EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://coopnacional.com	Checks	9 pruebas
Dominio	coopnacional.com	Hallazgos	15 totales
Fecha	13 de mayo de 2026 a las 16:32	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web presenta una puntuación de 73/100 con una nota de calificación C. Los resultados se basan en 9 checks pasivos ejecutados, donde se obtuvo 1 resultado OK y 1 fallo crítico, sin que fuera posible validar el resto de parámetros por errores de conexión. Debido a la imposibilidad de verificar el cifrado SSL/TLS y las cabeceras de seguridad, el sitio se considera actualmente vulnerable. Es imperativo corregir los problemas de acceso para garantizar la integridad de los datos de los usuarios.

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 SSL/TLS, lo que impide el cifrado de la información y expone los datos a interceptaciones.
[LOW] Archivo robots.txt: No se pudo acceder al archivo, lo que dificulta el control sobre el rastreo de los motores de búsqueda.
[LOW] Archivo sitemap.xml: El mapa del sitio no está disponible o es inaccesible, afectando la visibilidad y estructura del dominio.
[ERROR] Cabeceras de Seguridad: No se detectaron directivas de protección como HSTS o CSP, dejando el sitio expuesto a ataques de intermediarios.
[ERROR] Redirección HTTPS: El servidor no garantiza el salto automático de conexiones inseguras a conexiones cifradas.