EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jm.nexo	Checks	9 pruebas
Dominio	jm.nexo	Hallazgos	15 totales
Fecha	27 de mayo de 2026 a las 20:59	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio web muestra una puntuacion de 73/100 con una nota final de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resulto satisfactorio y 1 presento fallos explicitos, mientras que el resto no pudo ser verificado por errores de conexion. Los resultados indican una ausencia critica de protocolos de cifrado y configuraciones de seguridad basicas en el servidor. Debido a la incapacidad de validar el certificado SSL y las cabeceras de proteccion, el sitio se considera actualmente vulnerable. No se realizo un pentest activo durante este ciclo de evaluacion.

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 conexion SSL/TLS, lo que impide el cifrado de informacion entre el usuario y el servidor.
[HIGH] Cabeceras de Seguridad: Ausencia total de cabeceras HTTP de proteccion, lo que facilita ataques de inyeccion y suplantacion.
[HIGH] Redireccion HTTPS: El servidor no fuerza el uso de protocolos seguros, permitiendo conexiones vulnerables a traves de HTTP.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, aumentando el riesgo de robo de sesion.
[LOW] Robots.txt y Sitemap: No se detectaron los archivos robots.txt ni sitemap.xml, afectando la indexacion y el control de rastreo del sitio.