EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.vendo-ropa.com.ar	Checks	9 pruebas
Dominio	www.vendo-ropa.com.ar	Hallazgos	15 totales
Fecha	27 de abril de 2026 a las 02:37	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web presenta una puntuación final de 73/100, lo que otorga una calificación de grado C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resultó correcto, 0 generaron advertencias y 1 fue clasificado como fallo crítico. La imposibilidad de verificar componentes esenciales como el cifrado SSL y las cabeceras de seguridad sugiere una configuración de servidor altamente restrictiva o mal implementada. Debido a la ausencia de validación en los protocolos de cifrado y la falta de archivos de indexación básicos, se concluye que el sitio es actualmente vulnerable. No se puede garantizar la integridad ni la privacidad de los datos de los usuarios que interactúen 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] Conexión SSL: No se pudo establecer una conexión cifrada SSL/TLS, lo que impide proteger la comunicación entre el usuario y el servidor.
[CRITICAL] Cabeceras de Seguridad: No se detectaron cabeceras de protección, dejando al sitio expuesto a ataques de inyección de scripts y suplantación de identidad.
[CRITICAL] Redirección HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que el tráfico viaje en texto plano.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo que podría facilitar el robo de sesiones.
[LOW] Archivo robots.txt: Error al acceder al archivo, lo que impide controlar qué partes del sitio son rastreadas por los motores de búsqueda.
[LOW] Archivo sitemap.xml: El mapa del sitio no es accesible, dificultando la correcta indexación y auditoría de la estructura web.
[LOW] Detección de CMS: La configuración actual oculta el sistema de gestión de contenidos, lo cual previene el análisis de vulnerabilidades específicas de versión.