

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://cescjavier.dev	Checks	9 pruebas
Dominio	cescjavier.dev	Hallazgos	46 totales
Fecha	20 de julio de 2026 a las 02:19	Problemas	6 detectados

A

94/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web ha determinado una puntuación de 94/100, lo que otorga una calificación de nota A. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 7 verificaciones exitosas, 2 advertencias técnicas y 0 fallos críticos. La infraestructura presenta una configuración de cifrado y cabeceras de seguridad sobresaliente, aunque se han detectado exposiciones menores de información técnica y archivos de sistema. En conclusión, el sitio se considera altamente seguro, aunque requiere ajustes preventivos para reducir su superficie de ataque y mejorar el endurecimiento del servidor.

Resumen de Riesgos

0 CRITICO	0 ALTO	4 MEDIO	2 BAJO	40 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta robots.txt
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
80 dias restantes (expira: 2026-10-08T02:46:55.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-10T01:49:51.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO Server header expuesto
Server: cloudflare — Revela tecnologia del servidor

- BAJO

X-Powered-By expuesto
X-Powered-By: Next.js — Revela framework/lenguaje
- INFO

Content-Security-Policy
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://static.cloudflarei...
- INFO

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(), interest-cohort=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://cescjavier.dev/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- INFO

Tecnologias detectadas
React, Next.js, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO

Contenido mixto
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta robots.txt

- INFO

sitemap.xml
Presente, 9 URLs
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO

Puerto 21 (FTP)
Cerrado — Transferencia de archivos sin cifrar
- INFO

Puerto 22 (SSH)
Cerrado — Acceso remoto seguro
- INFO

Puerto 23 (Telnet)
Cerrado — Acceso remoto sin cifrar
- INFO

Puerto 25 (SMTP)
Cerrado — Envio de correo
- INFO

Puerto 80 (HTTP)
Abierto (esperado) — Servidor web
- INFO

Puerto 443 (HTTPS)
Abierto (esperado) — Servidor web seguro
- INFO

Puerto 3306 (MySQL)
Cerrado — Base de datos MySQL expuesta
- INFO

Puerto 3389 (RDP)
Cerrado — Escritorio remoto Windows
- INFO

Puerto 5432 (PostgreSQL)
Cerrado — Base de datos PostgreSQL expuesta
- INFO

Puerto 6379 (Redis)
Cerrado — Cache Redis sin autenticacion por defecto
- MEDIO

Puerto 8080 (HTTP-Alt)
ABIERTO — Servidor web alternativo / proxy
- INFO

Puerto 27017 (MongoDB)
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[LOW] Server header expuesto: el encabezado revela el uso de Cloudflare, lo que ayuda a un atacante a identificar la infraestructura de red.

[LOW] X-Powered-By expuesto: la cabecera indica el uso de Next.js, permitiendo la identificación del framework y la búsqueda de vulnerabilidades específicas.

[MEDIUM] Archivo /readme.html accesible: este archivo puede contener detalles sobre la versión del software y configuraciones internas del sistema.

[MEDIUM] Archivo /README.txt accesible: la exposición de este documento facilita la obtención de metadatos técnicos por parte de terceros no autorizados.

[MEDIUM] Ruta /wp-login.php activa: el panel de acceso está disponible públicamente, lo que permite intentos de intrusión por fuerza bruta o ataques de diccionario.

[LOW] Falta de robots.txt: la ausencia de este archivo impide dar instrucciones claras a los rastreadores sobre qué directorios no deben ser indexados.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: la presencia de un puerto de servicio alternativo abierto aumenta los puntos de entrada potenciales para un atacante.