

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://lscvsystems.com
Dominio lscvsystems.com
Fecha 7 de mayo de 2026 a las 17:33

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

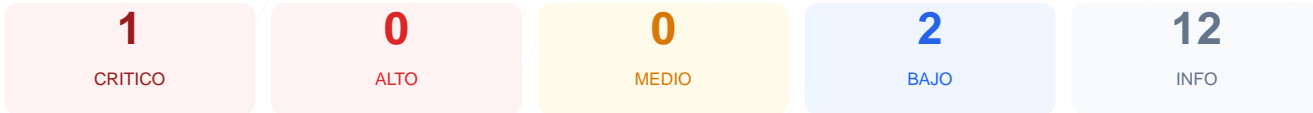
puntos de seguridad



RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio lscvsystems.com arrojó una puntuación de 73/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo únicamente un resultado satisfactorio y detectando fallos críticos en la infraestructura de cifrado y configuración. Los resultados indican una imposibilidad de verificar protocolos esenciales como SSL/TLS y las cabeceras de seguridad obligatorias. Debido a la ausencia de estas capas de protección fundamentales y problemas en la estructura de archivos del servidor, se concluye que el sitio es vulnerable.

Resumen de Riesgos



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	1 puerto(s) abierto(s), todos esperados

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

1 puerto(s) abierto(s), todos esperados

- **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 — Envío de correo
- **INFO Puerto 80 (HTTP)**
Cerrado — Servidor web
- **INFO Puerto 443 (HTTPS)**
Abierto (esperado) — 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 autenticación 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 conexion segura SSL/TLS, lo que impide el cifrado de la informacion y expone los datos a interceptaciones.
- [HIGH] Cabeceras de Seguridad: No se detectaron cabeceras HTTP de seguridad, dejando la plataforma desprotegida contra ataques de inyeccion y cross-site scripting.
- [HIGH] Redireccion HTTPS: El sitio no permite verificar si existe una transicion automatica de trafico inseguro a conexiones protegidas.
- [MEDIUM] Seguridad de Cookies: Existe una imposibilidad tecnica para verificar si las cookies de sesion cuentan con los atributos de seguridad necesarios.
- [LOW] Ausencia de robots.txt: Se detecto un error al intentar acceder al archivo de instrucciones para rastreadores, afectando la transparencia del sitio.
- [LOW] Ausencia de sitemap.xml: No se encontro el mapa del sitio, lo que dificulta la indexacion correcta y el analisis de la estructura web.
- [INFO] Deteccion de CMS y Contenido: El servidor bloquea o no proporciona informacion sobre el sistema de gestion de contenidos y posibles conflictos de contenido mixto.