ZAP Informes de Escaneo

Generated with ZAP on mart. 26 nov. 2024, at 20:23:37

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://www.badstore.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: `Alto`, `Medio`, `Bajo`, `Informativo`

Excluded: None

Confidence levels

Included: `Confirmado por Usuario`, `Alta`, `Media`, `Baja`

Excluded: `Confirmado por Usuario`, `Alta`, `Media`, `Baja`, `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				
		Confirmado por Usuario	Alta	Media	Baja	Total
Risk	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	4 (33,3 %)	1 (8,3 %)	2 (16,7 %)	7 (58,3 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	1 (8,3 %)	0 (0,0 %)	1 (8,3 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	3 (25,0 %)	1 (8,3 %)	4 (33,3 %)
	Total	0 (0,0 %)	4 (33,3 %)	5 (41,7 %)	3 (25,0 %)	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			
		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)
Site	http://www.badstore.net	0 (0)	7 (7)	1 (8)	4 (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
Ausencia de fichas (tokens) Anti-CSRF	Medio	2 (16,7 %)
CSP: Wildcard Directive	Medio	2 (16,7 %)
CSP: script-src unsafe-eval	Medio	1 (8,3 %)
Total		12

Alert type	Risk	Count
CSP: script-src unsafe-inline	Medio	2 (16,7 %)
CSP: style-src unsafe-inline	Medio	2 (16,7 %)
Hidden File Found (Archivo Oculto Encontrado)	Medio	4 (33,3 %)
Múltiples entradas de cabeceras X-Frame-Options	Medio	1 (8,3 %)
Cross-Domain JavaScript Source File Inclusion	Bajo	3 (25,0 %)
Divulgación de información - Comentarios sospechosos	Informativo	1 (8,3 %)
Modern Web Application	Informativo	1 (8,3 %)
Retrieved from Cache	Informativo	1 (8,3 %)
User Agent Fuzzer	Informativo	8 (66,7 %)
Total		12

Alerts

Risk=Medio, Confidence=Alta (4)

`http://www.badstore.net` (4)

CSP: Wildcard Directive (1)

▶ `GET http://www.badstore.net/`

CSP: script-src unsafe-eval (1)

▶ `GET http://www.badstore.net/`

CSP: script-src unsafe-inline (1)

▶ `GET http://www.badstore.net/`

CSP: style-src unsafe-inline (1)

▶ `GET http://www.badstore.net/`

Risk=`Medio`, Confidence=`Media` (1)

`http://www.badstore.net` (1)

Múltiples entradas de cabeceras X-Frame-Options (1)

▶ `GET http://www.badstore.net/`

Risk=`Medio`, Confidence=`Baja` (2)

`http://www.badstore.net` (2)

Ausencia de fichas (tokens) Anti-CSRF (1)

▶ `GET http://www.badstore.net/`

Hidden File Found (Archivo Oculto Encontrado) (1)

▶ GET http://www.badstore.net/.hg

Risk=Bajo, Confidence=Media (1)

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

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://www.badstore.net/

Risk=Informativo, Confidence=Media (3)

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

Modern Web Application (1)

▶ GET http://www.badstore.net/

Retrieved from Cache (1)

▶ GET http://www.badstore.net/

User Agent Fuzzer (1)

▶ GET http://www.badstore.net/

Risk=Informativo, Confidence=Baja (1)

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

Divulgación de información - Comentarios sospechosos (1)

▶ GET http://www.badstore.net/

Appendix

Alert types

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

Ausencia de fichas (tokens) Anti-CSRF

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy

- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-eval

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)

CWE ID	693
WASC ID	15
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/

- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Hidden File Found (Archivo Oculto Encontrado)

Source	raised by an active scanner (Hidden File Finder (Buscador de Archivos Ocultos))
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

Múltiples entradas de cabeceras X-Frame-Options

Source	raised by a passive scanner (Cabecera Anti-Clickjacking)
CWE ID	1021
WASC ID	15
Reference	- https://tools.ietf.org/html/rfc7034

Cross-Domain JavaScript Source File Inclusion

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

WASC ID	15

Divulgación de información - Comentarios sospechosos

Source	raised by a passive scanner (Divulgación de información - Comentarios sospechosos)
CWE ID	200
WASC ID	13

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
Reference	▪ https://Tools.ietf.org/html/rfc7234 ▪ https://tools.ietf.org/html/rfc7231 ▪ http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (sustituido por rfc7234)

User Agent Fuzzer

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