ZAP Scanning Report DMZ

Generated with The ZAP logoZAP on Sat 29 Apr 2023, at 23:46:56

Contents

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://firefox.settings.services.mozilla.com
- https://shavar.services.mozilla.com
- https://location.services.mozilla.com
- http://www.seclab.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%)	1 (3.8%)	2 (7.7%)	0 (0.0%)	3 (11.5%)
	Medium	0 (0.0%)	2 (7.7%)	6 (23.1%)	1 (3.8%)	9 (34.6%)
	Low	0 (0.0%)	1 (3.8%)	6 (23.1%)	1 (3.8%)	8 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	4 (15.4%)	2 (7.7%)	6 (23.1%)
	Total	0 (0.0%)	4 (15.4%)	18 (69.2%)	4 (15.4%)	26 (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://www.seclab.net**	3 (3)	9 (12)	8 (20)	6 (26)

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	2 (7.7%)
Total		26

Alert type	Risk	Count
Cross Site Scripting (Reflected)	High	17 (65.4%)
External Redirect	High	2 (7.7%)
.htaccess Information Leak	Medium	2 (7.7%)
Absence of Anti-CSRF Tokens	Medium	124 (476.9%)
Application Error Disclosure	Medium	9 (34.6%)
Content Security Policy (CSP) Header Not Set	Medium	164 (630.8%)
Directory Browsing - Apache 2	Medium	5 (19.2%)
Hidden File Found	Medium	1 (3.8%)
Missing Anti-clickjacking Header	Medium	112 (430.8%)
Vulnerable JS Library	Medium	1 (3.8%)
XSLT Injection	Medium	4 (15.4%)
Cookie No HttpOnly Flag	Low	10 (38.5%)
Cookie without SameSite Attribute	Low	20 (76.9%)
Information Disclosure - Debug Error Messages	Low	8 (30.8%)
Private IP Disclosure	Low	6 (23.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	92 (353.8%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	224 (861.5%)
Timestamp Disclosure - Unix	Low	38 (146.2%)
X-Content-Type-Options Header Missing	Low	163 (626.9%)
Information Disclosure - Sensitive Information in URL	Informational	8 (30.8%)
Information Disclosure - Suspicious Comments	Informational	57 (219.2%)
Modern Web Application	Informational	116 (446.2%)
User Agent Fuzzer	Informational	482 (1,853.8%)
User Controllable Charset	Informational	2 (7.7%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	50 (192.3%)
Total		26

Alerts

1. **Risk=High, Confidence=High (1)**
    1. **http://www.seclab.net (1)**
        1. **Cross Site Scripting (DOM Based) (1)**
            1. ▶ POST http://www.seclab.net/mutillidae/index.php?page=set-background-color.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
2. **Risk=High, Confidence=Medium (2)**
    1. **http://www.seclab.net (2)**
        1. **Cross Site Scripting (Reflected) (1)**
            1. ▶ POST http://www.seclab.net/mutillidae/index.php?page=javascript%3Aalert%281%29%3B
        2. **External Redirect (1)**
            1. ▶ GET http://www.seclab.net/mutillidae/index.php?forwardurl=http%3A%2F%2F150811784445149171.owasp.org&page=redirectandlog.php
3. **Risk=Medium, Confidence=High (2)**
    1. **http://www.seclab.net (2)**
        1. **Content Security Policy (CSP) Header Not Set (1)**
            1. ▶ GET http://www.seclab.net/robots.txt
        2. **Hidden File Found (1)**
            1. ▶ GET http://www.seclab.net/phpinfo.php
4. **Risk=Medium, Confidence=Medium (6)**
    1. **http://www.seclab.net (6)**
        1. **.htaccess Information Leak (1)**
            1. ▶ GET http://www.seclab.net/twiki/bin/attach/Main/.htaccess
        2. **Application Error Disclosure (1)**
            1. ▶ GET http://www.seclab.net/dav/
        3. **Directory Browsing - Apache 2 (1)**
            1. ▶ GET http://www.seclab.net/dav/

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

            1. ▶ GET http://www.seclab.net

        5. **Vulnerable JS Library (1)**

            1. ▶ GET http://www.seclab.net/mutillidae/javascript/ddsmoothmenu/jquery.min.js

        6. **XSLT Injection (1)**

            1. ▶ POST http://www.seclab.net/mutillidae/index.php?page=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Fwww.seclab.net%3A22%27%29%22%2F%3E

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

    1. **http://www.seclab.net (1)**

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

            1. ▶ GET http://www.seclab.net/phpMyAdmin/

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

    1. **http://www.seclab.net (1)**

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

            1. ▶ GET http://www.seclab.net/sitemap.xml

7. **Risk=Low, Confidence=Medium (6)**

    1. **http://www.seclab.net (6)**

        1. **Cookie No HttpOnly Flag (1)**

            1. ▶ GET http://www.seclab.net/dvwa/

        2. **Cookie without SameSite Attribute (1)**

            1. ▶ GET http://www.seclab.net/phpMyAdmin/

        3. **Information Disclosure - Debug Error Messages (1)**

            1. ▶ GET http://www.seclab.net/mutillidae/

        4. **Private IP Disclosure (1)**

            1. ▶ GET http://www.seclab.net/mutillidae/index.php?page=view-someones-blog.php

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

            1. ▶ GET http://www.seclab.net

        6. **X-Content-Type-Options Header Missing (1)**

      1. ▶ GET http://www.seclab.net

8. **Risk=Low, Confidence=Low (1)**

   1. **http://www.seclab.net (1)**

      1. **Timestamp Disclosure - Unix (1)**

         1. ▶ GET http://www.seclab.net/twiki/bin/view/Main/WebHome

9. **Risk=Informational, Confidence=Medium (4)**

   1. **http://www.seclab.net (4)**

      1. **Information Disclosure - Sensitive Information in URL (1)**

         1. ▶ GET http://www.seclab.net/phpMyAdmin/phpmyadmin.css.php?convcharset=utf-8&js_frame=right&lang=en-utf-8&nocache=2457687151&token=73003436b893777d5db2fb94af38cca7

      2. **Information Disclosure - Suspicious Comments (1)**

         1. ▶ GET http://www.seclab.net/mutillidae/

      3. **Modern Web Application (1)**

         1. ▶ GET http://www.seclab.net/phpMyAdmin/

      4. **User Agent Fuzzer (1)**

         1. ▶ POST http://www.seclab.net/mutillidae/index.php?page=view-someones-blog.php

10. **Risk=Informational, Confidence=Low (2)**

    1. **http://www.seclab.net (2)**

       1. **User Controllable Charset (1)**

          1. ▶ POST http://www.seclab.net/phpMyAdmin/index.php

       2. **User Controllable HTML Element Attribute (Potential XSS) (1)**

          1. ▶ POST http://www.seclab.net/phpMyAdmin/index.php

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 (plugin ID: 40026)

CWE ID	79
WASC ID	8
Reference	1. http://projects.webappsec.org/Cross-Site-Scripting 2. http://cwe.mitre.org/data/definitions/79.html

2. **Cross Site Scripting (Reflected)**

Source	raised by an active scanner (plugin ID: 40012)
CWE ID	79
WASC ID	8
Reference	1. http://projects.webappsec.org/Cross-Site-Scripting 2. http://cwe.mitre.org/data/definitions/79.html

3. **External Redirect**

Source	raised by an active scanner (plugin ID: 20019)
CWE ID	601
WASC ID	38
Reference	1. http://projects.webappsec.org/URL-Redirector-Abuse 2. http://cwe.mitre.org/data/definitions/601.html

4. **.htaccess Information Leak**

Source	raised by an active scanner (plugin ID: 40032)
CWE ID	94
WASC ID	14
Reference	1. http://www.htaccess-guide.com/

5. **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. http://cwe.mitre.org/data/definitions/352.html

6. **Application Error Disclosure**

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

7. **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_Cheat_Sheet.html 3. http://www.w3.org/TR/CSP/ 4. http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html

5. http://www.html5rocks.com/en/tutorials/security/content-security-policy/
6. http://caniuse.com/#feat=contentsecuritypolicy
7. http://content-security-policy.com/

8. **Directory Browsing - Apache 2**

Source	raised by a passive scanner (Directory Browsing)
CWE ID	548
WASC ID	16
Reference	1. https://cwe.mitre.org/data/definitions/548.html

9. **Hidden File Found**

Source	raised by an active scanner (plugin ID: 40035)
CWE ID	538
WASC ID	13
Reference	1. https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html 2. https://www.php.net/manual/en/function.phpinfo.php

10. **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

11. **Vulnerable JS Library**

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	1. https://nvd.nist.gov/vuln/detail/CVE-2012-6708 2. http://research.insecurelabs.org/jquery/test/ 3. https://bugs.jquery.com/ticket/9521 4. http://bugs.jquery.com/ticket/11290 5. https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ 6. https://nvd.nist.gov/vuln/detail/CVE-2019-11358 7. https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b 8. https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ 9. https://nvd.nist.gov/vuln/detail/CVE-2011-4969

12. **XSLT Injection**

Source	raised by an active scanner (plugin ID: 90017)
CWE ID	91
WASC ID	23
Reference	1. https://www.contextis.com/blog/xslt-server-side-injection-attacks

13. **Cookie No HttpOnly Flag**

Source	raised by a passive scanner (Cookie No HttpOnly Flag)

CWE ID	1004
WASC ID	13
Reference	1. https://owasp.org/www-community/HttpOnly

14. **Cookie without SameSite Attribute**

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	1. https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

15. **Information Disclosure - Debug Error Messages**

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

16. **Private IP Disclosure**

Source	raised by a passive scanner (Private IP Disclosure)
CWE ID	200
WASC ID	13
Reference	1. https://tools.ietf.org/html/rfc1918

17. **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

18. **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

19. **Timestamp Disclosure - Unix**

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	200
WASC ID	13
Reference	1. http://projects.webappsec.org/w/page/13246936/Information%20Leakage

20. **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

21. **Information Disclosure - Sensitive Information in URL**

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

22. **Information Disclosure - Suspicious Comments**

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

23. **Modern Web Application**

Source	raised by a passive scanner (Modern Web Application)

24. **User Agent Fuzzer**

Source	raised by an active scanner (plugin ID: 10104)
Reference	1. https://owasp.org/wstg

25. **User Controllable Charset**

Source	raised by a passive scanner (User Controllable Charset)
CWE ID	20
WASC ID	20

26. **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