EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.infoscreenauto.ayudalabs.com	Checks	9 pruebas
Dominio	www.infoscreenauto.ayudalabs.com	Hallazgos	15 totales
Fecha	24 de abril de 2026 a las 06:20	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha resultado en una puntuación de 73/100, lo que equivale a una nota C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 1 resultado satisfactorio y 1 fallo detectado, además de varios errores de conexión que impidieron validar protocolos fundamentales. La incapacidad del sistema para verificar el cifrado SSL y las cabeceras de seguridad sugiere una configuración de servidor restrictiva o mal implementada. Debido a la falta de validación en elementos críticos de protección de datos y configuración de red, se concluye que el sitio es vulnerable.

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] Conexion SSL: No se pudo establecer una conexión SSL/TLS, lo que impide garantizar la confidencialidad de los datos entre el usuario y el servidor.
[LOW] robots.txt: El sistema registró un error al intentar acceder a este archivo, lo que impide gestionar correctamente el rastreo de los motores de búsqueda.
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la indexación estructurada y la verificación de la jerarquía de contenidos.
[INFO] Cabeceras de Seguridad: Error en la verificación que indica la posible ausencia de directivas contra ataques de clickjacking e inyección de código.
[INFO] Redireccion HTTPS: No se pudo confirmar si el sitio fuerza el tráfico seguro, dejando abierta la posibilidad de conexiones interceptables mediante HTTP.
[INFO] Seguridad de Cookies: La falta de acceso a los parámetros de cookies impide confirmar si poseen los atributos de seguridad necesarios para evitar el robo de sesiones.