ZAP por Informe de Escaneo Checkmarx

Generated with ZAP on lun 30 jun 2025, at 08:55:56

ZAP Versión: 2.16.1

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:8080

(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 (7,7 %)	1 (7,7 %)	1 (7,7 %)	3 (23,1 %)
	Bajo	0 (0,0 %)	1 (7,7 %)	4 (30,8 %)	1 (7,7 %)	6 (46,2 %)
	Informativo	0 (0,0 %)	1 (7,7 %)	2 (15,4 %)	1 (7,7 %)	4 (30,8 %)
	Total	0 (0,0 %)	3 (23,1 %)	7 (53,8 %)	3 (23,1 %)	13 (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:80**	0 (0)	3 (3)	6 (9)	4 (13)
	80				

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 Tokens Anti-CSRF	Medio	6 (46,2 %)
Cabecera Content Security Policy (CSP) no configurada	Medio	23 (176,9 %)
Falta de cabecera Anti-Clickjacking	Medio	18 (138,5 %)
Cookie Sin Flag HttpOnly	Bajo	1 (7,7 %)
Total		13

Alert type	Risk	Count
Cookie sin el atributo SameSite	Bajo	1 (7,7 %)
Divulgación de Marcas de Tiempo - Unix	Bajo	5 (38,5 %)
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""	Bajo	33 (253,8 %)
El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP	Bajo	52 (400,0 %)
Falta encabezado X-Content-Type-Options	Bajo	32 (246,2 %)
Atributo de elemento HTML controlable por el usuario (XSS potencial)	Informativo	1 (7,7 %)
Divulgación de Información - Información sensible en URL	Informativo	1 (7,7 %)
Petición de Autenticación Identificada	Informativo	1 (7,7 %)
Respuesta de Gestión de Sesión Identificada	Informativo	1 (7,7 %)
Total		13

Alerts

Risk=Medio, Confidence=Alta (1)

http://localhost:8080 (1)

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

▶ GET http://localhost:8080/sitemap.xml

Risk=Medio, Confidence=Media (1)

http://localhost:8080 (1)

Falta de cabecera Anti-Clickjacking (1)

▶ GET http://localhost:8080/

Risk=Medio, Confidence=Baja (1)

http://localhost:8080 (1)

Ausencia de Tokens Anti-CSRF (1)

▶ GET http://localhost:8080/guestbook.php

Risk=Bajo, Confidence=Alta (1)

http://localhost:8080 (1)

El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP (1)

▶ GET http://localhost:8080/sitemap.xml

Risk=Bajo, Confidence=Media (4)

http://localhost:8080 (4)

Cookie Sin Flag HttpOnly (1)

▶ GET http://localhost:8080/

Cookie sin el atributo SameSite (1)

▶ GET http://localhost:8080/

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

▶ GET http://localhost:8080/

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

▶ GET http://localhost:8080/

Risk=Bajo, Confidence=Baja (1)

http://localhost:8080 (1)

Divulgación de Marcas de Tiempo - Unix (1)

▶ GET http://localhost:8080/calendar.php

Risk=Informativo, Confidence=Alta (1)

http://localhost:8080 (1)

Petición de Autenticación Identificada (1)

▶ POST http://localhost:8080/users/login.php

Risk=Informativo, Confidence=Media (2)

http://localhost:8080 (2)

Divulgación de Información - Información sensible en URL (1)

▶ GET http://localhost:8080/users/sample.php?userid=1

Respuesta de Gestión de Sesión Identificada (1)

▶ GET http://localhost:8080/

Risk=Informativo, Confidence=Baja (1)

http://localhost:8080 (1)

Atributo de elemento HTML controlable por el usuario (XSS potencial) (1)

▶ GET http://localhost:8080/pictures/search.php?query=ZAP

Appendix

Alert Types

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

Ausencia de Tokens Anti-CSRF

Source	raised by a passive scanner (Ausencia de Tokens Anti-CSRF)
CWE ID	352
WASC ID	9
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheet

s/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

- 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 - 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/

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

Cookie Sin Flag HttpOnly

Source	raised by a passive scanner (Cookie Sin Flag HttpOnly)
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

Divulgación de Marcas de Tiempo - Unix

Source	raised by a passive scanner (Divulgación de Marcas de Tiempo)
CWE ID	497
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	497
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

El servidor filtra información de versión a través del campo "Server" del encabezado de respuesta HTTP

Source	raised by a passive scanner (Cabecera de Respuesta del Servidor HTTP)
CWE ID	497
WASC ID	13
Reference	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)

- https://www.troyhunt.com/shhh-dont-let-your-response-headers/

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

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

Source	raised by a passive scanner (Atributo de elemento HTML controlable por el usuario (XSS potencial))
CWE ID	20
WASC ID	20
Reference	- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Divulgación de Información - Información sensible en URL

Source	raised by a passive scanner (Divulgación de Información - Información sensible en URL)
CWE ID	598

WASC ID 13

Petición de Autenticación Identificada

Source raised by a passive scanner (Petición de Autenticación Identificada)

Reference
- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

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