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://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

Summa/:!es

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	H:tgh	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%)
	Lox	0 (0.0%)	1 (9.1%)	2 (18.2%)	0 (0.0%)	3 (27.3%)
	Informationa 1	0 (0.0%)	0 (0.0%)	1 (9.1%)	4 (36.4%)	5 (45.5%)
	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.)

	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
http://testphp.vulnweb.com	0 (0)	3 (3)	3 (6)	5 (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.)

Absence of Anti-CSRF Tokens	Medium	39 (354.5%)
Content Security Policy (CSP) Header Not Set	Nedium	47 (427.3%)
Missing Anti-clickjacking Header	Medium	43 (390.9%)
Total		11

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	61 (554.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	73 (663. 6%)
X-Content-Type-Options Header Missing	Low	67 (609.1%)
Authentication Request Identified	Informational	1 (9.1%)
Charset Mismatch (Header Versus Nleta Content-Type Charset)	Informational	30 (272.7%)
Information Disclosure - Suspicious Comments	Informational	1 (9.1%)
Nlodern Web Application	Informational	9 (81 .8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (27.3%)
Total		11

Aems

Risk-Ned1um, Confidence=H1gh (1)

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

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

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

Risk=Hed1um, Confidence=Hedium (1)

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

Missing Anti-clickjacking Header (1)

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

Risk-Ned1um, 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)

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

Risk=Low, Confidence=Ned1um (2)

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

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

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

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

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

Risk=Informat1ona1, Confidence=Ned1um (1)

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

Modern Web Application (1)

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

Risk- Informat1ona1, Confidences Low (4)

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

Authentication Request Identified (1)

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)

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

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

```
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

raised by a passive scanner (Absence of Anti-CSRF Tokens)

352

9

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://cwe. mitre.org/data/definitions/352.html

Content Security Policy (CSP) Header Not Set

raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

693

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/

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

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	200
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	200
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/

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

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	• https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)

200

13

Modern Web Application

raised by a passive scanner (Modern Web Application)

User Controllable HTML Element Attribute (Potential XSS)

raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))

20

20

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