ZAP Scanning Report

Generated with ZAP on Sun 29 May 2022, at 11:26:45

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=High, Confidence=Medium (2)
  - Risk=Medium, Confidence=High (1)
  - Risk=Medium, Confidence=Medium (2)
  - Risk=Medium, Confidence=Low (1)
  - Risk=Low, Confidence=Medium (4)
  - Risk=Low, Confidence=Low (1)
  - Risk=Informational, Confidence=Medium (1)
  - Risk=Informational, Confidence=Low (1)
- 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`
- `http://testfire.net`

(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%)	2 (15.4%)	0 (0.0%)	2 (15.4%)
	Medium	0 (0.0%)	1 (7.7%)	2 (15.4%)	1 (7.7%)	4 (30.8%)
	Low	0 (0.0%)	0 (0.0%)	4 (30.8%)	1 (7.7%)	5 (38.5%)
	Informational	0 (0.0%)	0 (0.0%)	1 (7.7%)	1 (7.7%)	2 (15.4%)
	Total	0 (0.0%)	1 (7.7%)	9 (69.2%)	3 (23.1%)	13 (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)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://testphp.vulnweb.com	1 (1)	1 (2)	1 (3)	1 (4)
	http://testfire.net	1 (1)	3 (4)	4 (8)	1 (9)

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 (Reflected)	High	18 (138.5%)
SQL Injection	High	7 (53.8%)
.htaccess Information Leak	Medium	7 (53.8%)
Absence of Anti-CSRF Tokens	Medium	181 (1,392.3%)
Content Security Policy (CSP) Header Not Set	Medium	188 (1,446.2%)
Total		13

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	108 (830.8%)
Cookie without SameSite Attribute	Low	3 (23.1%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (7.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	63 (484.6%)
Timestamp Disclosure - Unix	Low	112 (861.5%)
X-Content-Type-Options Header Missing	Low	169 (1,300.0%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	32 (246.2%)
Information Disclosure - Suspicious Comments	Informational	16 (123.1%)
Total		13

Alerts

Risk=High, Confidence=Medium (2)

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

SQL Injection (1)

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

http://testfire.net (1)

Cross Site Scripting (Reflected) (1)

▶ POST http://testfire.net/sendFeedback

Risk=Medium, Confidence=High (1)

http://testfire.net (1)

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

▶ GET http://testfire.net/

Risk=Medium, Confidence=Medium (2)

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

.htaccess Information Leak (1)

▶ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess

http://testfire.net (1)

Missing Anti-clickjacking Header (1)

▶ GET http://testfire.net/

Risk=Medium, Confidence=Low (1)

http://testfire.net (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://testfire.net/

Risk=Low, Confidence=Medium (4)

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

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

▶ GET http://testphp.vulnweb.com/

http://testfire.net (3)

Cookie without SameSite Attribute (1)

▶ GET http://testfire.net/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://testfire.net/index.jsp?content=personal_investments.htm

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

▶ GET http://testfire.net/

Risk=Low, Confidence=Low (1)

http://testfire.net (1)

Timestamp Disclosure - Unix (1)

▶ GET http://testfire.net/index.jsp?content=inside_press.htm

Risk=Informational, Confidence=Medium (1)

http://testfire.net (1)

Information Disclosure - Suspicious Comments (1)

▶ `GET http://testfire.net/login.jsp`

Risk=Informational, Confidence=Low (1)

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

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

▶ `GET http://testphp.vulnweb.com/`

Appendix

Alert types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

SQL Injection

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

.htaccess Information Leak

Source	raised by an active scanner (.htaccess Information Leak)
CWE ID	94
WASC ID	14
Reference	▪ http://www.htaccess-guide.com/

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

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 ▪ http://www.w3.org/TR/CSP/ ▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html ▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ ▪ http://caniuse.com/#feat=contentsecuritypolicy ▪ http://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

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

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

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	- http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx - http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13

Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Charset Mismatch (Header Versus Meta Content-Type Charset)

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	▪ http://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)
CWE ID	200
WASC ID	13