EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://alofoke.net	Checks	9 pruebas
Dominio	alofoke.net	Hallazgos	13 totales
Fecha	16 de agosto de 2026 a las 03:29	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha concluido con una puntuación perfecta de 100/100 y una calificación de nota A. Durante el proceso de auditoría se llevaron a cabo 9 controles de tipo pasivo, obteniendo 1 resultado satisfactorio y cero registros de advertencias o fallos. Los protocolos de inspección no identificaron brechas de seguridad ni debilidades en la superficie de exposición analizada. Cabe destacar que el pentest activo no fue ejecutado en esta instancia del escaneo. Basándose en estos resultados, se determina que el sitio es seguro y cumple con los estándares de integridad evaluados.

Resumen de Riesgos

0	1	0	0	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 302 — No redirige a HTTPS

Puertos Abiertos — 100/100

Estado: OK

1 puerto(s) abierto(s), todos esperados

- 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)**
  Cerrado — 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

No se detectaron vulnerabilidades durante el ciclo de escaneo pasivo. Los hallazgos relacionados con debilidades de tipo CWE, cabeceras de seguridad faltantes o exposición de subdominios fueron inexistentes debido a la puntuación máxima obtenida. Al no haberse realizado un pentest activo, no se identificaron endpoints de API descubiertos ni riesgos adicionales en la infraestructura. El reporte de auditoría no arroja fallos reales que comprometan la seguridad de la plataforma.