EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://elchelako.com	Checks	9 pruebas
Dominio	elchelako.com	Hallazgos	15 totales
Fecha	16 de agosto de 2026 a las 03:40	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio elchelako.com ha arrojado una puntuación de 73/100, lo que corresponde a una nota C. Los resultados de los 9 checks pasivos ejecutados muestran deficiencias críticas, ya que la mayoría de los parámetros de seguridad fundamentales no pudieron ser verificados satisfactoriamente. Solo se obtuvo un resultado positivo en la revisión de puertos abiertos, mientras que fallaron elementos esenciales como el cifrado y la configuración de archivos de rastreo. Debido a la imposibilidad de confirmar una conexión segura y la falta de cabeceras de protección, se concluye que el sitio es actualmente vulnerable. Esta situación expone a los usuarios y a la integridad de la plataforma a riesgos de interceptación y ataques de diversa índole.

Resumen de Riesgos

1	0	0	2	12
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder
- BAJO **sitemap.xml**
  Error al acceder

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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

[CRITICAL] Conexión SSL/TLS: El sistema no pudo establecer o verificar una conexión cifrada, lo que permite la interceptación de datos en tránsito.
[CRITICAL] Cabeceras de Seguridad: No se detectaron cabeceras HTTP de protección, dejando el sitio expuesto a ataques de inyección y suplantación.
[CRITICAL] Redirección HTTPS: La ausencia de una redirección forzada hacia un entorno seguro facilita ataques de degradación de conexión.
[LOW] Archivo Robots.txt: No se pudo acceder al archivo de directivas de rastreo, lo que afecta el control sobre los motores de búsqueda.
[LOW] Sitemap XML: La falta de un mapa del sitio impide una indexación estructurada y puede ocultar errores en la arquitectura web.