Informe de Escaneo ZAP

Generated with ZAP on dom 1 dic 2024, at 15:53:18

ZAP Versión: 2.15.0

ZAP by Checkmarx

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://localhost:3000`

(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 %)	2 (18,2 %)	2 (18,2 %)	1 (9,1 %)	5 (45,5 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	2 (18,2 %)	1 (9,1 %)	3 (27,3 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	3 (27,3 %)	0 (0,0 %)	3 (27,3 %)
	Total	0 (0,0 %)	2 (18,2 %)	7 (63,6 %)	2 (18,2 %)	11 (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://localhost:3000	0 (0)	5 (5)	3 (8)	3 (11)

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
CSP: Directiva Wildcard	Medio	1 (9,1 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	1 (9,1 %)
Configuración Incorrecta Cross-Domain	Medio	7 (63,6 %)
Directory Browsing (Exploración de directorios)	Medio	1 (9,1 %)
Falta de cabecera Anti-Clickjacking	Medio	1 (9,1 %)
Divulgación de Marcas de Tiempo - Unix	Bajo	1 (9,1 %)
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP	Bajo	7 (63,6 %)
Total		11

Alert type	Risk	Count
""X-Powered-By""		
Falta encabezado X-Content-Type-Options	Bajo	6 (54,5 %)
Aplicación Web Moderna	Informativo	1 (9,1 %)
Divulgación de información - Comentarios sospechosos	Informativo	16 (145,5 %)
Librería JS Vulnerable	Informativo	1 (9,1 %)
Total		11

Alerts

Risk=Medio, Confidence=Alta (2)

http://localhost:3000 (2)

CSP: Directiva Wildcard (1)

▶ GET http://localhost:3000/sitemap.xml

Cabecera Content Security Policy (CSP) no configurada (1)

▶ GET http://localhost:3000

Risk=Medio, Confidence=Media (2)

http://localhost:3000 (2)

Configuración Incorrecta Cross-Domain (1)

▶ GET http://localhost:3000/favicon.ico

Falta de cabecera Anti-Clickjacking (1)

▶ GET http://localhost:3000

Risk=Medio, Confidence=Baja (1)

http://localhost:3000 (1)

Directory Browsing (Exploración de directorios) (1)

▶ GET http://localhost:3000/static/js/bundle.js/

Risk=Bajo, Confidence=Media (2)

http://localhost:3000 (2)

El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ''''X-Powered-By'''' (1)

▶ GET http://localhost:3000/logo192.png

Falta encabezado X-Content-Type-Options (1)

▶ GET http://localhost:3000/logo192.png

Risk=Bajo, Confidence=Baja (1)

http://localhost:3000 (1)

Divulgación de Marcas de Tiempo - Unix (1)

▶ GET http://localhost:3000/static/js/bundle.js

Risk=Informativo, Confidence=Media (3)

http://localhost:3000 (3)

Aplicación Web Moderna (1)

▶ GET http://localhost:3000

Divulgación de información - Comentarios sospechosos (1)

▶ GET http://localhost:3000

Librería JS Vulnerable (1)

▶ GET http://localhost:3000/static/js/bundle.js

Appendix

Alert types

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

CSP: Directiva Wildcard

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

y+policy

- https://content-security-policy.com/
- https://github.com/HtmlUnit/htmlunit-csp
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Cabecera Content Security Policy (CSP) no configurada

Source	raised by a passive scanner (Cabecera Content Security Policy (CSP) no configurada)
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 - https://www.w3.org/TR/CSP/ - https://w3c.github.io/webappsec-csp/ - https://web.dev/articles/csp - https://caniuse.com/#feat=contentsecuritypolicy - https://content-security-policy.com/

Configuración Incorrecta Cross-Domain

Source	raised by a passive scanner (Configuración Incorrecta Cross-Domain)
CWE ID	264
WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Directory Browsing (Exploración de directorios)

Source	raised by an active scanner (Directory Browsing (Exploración de directorios))
CWE ID	548
WASC ID	48
Reference	▪ https://httpd.apache.org/docs/mod/core.html#options

Falta de cabecera Anti-Clickjacking

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

Divulgación de Marcas de Tiempo - Unix

Source	raised by a passive scanner (Divulgación de Marcas de Tiempo)
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.html

El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ''''X-Powered-By''''

Source	raised by a passive scanner (El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ''''X-Powered-By'''')
CWE ID	200
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework ▪ https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Falta encabezado X-Content-Type-Options

Source	raised by a passive scanner (Falta encabezado X-Content-Type-Options)
CWE ID	693
WASC ID	15

Reference	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers

Aplicación Web Moderna

Source	raised by a passive scanner (Aplicación Web Moderna)

Divulgación de información - Comentarios sospechosos

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

Librería JS Vulnerable

Source	raised by a passive scanner (Librería JS Vulnerable (Gracias a Retire.js))
CWE ID	829