

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://giovanysosa.dev/	Checks	9 pruebas
Dominio	giovanysosa.dev	Hallazgos	49 totales
Fecha	23 de julio de 2026 a las 17:13	Problemas	8 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado ha obtenido una puntuación de 86/100, lo que equivale a una nota B en términos de postura de seguridad web. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó una advertencia y 1 se marcó como fallo crítico por la ausencia de configuraciones preventivas. La infraestructura presenta una base sólida en cifrado y transporte de datos, pero carece de cabeceras de seguridad fundamentales y expone servicios innecesarios. Se concluye que el sitio es parcialmente vulnerable a ataques de inyección y reconocimiento debido a estos fallos de configuración.

Resumen de Riesgos

0 CRITICO	1 ALTO	4 MEDIO	3 BAJO	41 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
84 dias restantes (expira: 2026-10-16T02:00:05.000Z)
- INFO Fecha de emision
Emitido desde: 2026-07-18T01:01:38.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

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

- BAJO

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

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=63072000; includeSubDomains; preload
- INFO

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

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

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

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 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

- INFO

Archivo /readme.html
No accesible (correcto)

- INFO

Archivo /README.txt
No accesible (correcto)
- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (1937 bytes)
- INFO

Reglas robots.txt
11 Disallow, 2 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- BAJO

Ruta sensible en robots.txt
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO

Sitemap en robots.txt
https://giovanyososa.dev/sitemap.xml
- 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

[HIGH] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que puede ser utilizado para acceder a servicios internos o proxies de forma no autorizada.

[MEDIUM] Referrer-Policy: La ausencia de esta directiva impide controlar cuánta información de navegación se envía a otros sitios web al seguir enlaces.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización, aumentando el riesgo de privacidad.

[MEDIUM] Ruta sensible en robots.txt: El archivo expone la ubicación de un directorio administrativo, lo cual facilita el reconocimiento por parte de atacantes.

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, permitiendo a un atacante perfilar la tecnología del servidor.

[LOW] X-Powered-By expuesto: Se detectó el uso del framework Next.js, información que puede ser aprovechada para buscar vulnerabilidades específicas de dicha versión.

[LOW] Bloqueo total en robots.txt: La directiva Disallow: / bloquea la indexación, lo cual no es una vulnerabilidad de seguridad per se, pero afecta la visibilidad del sitio.