ZAP Informes de Escaneo

Generado con ZAP el 24 nov 2023, a las 16:05:15

Versión ZAP: 2.14.0

Contenido

Acerca de este informe

Parámetros del informe

Contextos

No se seleccionó ningún contexto, por lo que todos los contextos se incluyeron de forma predeterminada.

Sitios

Se incluyeron los siguientes sitios:

- `http://localhost:3000`

(Si no se seleccionó ningún sitio, todos los sitios se incluyeron de forma predeterminada).

Un sitio incluido también debe estar dentro de uno de los contextos incluidos para que sus datos se incluyan en el informe.

Niveles de riesgo

Included: `Alto`, `Medio`, `Bajo`, `Informativo`

Excluido : Ninguno

Niveles de confianza

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

Excluded: `Confirmado por Usuario`, `Alta`, `Media`, `Baja`, `Falso positivo`

Resúmenes

Alerta cuenta por riesgo y confianza

Esta tabla muestra el número de alertas para cada nivel de riesgo y confianza incluidos en el informe.

(Los porcentajes entre paréntesis representan el recuento como porcentaje del número total de alertas incluidas en el informe, redondeado a un decimal).

		Confianza				
		Confirmado por Usuario	Alta	Medios de comunicación	Baja	Total
Riesgo	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	2 (11,8 %)	2 (11,8 %)	1 (5,9 %)	5 (29,4 %)
	Bajo	0 (0,0 %)	0 (0,0 %)	6 (35,3 %)	0 (0,0 %)	6 (35,3 %)
	Informativo	0 (0,0 %)	1 (5,9 %)	2 (11,8 %)	3 (17,6 %)	6 (35,3 %)
	Total	0 (0,0 %)	3 (17,6 %)	10 (58,8 %)	4 (23,5 %)	17 (100%)

Recuento de alertas por sitio y riesgo

Esta tabla muestra, para cada sitio para el cual se generaron una o más alertas, la cantidad de alertas generadas en cada nivel de riesgo.

Se han excluido de estos recuentos las alertas con un nivel de confianza de "falso positivo".

(Los números entre paréntesis son el número de alertas generadas para el sitio en ese nivel de riesgo o por encima de él).

	Riesgo			
	Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)
Sitio http://localhost:3000	0 (0)	5 (5)	6 (11)	6 (17)

Recuentos de alertas por tipo de alerta

Esta tabla muestra la cantidad de alertas de cada tipo de alerta, junto con el nivel de riesgo del tipo de alerta.

(Los porcentajes entre paréntesis representan cada recuento como porcentaje, redondeado a un decimal, del número total de alertas incluidas en este informe).

Tipo de alerta	Riesgo	Contar
Divulgación de errores de aplicación	Medio	3 (17,6 %)
Ausencia de fichas (tokens) Anti-CSRF	Medio	150 (882,4 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	74 (435,3 %)
Falta de cabecera Anti-Clickjacking	Medio	67 (394,1 %)
Hidden File Found (Archivo Oculto Encontrado)	Medio	1 (5,9 %)
Cookie sin bandera HttpOnly	Bajo	8 (47,1 %)
Cookie sin el atributo SameSite	Bajo	8
Total		17

Tipo de alerta	Riesgo	Contar (47,1 %)
Inclusión de archivos fuente JavaScript entre dominios	Bajo	52 (305,9 %)
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ''''X-Powered-By''''	Bajo	71 (417,6 %)
Gran redirección detectada (posible fuga de información confidencial)	Bajo	2 (11,8 %)
Falta el encabezado X-Content-Type-Options	Bajo	124 (729,4 %)
Amplia gama de Cookies	Informativo	16 (94,1 %)
Solicitud de autenticación identificada	Informativo	1 (5,9 %)
Divulgación de información - Comentarios sospechosos	Informativo	2 (11,8 %)
Aplicación web moderna	Informativo	1 (5,9 %)
Respuesta de gestión de sesión identificada	Informativo	19 (111,8 %)
Atributo de elemento HTML controlable por el usuario (Posible XSS)	Informativo	200 (1.176,5 %)
Total		17

Alertas

Risk=Medio, Confidence=Alta (2)

http://localhost:3000 (2)

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

▶ OBTENER http://localhost:3000/robots.txt

Hidden File Found (Archivo Oculto Encontrado) (1)

▶ GET http://localhost:3000/.git/config

Risk=Medio, Confidence=Media (2)

http://localhost:3000 (2)

Application Error Disclosure (1)

▶ GET http://localhost:3000/contact.php

Falta de cabecera Anti-Clickjacking (1)

▶ GET http://localhost:3000/about.php

Risk=Medio, Confidence=Baja (1)

http://localhost:3000 (1)

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

▶ GET http://localhost:3000/home.php

Risk=Bajo, Confidence=Media (6)

http://localhost:3000 (6)

Cookie No HttpOnly Flag (1)

▶ GET http://localhost:3000/home.php

Cookie sin el atributo SameSite (1)

▶ GET http://localhost:3000/home.php

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://localhost:3000/about.php

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

▶ GET http://localhost:3000/orders.php

Gran redirección detectada (posible fuga de información confidencial) (1)

▶ GET http://localhost:3000/cart.php

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

▶ GET http://localhost:3000/about.php

Risk=Informativo, Confidence=Alta (1)

http://localhost:3000 (1)

Authentication Request Identified (1)

▶ POST http://localhost:3000/login.php

Risk=Informativo, Confidence=Media (2)

http://localhost:3000 (2)

Modern Web Application (1)

▶ GET http://localhost:3000/recetas.php

Session Management Response Identified (1)

▶ GET http://localhost:3000/home.php

Risk=Informativo, Confidence=Baja (3)

http://localhost:3000 (3)

Amplia gama de Cookies (1)

▶ GET http://localhost:3000/home.php

Divulgación de información - Comentarios sospechosos (1)

▶ GET http://localhost:3000/js/script.js

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

▶ GET http://localhost:3000/category.php?category=Postres

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

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

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 ▪ 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/

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

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 • https://git-scm.com/docs/git-config

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 sin el atributo SameSite

Source	raised by a passive scanner (Cookie sin el atributo SameSite)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

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	▪ 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

Gran redirección detectada (posible fuga de información confidencial)

Source	raised by a passive scanner (Gran redirección detectada (posible fuga de información confidencial))
ID CWE	201
Identificación WASC	13
Referencia	▪ [cadena vacía]

Falta el encabezado X-Content-Type-Options

Fuente	planteado por un escáner pasivo (Falta el encabezado X-Content-Type-Options)
ID CWE	693
Identificación WASC	15
Referencia	▪ 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

Fuente	levantado por un escáner pasivo (Amplia gama de Cookies)
ID CWE	565
Identificación WASC	15
Referencia	▪ 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

Solicitud de autenticación identificada

Fuente	planteado por un escáner pasivo (Solicitud de autenticación identificada)
Referencia	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Divulgación de información - Comentarios sospechosos

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

Identificación WASC	13

Aplicación web moderna

Fuente	planteado por un escáner pasivo (aplicación web moderna)

Respuesta de gestión de sesión identificada

Fuente	generado por un escáner pasivo (Respuesta de gestión de sesión identificada)
Referencia	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

Atributo de elemento HTML controlable por el usuario (Posible XSS)

Fuente	generado por un escáner pasivo (atributo de elemento HTML controlable por el usuario (potencial XSS))
ID CWE	20
Identificación WASC	20
Referencia	▪ http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute