ZAP Scanning Report

Generated with The ZAP logoZAP on Mon 13 May 2024, at 01:45:01

ZAP Version: 2.14.0

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

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%)	1 (8.3%)	0 (0.0%)	0 (0.0%)	1 (8.3%)
	Medium	0 (0.0%)	1 (8.3%)	1 (8.3%)	1 (8.3%)	3 (25.0%)
	Low	0 (0.0%)	1 (8.3%)	2 (16.7%)	0 (0.0%)	3 (25.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (8.3%)	4 (33.3%)	5 (41.7%)
	Total	0 (0.0%)	3 (25.0%)	4 (33.3%)	5 (41.7%)	12 (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)
Site http://testphp.vulnweb.com	1 (1)	3 (4)	3 (7)	5 (12)

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 (DOM Based)	High	1 (8.3%)
Absence of Anti-CSRF Tokens	Medium	40 (333.3%)
Content Security Policy (CSP) Header Not Set	Medium	48 (400.0%)
Missing Anti-clickjacking Header	Medium	44 (366.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	62 (516.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	74 (616.7%)
X-Content-Type-Options Header Missing	Low	68 (566.7%)
Authentication Request Identified	Informational	1 (8.3%)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	31 (258.3%)
Information Disclosure - Suspicious Comments	Informational	1 (8.3%)
Modern Web Application	Informational	9 (75.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (25.0%)
Total		12

Alerts

1. Risk=High, Confidence=High (1)
    1. http://testphp.vulnweb.com (1)
        1. Cross Site Scripting (DOM Based) (1)
            1. ▶ GET http://testphp.vulnweb.com/#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
2. Risk=Medium, Confidence=High (1)
    1. http://testphp.vulnweb.com (1)
        1. Content Security Policy (CSP) Header Not Set (1)
            1. ▶ GET http://testphp.vulnweb.com/
3. Risk=Medium, Confidence=Medium (1)
    1. http://testphp.vulnweb.com (1)
        1. Missing Anti-clickjacking Header (1)
            1. ▶ GET http://testphp.vulnweb.com/
4. Risk=Medium, Confidence=Low (1)
    1. http://testphp.vulnweb.com (1)
        1. Absence of Anti-CSRF Tokens (1)
            1. ▶ GET http://testphp.vulnweb.com/
5. Risk=Low, Confidence=High (1)
    1. http://testphp.vulnweb.com (1)
        1. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
            1. ▶ GET http://testphp.vulnweb.com/
6. Risk=Low, Confidence=Medium (2)
    1. http://testphp.vulnweb.com (2)
        1. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)
            1. ▶ GET http://testphp.vulnweb.com/
        2. X-Content-Type-Options Header Missing (1)
            1. ▶ GET http://testphp.vulnweb.com/
7. Risk=Informational, Confidence=Medium (1)
    1. http://testphp.vulnweb.com (1)
        1. Modern Web Application (1)
            1. ▶ GET http://testphp.vulnweb.com/artists.php
8. Risk=Informational, Confidence=Low (4)
    1. http://testphp.vulnweb.com (4)
        1. Authentication Request Identified (1)
            1. ▶ POST http://testphp.vulnweb.com/secured/newuser.php
        2. Charset Mismatch (Header Versus Meta Content-Type Charset) (1)
            1. ▶ GET http://testphp.vulnweb.com/
        3. Information Disclosure - Suspicious Comments (1)
            1. ▶ GET http://testphp.vulnweb.com/AJAX/index.php
        4. 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.

1. **Cross Site Scripting (DOM Based)**

Source	raised by an active scanner (Cross Site Scripting (DOM Based))
CWE ID	79
WASC ID	8
Reference	1. http://projects.webappsec.org/Cross-Site-Scripting 2. https://cwe.mitre.org/data/definitions/79.html

2. **Absence of Anti-CSRF Tokens**

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	1. http://projects.webappsec.org/Cross-Site-Request-Forgery 2. https://cwe.mitre.org/data/definitions/352.html

3. **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	1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy 3. http://www.w3.org/TR/CSP/ 4. http://w3c.github.io/webappsec/specs/content-security-policy/csp-speci 5. http://www.html5rocks.com/en/tutorials/security/content-security-polic 6. http://caniuse.com/#feat=contentsecuritypolicy 7. http://content-security-policy.com/

4. **Missing Anti-clickjacking Header**

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

5. **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	1. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx 2. http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

6. **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	1. http://httpd.apache.org/docs/current/mod/core.html#servertokens 2. http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 3. http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx 4. http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

7. **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	1. http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 2. https://owasp.org/www-community/Security_Headers

8. **Authentication Request Identified**

Source	raised by a passive scanner (Authentication Request Identified)
Reference	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

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

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	1. http://code.google.com/p/browsersec/wiki/Part2#Character_set_handlin

10. **Information Disclosure - Suspicious Comments**

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13

11. **Modern Web Application**

Source	raised by a passive scanner (Modern Web Application)

12. **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	1. http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute