ZAP Scanning Report Outside Network

Generated with ZAP on Sun 30 Apr 2023, at 00:08:13

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://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 (3.0%)	13 (39.4%)	0 (0.0%)	14 (42.4%)
	Medium	0 (0.0%)	1 (3.0%)	4 (12.1%)	1 (3.0%)	6 (18.2%)
	Low	0 (0.0%)	1 (3.0%)	6 (18.2%)	1 (3.0%)	8 (24.2%)
	Informational	0 (0.0%)	0 (0.0%)	3 (9.1%)	2 (6.1%)	5 (15.2%)
	Total	0 (0.0%)	3 (9.1%)	26 (78.8%)	4 (12.1%)	33 (100%)

	Confidence				
	User Confirmed	High	Medium	Low	Total

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	14 (14)	6 (20)	8 (28)	5 (33)

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 (6.1%)
Cross Site Scripting (Persistent)	High	5 (15.2%)
Cross Site Scripting (Reflected)	High	1177 (3,566.7%)
External Redirect	High	295 (893.9%)
Path Traversal	High	9 (27.3%)
Remote Code Execution - CVE-2012-1823	High	28 (84.8%)
SQL Injection	High	233 (706.1%)
SQL Injection - Hypersonic SQL - Time Based	High	4 (12.1%)
SQL Injection - MySQL	High	14 (42.4%)
SQL Injection - Oracle - Time Based	High	4 (12.1%)
Total		33

Alert type	Risk	Count
SQL Injection - PostgreSQL - Time Based	High	3 (9.1%)
SQL Injection - SQLite	High	2 (6.1%)
Server Side Include	High	1 (3.0%)
Source Code Disclosure - CVE-2012-1823	High	9 (27.3%)
Absence of Anti-CSRF Tokens	Medium	6092 (18,460.6%)
Application Error Disclosure	Medium	225 (681.8%)
Content Security Policy (CSP) Header Not Set	Medium	4652 (14,097.0%)
Directory Browsing - Apache 2	Medium	9 (27.3%)
Missing Anti-clickjacking Header	Medium	4553 (13,797.0%)
Vulnerable JS Library	Medium	1 (3.0%)
Cookie No HttpOnly Flag	Low	21 (63.6%)
Cookie without SameSite Attribute	Low	32 (97.0%)
Total		33

Alert type	Risk	Count
Information Disclosure - Debug Error Messages	Low	308 (933.3%)
Private IP Disclosure	Low	136 (412.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	143 (433.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5094 (15,436.4%)
Timestamp Disclosure - Unix	Low	1075 (3,257.6%)
X-Content-Type-Options Header Missing	Low	4640 (14,060.6%)
Information Disclosure - Sensitive Information in URL	Informational	9 (27.3%)
Information Disclosure - Suspicious Comments	Informational	81 (245.5%)
Modern Web Application	Informational	4522 (13,703.0%)
User Controllable Charset	Informational	2 (6.1%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	1594 (4,830.3%)
Total		33

Alerts

Risk=High, Confidence=High (1)

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

Cross Site Scripting (DOM Based) (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
```

Risk=High, Confidence=Medium (13)

http://www.seclab.net (13)

Cross Site Scripting (Persistent) (1)

```
▶ GET http://www.seclab.net/twiki/bin/view
/Main/WebHome?unlock=on
```

Cross Site Scripting (Reflected) (1)

```
▶ POST http://www.seclab.net/mutillidae
/index.php?page=add-to-your-blog.php
```

External Redirect (1)

```
▶ POST http://www.seclab.net/twiki/bin/passwd
/Main/WebHome
```

Path Traversal (1)

▸ GET http://www.seclab.net/twiki/bin/search/Know/?bookview=on&casesensitive=on&limit=all&nosearch=on&nosummary=on&nototal=on&order=modified&regex=on&reverse=on&scope=text&search=c%3A%2F&web=all

Remote Code Execution - CVE-2012-1823 (1)

▸ POST http://www.seclab.net/dvwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input

SQL Injection (1)

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

SQL Injection - Hypersonic SQL - Time Based (1)

▸ POST http://www.seclab.net/mutillidae/index.php?page=register.php

SQL Injection - MySQL (1)

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

SQL Injection - Oracle - Time Based (1)

▸ POST http://www.seclab.net/mutillidae/index.php?page=register.php

SQL Injection - PostgreSQL - Time Based (1)

▸ POST http://www.seclab.net/mutillidae/index.php?page=register.php

SQL Injection - SQLite (1)

▸ GET http://www.seclab.net/twiki/bin/search

/Know/?bookview=on&scope=text&search=ZAP&web=on

Server Side Include (1)

▸ GET http://www.seclab.net/twiki/bin/rdiff/TWiki/TWikiInstallationGuide?rev1=1.52&rev2=%3C%21--%23EXEC+cmd%3D%22ls+%2F%22--%3E

Source Code Disclosure - CVE-2012-1823 (1)

▸ GET http://www.seclab.net/dvwa/login.php?-s

Risk=Medium, Confidence=High (1)

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

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

▸ GET http://www.seclab.net

Risk=Medium, Confidence=Medium (4)

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

Application Error Disclosure (1)

▸ GET http://www.seclab.net/dav/

Directory Browsing - Apache 2 (1)

▸ GET http://www.seclab.net/dav/

Missing Anti-clickjacking Header (1)

▸ GET http://www.seclab.net

Vulnerable JS Library (1)

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

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

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

Risk=Low, Confidence=High (1)

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

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

▶ GET http://www.seclab.net

Risk=Low, Confidence=Medium (6)

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

Cookie No HttpOnly Flag (1)

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

Cookie without SameSite Attribute (1)

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

Information Disclosure - Debug Error Messages (1)

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

Private IP Disclosure (1)

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

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

▶ GET http://www.seclab.net

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

▶ GET http://www.seclab.net

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

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

Risk=Informational, Confidence=Medium (3)

http://www.seclab.net (3)

Information Disclosure - Sensitive Information in URL (1)

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

token=2d7a8956744ed1ed5c5c47eb994e8946

Information Disclosure - Suspicious Comments (1)

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

Modern Web Application (1)

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

Risk=Informational, Confidence=Low (2)

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

User Controllable Charset (1)

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

User Controllable HTML Element Attribute (Potential XSS) (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.

Cross Site Scripting (DOM Based)

Source raised by an active scanner (plugin ID: 40026)

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

Cross Site Scripting (Persistent)

Source	raised by an active scanner (plugin ID: 40014)
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

Cross Site Scripting (Reflected)

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

External Redirect

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

Path Traversal

Source	raised by an active scanner (plugin ID: 6)
CWE ID	22
WASC ID	33
Reference	▪ http://projects.webappsec.org/Path-Traversal ▪ http://cwe.mitre.org/data/definitions/22.html

Remote Code Execution - CVE-2012-1823

Source	raised by an active scanner (plugin ID: 20018)
CWE ID	20
WASC ID	20
Reference	▪ http://projects.webappsec.org/Improper-Input-Handling

- http://cwe.mitre.org/data/definitions/89.html

SQL Injection

Source	raised by an active scanner (plugin ID: 40018)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - Hypersonic SQL - Time Based

Source	raised by an active scanner (plugin ID: 40020)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - MySQL

Source	raised by an active scanner (plugin ID: 40019)
CWE ID	89
WASC ID	19

Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - Oracle - Time Based

Source	raised by an active scanner (plugin ID: 40021)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - PostgreSQL - Time Based

Source	raised by an active scanner (plugin ID: 40022)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - SQLite

Source	raised by an active scanner (plugin ID: 40024)
CWE ID	89

WASC ID	19
Reference	- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Server Side Include

Source	raised by an active scanner (plugin ID: 40009)
CWE ID	97
WASC ID	31
Reference	- http://www.carleton.ca/~dmcfet/html/ssi.html

Source Code Disclosure - CVE-2012-1823

Source	raised by an active scanner (plugin ID: 20017)
CWE ID	20
WASC ID	20
Reference	- http://projects.webappsec.org/Improper-Input-Handling - http://cwe.mitre.org/data/definitions/89.html

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

Application Error Disclosure

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

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/

Directory Browsing - Apache 2

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

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

Vulnerable JS Library

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

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

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

Information Disclosure - Debug Error Messages

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

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)

CWE ID	200
WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

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

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	▪ http://httpd.apache.org/docs/current

/mod/core.html#servertokens

- http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007
- 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

Information Disclosure - Sensitive Information in URL

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

Information Disclosure - Suspicious Comments

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

User Controllable Charset

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

WASC ID	20

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