

ZAP Informes de Escaneo

SIMAPE

Generated with  ZAP on lun 28 oct 2024, at 12:41:35

ZAP Version: 2.14.0

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=Medio, Confidence=Alta \(1\)](#)
 - [Risk=Medio, Confidence=Media \(2\)](#)
 - [Risk=Medio, Confidence=Baja \(1\)](#)
 - [Risk=Bajo, Confidence=Media \(3\)](#)
 - [Risk=Informativo, Confidence=Media \(2\)](#)
 - [Risk=Informativo, Confidence=Baja \(2\)](#)

- [Appendix](#)
 - [Alert types](#)

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 %)	1 (9,1 %)	2 (18,2 %)	1 (9,1 %)	4 (36,4 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	3 (27,3 %)	0 (0,0 %)	3 (27,3 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	2 (18,2 %)	2 (18,2 %)	4 (36,4 %)
	Total	0 (0,0 %)	1 (9,1 %)	7 (63,6 %)	3 (27,3 %)	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			
		Informativo			
		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Informativo)	Bajo (>= Informativo)
Site	http://localhost:3000	0 (0)	4 (4)	3 (7)	4 (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
Ausencia de Ttokens Anti-CSRF	Medio	1 (9,1 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	3 (27,3 %)
Configuración Incorrecta Cross-Domain	Medio	11 (100,0 %)
Falta de cabecera Anti-Clickjacking	Medio	1 (9,1 %)
Cookie sin el atributo SameSite	Bajo	3 (27,3 %)
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""	Bajo	11 (100,0 %)
Total		11

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Bajo	8 (72,7 %)
Amplia gama de Cookies	Informativo	4 (36,4 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (18,2 %)
Modern Web Application	Informativo	3 (27,3 %)
Respuesta de Gestión de Sesión Identificada	Informativo	5 (45,5 %)
Total		11

Alerts

Risk=Medio, Confidence=Alta (1)

<http://localhost:3000> (1)

[Cabecera Content Security Policy \(CSP\) no configurada \(1\)](#)

► GET <http://localhost:3000/sitemap.xml>

Risk=Medio, Confidence=Media (2)

<http://localhost:3000> (2)

[Configuración Incorrecta Cross-Domain \(1\)](#)

► GET <http://localhost:3000/js/bannerUsuario.js>

Falta de cabecera Anti-Clickjacking (1)

► GET http://localhost:3000/

Risk=Medio, Confidence=Baja (1)

http://localhost:3000 (1)

Ausencia de Ttokens Anti-CSRF (1)

► GET http://localhost:3000/

Risk=Bajo, Confidence=Media (3)

http://localhost:3000 (3)

Cookie sin el atributo SameSite (1)

► GET http://localhost:3000/robots.txt

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

► POST http://localhost:3000/login

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

► GET http://localhost:3000/icons/pfp.png

Risk=Informativo, Confidence=Media (2)

http://localhost:3000 (2)

Modern Web Application (1)

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

Respuesta de Gestión de Sesión Identificada (1)

► GET http://localhost:3000/

Risk=Informativo, Confidence=Baja (2)

http://localhost:3000 (2)

Amplia gama de Cookies (1)

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

Divulgación de información - Comentarios sospechosos (1)

► GET http://localhost:3000/js/login.js

Appendix

Alert types

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

Ausencia de Ttokens Anti-CSRF

Source

raised by a passive scanner ([Ausencia de Ttokens 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>

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	<ul style="list-style-type: none">■ 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/

Configuración Incorrecta Cross-Domain

Source	raised by a passive scanner (Configuración Incorrecta Cross-Domain)
--------	---

CWE ID	264
WASC ID	14
Reference	<ul style="list-style-type: none"> ▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Falta de cabecera Anti-Clickjacking

Source	raised by a passive scanner (Cabecera Anti-Clickjacking)
CWE ID	1021
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Cookie sin el atributo SameSite

Source	raised by a passive scanner (Cookie sin el atributo SameSite)
CWE ID	1275
WASC ID	13
Reference	<ul style="list-style-type: none"> ▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

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"")
---------------	---

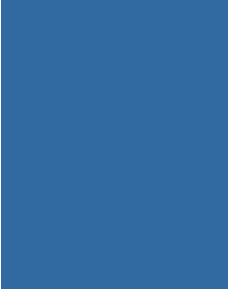
CWE ID	<u>200</u>
WASC ID	13
Reference	<ul style="list-style-type: none"> http://blogs.msdn.com/b/varunm/Archive/2013/04/23/Remove-Unwanted-http-Response-headers.aspx http://www.troyhunt.com/2012/02/shhh-don 't-deje-la-respuesta-headers.html

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	<u>693</u>
WASC ID	15
Reference	<ul style="list-style-type: none"> http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security-Headers

Amplia gama de Cookies

Source	raised by a passive scanner (Amplia gama de Cookies)
CWE ID	<u>565</u>
WASC ID	15
Reference	<ul style="list-style-type: none"> https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-



[Session Management Testing/02-Testing_for_Cookies_Attributes.html](#)

- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

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](#))

Respuesta de Gestión de Sesión Identificada

Source

raised by a passive scanner ([Respuesta de Gestión de Sesión Identificada](#))

Reference

- <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id>