

# ZAP Scanning Report

Generated with  ZAP

ZAP Version: 2.15.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

## Contents

- [About this report](#)
  - [Report parameters](#)
- [Summaries](#)
  - [Alert counts by risk and confidence](#)
  - [Alert counts by site and risk](#)
  - [Alert counts by alert type](#)
- [Alerts](#)
  - [Risk=Medium, Confidence=High \(1\)](#)
  - [Risk=Medium, Confidence=Medium \(1\)](#)
  - [Risk=Medium, Confidence=Low \(1\)](#)
  - [Risk=Low, Confidence=High \(1\)](#)
  - [Risk=Low, Confidence=Medium \(2\)](#)

- [Risk=Informational, Confidence=Medium \(1\)](#)
- [Risk=Informational, Confidence=Low \(4\)](#)
- [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:

- <http://testphp.vulnweb.com>

(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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
	Informational	0 (0.0%)	0 (0.0%)	1 (9.1%)	4 (36.4%)	5 (45.5%)
	1					
Total		0 (0.0%)	2 (18.2%)	4 (36.4%)	5 (45.5%)	11 (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.)

Site	Risk				Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)	
<a href="http://testphp.vulnweb.com">http://testphp.vulnweb.com</a>	0	3	3	5	
	(0)	(3)	(6)	(11)	

### 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="#">Absence of Anti-CSRF Tokens</a>	Medium	39 (354.5%)
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	47 (427.3%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	43 (390.9%)
Total		11

Alert type	Risk	Count
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	61 (554.5%)
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	73 (663.6%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	67 (609.1%)
<a href="#">Authentication Request Identified</a>	Informational	1 (9.1%)
<a href="#">Charset Mismatch (Header Versus Meta Content-Type Charset)</a>	Informational	30 (272.7%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	1 (9.1%)
<a href="#">Modern Web Application</a>	Informational	9 (81.8%)
<a href="#">User Controllable HTML Element Attribute (Potential XSS)</a>	Informational	3 (27.3%)
Total		11

## Alerts

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

<http://testphp.vulnweb.com> (1)

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

► GET http://testphp.vulnweb.com/sitemap.xml

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

http://testphp.vulnweb.com (1)

**Missing Anti-clickjacking Header (1)**

► GET http://testphp.vulnweb.com/login.php

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

http://testphp.vulnweb.com (1)

**Absence of Anti-CSRF Tokens (1)**

► GET http://testphp.vulnweb.com/login.php

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

http://testphp.vulnweb.com (1)

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

► GET http://testphp.vulnweb.com/sitemap.xml

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

http://testphp.vulnweb.com (2)

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

► GET http://testphp.vulnweb.com/login.php

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

► GET http://testphp.vulnweb.com/login.php

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

http://testphp.vulnweb.com (1)

### **Modern Web Application (1)**

► GET http://testphp.vulnweb.com/artists.php

**Risk=Informational, Confidence=Low (4)**

http://testphp.vulnweb.com (4)

### **Authentication Request Identified (1)**

► POST http://testphp.vulnweb.com/secured/newuser.php

### **Charset Mismatch (Header Versus Meta Content-Type Charset) (1)**

► GET http://testphp.vulnweb.com/login.php

### **Information Disclosure - Suspicious Comments (1)**

► GET http://testphp.vulnweb.com/AJAX/index.php

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

► POST http://testphp.vulnweb.com/search.php?test=query

# Appendix

## Alert types

---

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

### Absence of Anti-CSRF Tokens

Source	raised by a passive scanner ( <a href="#">Absence of Anti-CSRF Tokens</a> )
CWE ID	<a href="#">352</a>
WASC ID	9
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</a></li><li>▪ <a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a></li></ul>

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

Source	raised by a passive scanner ( <a href="#">Content Security Policy (CSP) Header Not Set</a> )
CWE ID	<a href="#">693</a>
WASC ID	15



**Reference**

- [https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\\_Content\\_Security\\_Policy](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://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/>

**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/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>

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

<b>Source</b>	raised by a passive scanner ( <a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a> )
---------------	---

<b>CWE ID</b>	<a href="#">200</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/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a></li><li>▪ <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</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="#">200</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
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="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)</a></li><li>▪ <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a></li></ul>

### Authentication Request Identified

<b>Source</b>	raised by a passive scanner ( <a href="#">Authentication Request Identified</a> )
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a></li></ul>

### Charset Mismatch (Header Versus Meta Content-Type Charset)

<b>Source</b>	raised by a passive scanner ( <a href="#">Charset Mismatch</a> )
<b>CWE ID</b>	<a href="#">436</a>
<b>WASC ID</b>	15
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection">https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection</a></li></ul>

### Information Disclosure - Suspicious Comments

<b>Source</b>	raised by a passive scanner ( <a href="#">Information Disclosure - Suspicious Comments</a> )
---------------	--

**CWE ID** [200](#)

**WASC ID** 13

## Modern Web Application

**Source** raised by a passive scanner ([Modern Web Application](#))

## 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](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html)