ZAP Scanning Report

Generated with ZAP on ter. 23 mai. 2023, at 09:06:18

Contents

About this report

Report description

Trabalho de ISG

Report parameters

Contexts

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

Sites

The following sites were included:

- `http://127.0.0.1`

(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: `Alto`, `Médio`, `Baixo`, `Informativo`

Excluded: None

Confidence levels

Included: `User Confirmed`, `Alto`, `Médio`, `Baixo`

Excluded: User Confirmed, Alto, Médio, Baixo, Falso Positivo

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	**Alto**	**Médio**	**Baixo**	**Total**
Risk	**Alto**	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	2 (11,1%)	4 (22,2%)	1 (5,6%)	7 (38,9%)
	Baixo	0 (0,0%)	1 (5,6%)	5 (27,8%)	1 (5,6%)	7 (38,9%)
	Informativo	0 (0,0%)	0 (0,0%)	2 (11,1%)	2 (11,1%)	4 (22,2%)
	Total	0 (0,0%)	3 (16,7%)	11 (61,1%)	4 (22,2%)	18 (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			
		Alto **(= Alto)**	**Médio** **(>= Médio)**	**Baixo** **(>= Baixo)**	**Informativo** **(>= Informativo)**
Site	**http://127.0.0.1**	0 (0)	7 (7)	7 (14)	4 (18)

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
Application Error Disclosure	Médio	9 (50,0%)
Ausência de tokens Anti-CSRF	Médio	2 (11,1%)
Content Security Policy (CSP) Header Not Set	Médio	45 (250,0%)
Total		18

Alert type	Risk	Count
Hidden File Found	Médio	1 (5,6%)
Missing Anti-clickjacking Header	Médio	10 (55,6%)
Navegação no Diretório	Médio	6 (33,3%)
XSLT Injection	Médio	1 (5,6%)
Application Error Disclosure	Baixo	17 (94,4%)
Cookie with Invalid SameSite Attribute	Baixo	1 (5,6%)
Cookie without SameSite Attribute	Baixo	2 (11,1%)
Divulgação de Data e Hora - Unix	Baixo	1 (5,6%)
Divulgação de informações - Mensagens de Erro de Depuração	Baixo	9 (50,0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	63 (350,0%)
X-Content-Type-Options Header Missing	Baixo	25 (138,9%)
Cookie Poisoning	Informativo	1 (5,6%)
Divulgação de Informações - Comentários Suspeitos	Informativo	1 (5,6%)
Total		18

Alert type	Risk	Count
User Agent Fuzzer	Informativo	324 (1.800,0%)
User Controllable HTML Element Attribute (Potential XSS)	Informativo	7 (38,9%)
Total		18

Alerts

Risk=Médio, Confidence=Alto (2)

http://127.0.0.1 (2)

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

▶ GET http://127.0.0.1/robots.txt

Hidden File Found (1)

▶ GET http://127.0.0.1/server-status

Risk=Médio, Confidence=Médio (4)

http://127.0.0.1 (4)

Application Error Disclosure (1)

▶ GET http://127.0.0.1/DVWA/instructions.php

Missing Anti-clickjacking Header (1)

▶ GET http://127.0.0.1/DVWA/

Navegação no Diretório (1)

▶ GET http://127.0.0.1/DVWA/docs/

XSLT Injection (1)

▶ GET http://127.0.0.1
/DVWA/instructions.php?doc=%3Cxsl%3Avalue-of+select
%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E

Risk=Médio, Confidence=Baixo (1)

http://127.0.0.1 (1)

Ausência de tokens Anti-CSRF (1)

▶ GET http://127.0.0.1/DVWA/setup.php

Risk=Baixo, Confidence=Alto (1)

http://127.0.0.1 (1)

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

▶ GET http://127.0.0.1/DVWA

Risk=Baixo, Confidence=Médio (5)

http://127.0.0.1 (5)

Application Error Disclosure (1)

▶ GET http://127.0.0.1/DVWA/vulnerabilities/brute/

Cookie with Invalid SameSite Attribute (1)

▶ GET http://127.0.0.1/DVWA/

Cookie without SameSite Attribute (1)

▶ GET http://127.0.0.1/DVWA/

Divulgação de informações - Mensagens de Erro de Depuração (1)

▶ GET http://127.0.0.1/DVWA/instructions.php

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

▶ GET http://127.0.0.1/DVWA/setup.php

Risk=Baixo, Confidence=Baixo (1)

http://127.0.0.1 (1)

Divulgação de Data e Hora - Unix (1)

▶ GET http://127.0.0.1/DVWA/phpinfo.php

Risk=Informativo, Confidence=Médio (2)

http://127.0.0.1 (2)

Divulgação de Informações - Comentários Suspeitos (1)

▶ GET http://127.0.0.1/DVWA/setup.php

User Agent Fuzzer (1)

▶ POST http://127.0.0.1/DVWA/security.php

Risk=Informativo, Confidence=Baixo (2)

`http://127.0.0.1` (2)

Cookie Poisoning (1)

▶ `POST http://127.0.0.1/DVWA/security.php`

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

▶ `GET http://127.0.0.1/DVWA/instructions.php?doc=readme`

Appendix

Alert types

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

Application Error Disclosure

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

Ausência de tokens Anti-CSRF

Source	raised by a passive scanner (Ausência de tokens Anti-CSRF)
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/

Hidden File Found

Source	raised by an active scanner (Hidden File Finder)
CWE ID	538
WASC ID	13
Reference	▪ https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html ▪ https://httpd.apache.org/docs/current/mod/mod_status.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

Navegação no Diretório

Source	raised by an active scanner (Navegação no Diretório)
CWE ID	548
WASC ID	48
Reference	▪ http://httpd.apache.org/docs/mod/core.html#options

- http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html

XSLT Injection

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

Application Error Disclosure

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

Cookie with Invalid 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

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

Divulgação de Data e Hora - Unix

Source	raised by a passive scanner (Divulgação de Data e Hora)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Divulgação de informações - Mensagens de Erro de Depuração

Source	raised by a passive scanner (Divulgação de informações - Mensagens de Erro de Depuração)
CWE ID	200
WASC ID	13

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

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

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	20

WASC ID	20
Reference	- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-cookie

Divulgação de Informações - Comentários Suspeitos

Source	raised by a passive scanner (Divulgação de Informações - Comentários Suspeitos)
CWE ID	200
WASC ID	13

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	- https://owasp.org/wstg

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