EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.warma-ext.com	Checks	9 pruebas
Dominio	www.warma-ext.com	Hallazgos	15 totales
Fecha	19 de septiembre de 2026 a las 00:18	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio warma-ext.com arroja una puntuación de 73/100, lo que se traduce en una nota C. Se ejecutaron 9 checks pasivos de los cuales solo 1 resultó satisfactorio y 1 presentó fallos directos, mientras que el resto de los parámetros no pudieron ser validados correctamente. El análisis no incluyó un pentest activo, limitándose a la inspección de la superficie externa. Debido a la incapacidad de establecer conexiones seguras y verificar cabeceras esenciales, se concluye que el sitio es actualmente vulnerable. La falta de protocolos de cifrado verificables representa un riesgo significativo para cualquier usuario que interactúe con la plataforma.

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] Fallo en conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que expone los datos transmitidos a interceptaciones por parte de terceros.
[CRITICAL] Error en cabeceras de seguridad: La imposibilidad de verificar cabeceras básicas deja al servidor vulnerable ante ataques de inyección y suplantación.
[HIGH] Ausencia de redirección HTTPS: No se confirmó el forzado de tráfico seguro, permitiendo potenciales accesos a través de protocolos no cifrados.
[LOW] Falta de robots.txt y sitemap.xml: El servidor deniega el acceso o carece de archivos de indexación, lo que afecta la visibilidad y gestión del rastreo web.
[MEDIUM] Indeterminación de seguridad en cookies: No se pudo validar si las cookies de sesión cuentan con los atributos de seguridad necesarios para evitar el robo de identidad.