

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nokfi.app	Checks	9 pruebas
Dominio	nokfi.app	Hallazgos	43 totales
Fecha	7 de agosto de 2026 a las 23:30	Problemas	9 detectados

B

84/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web ha arrojado una puntuación de 84/100, lo que corresponde a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 3 advertencias por configuraciones mejorables y 1 fallo en la estructura de archivos de indexación. Aunque la plataforma presenta una base de cifrado sólida, la falta de políticas de seguridad estrictas en las cabeceras y la exposición de rutas administrativas representan un riesgo. Se concluye que el sitio es funcionalmente seguro pero vulnerable a ataques de reconocimiento y de intermediario si no se aplican las correcciones sugeridas.

Resumen de Riesgos

0 CRITICO	2 ALTO	6 MEDIO	1 BAJO	34 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 85 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
85 dias restantes (expira: 2026-11-01T06:54:52.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-03T06:54:53.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

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

- INFO

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

X-Frame-Options
Presente: DENY
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

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

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

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

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://nokfi.app/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- 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

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
- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

INFO

security.txt

Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO

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

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

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

Puerto 25 (SMTP)
- Cerrado — Envío 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
- INFO

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

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

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Strict-Transport-Security: La ausencia de esta cabecera impide que el navegador fuerce conexiones HTTPS de forma permanente, permitiendo ataques de degradación de protocolo.

[MEDIUM] Rutas de administración accesibles: Se detectó acceso público a los endpoints /wp-login.php, /administrator/ y /user/login, facilitando intentos de intrusión por fuerza bruta.

[MEDIUM] Archivos de información expuestos: Los archivos /readme.html y /README.txt son accesibles, lo que podría revelar detalles técnicos sobre la infraestructura interna.

[MEDIUM] Puerto 22 (SSH) abierto: La exposición de este puerto permite intentos de acceso remoto directo al servidor, aumentando la superficie de ataque.

[LOW] Cabecera Server expuesta: El servidor revela el uso de nginx, información que los atacantes utilizan para buscar vulnerabilidades específicas del software.

[LOW] Ausencia de archivos de control: No se detectaron los archivos robots.txt ni sitemap.xml, lo cual afecta negativamente a la organización y seguridad del rastreo web.