	Reason	Site	Description	Statistic
Info	Informational	https://192.168.29.20	Count of total endpoints	1

## Alerts

**Risk=Medium, Confidence=High (1)**

**[http://192.168.29.20 \(1\)](http://192.168.29.20)**

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

► GET <http://192.168.29.20/DVWA>

**Risk=Medium, Confidence=Medium (2)**

**[https://192.168.29.20 \(1\)](https://192.168.29.20)**

**HTTP Only Site (1)**

► GET <http://192.168.29.20/DVWA/>



<http://192.168.29.20> (1)

**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)**

- ▶ GET <http://192.168.29.20/DVWA/>

## Appendix

## Alert Types

---

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

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

<b>Source</b>	raised by a passive scanner ( <a href="#">Content Security Policy (CSP) Header Not Set</a> )
<b>CWE ID</b>	<a href="#">693</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP">https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP</a></li><li>▪ <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a></li><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a></li><li>▪ <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a></li><li>▪ <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a></li><li>▪ <a href="https://content-security-policy.com/">https://content-security-policy.com/</a></li></ul>

### HTTP Only Site

<b>Source</b>	raised by an active scanner ( <a href="#">HTTP Only Site</a> )
<b>CWE ID</b>	<a href="#">311</a>

<b>WASC ID</b>	4
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html</a></li><li>▪ <a href="https://letsencrypt.org/">https://letsencrypt.org/</a></li></ul>

### Missing Anti-clickjacking Header

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

### Cookie without SameSite Attribute

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

### In Page Banner Information Leak

<b>Source</b>	raised by a passive scanner ( <a href="#">In Page Banner Information Leak</a> )
---------------	---

<b>CWE ID</b>	<a href="#">497</a>
<b>WASC ID</b>	13
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/</a></li></ul>

### Server Leaks Version Information via "Server" HTTP Response Header Field

<b>Source</b>	raised by a passive scanner ( <a href="#">HTTP Server Response Header</a> )
<b>CWE ID</b>	<a href="#">497</a>
<b>WASC ID</b>	13
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a></li><li>▪ <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a></li><li>▪ <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a></li></ul>

### X-Content-Type-Options Header Missing

<b>Source</b>	raised by a passive scanner ( <a href="#">X-Content-Type-Options Header Missing</a> )
<b>CWE ID</b>	<a href="#">693</a>
<b>WASC ID</b>	15

**Reference**

- [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941\(v=vs.85\)](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**

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

### Tech Detected - Ubuntu

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

### User Agent Fuzzer

<b>Source</b>	raised by an active scanner ( <a href="#">User Agent Fuzzer</a> )
<b>Reference</b>	▪ <a href="https://owasp.org/wstg">https://owasp.org/wstg</a>