EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://elmalecondelsalsa.com	Checks	9 pruebas
Dominio	elmalecondelsalsa.com	Hallazgos	15 totales
Fecha	17 de septiembre de 2026 a las 01:08	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio elmalecondelsalsa.com arroja una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 1 resultó exitoso, 0 generaron advertencias y 1 fue identificado como fallo directo, sumado a múltiples errores de conectividad en servicios críticos. La imposibilidad de verificar parámetros esenciales como el cifrado de datos y las cabeceras de protección indica una configuración técnica inestable. Debido a la falta de validación en los protocolos de seguridad básicos, se concluye que el sitio es vulnerable y presenta riesgos significativos para la integridad de la información.

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

[CRÍTICO] Conexión SSL/TLS: No se pudo establecer una comunicación cifrada, lo que permite la interceptación de datos sensibles entre el usuario y el servidor.
[ALTO] Cabeceras de Seguridad: La ausencia de verificación en las cabeceras impide mitigar ataques de tipo Cross-Site Scripting (XSS) e inyección de clics.
[ALTO] Redirección HTTPS: No se confirmó la transición automática de tráfico no seguro a seguro, dejando expuestas las sesiones de navegación.
[BAJO] Ausencia de Robots.txt: El servidor no dispone de un archivo de instrucciones para buscadores, lo que dificulta el control del rastreo web.
[BAJO] Ausencia de Sitemap.xml: La falta de un mapa del sitio afecta la indexación y puede exponer directorios que no deberían ser públicos.