EscanearVulnerabilidades

Informe de Seguridad Web

URL	http://b—4cdo9.com	Checks	9 pruebas
Dominio	xn--cdo9-fr6hy65x.com	Hallazgos	16 totales
Fecha	27 de julio de 2026 a las 09:27	Problemas	4 detectados

C

64/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad del dominio analizado ha resultado en una puntuación de 64/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos que revelaron deficiencias críticas, incluyendo la ausencia total de cifrado SSL/TLS y fallos en la configuración de cabeceras de seguridad. El sitio presenta riesgos significativos debido a que la comunicación no es privada y carece de archivos de control de rastreo. No se detectó un sistema de gestión de contenidos activo, lo que dificulta la verificación de versiones de software. Con base en estos hallazgos, se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad web.

Resumen de Riesgos

1	1	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	50	AVISO	El sitio no usa HTTPS, no aplica chequeo de cont...
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

Contenido Mixto — 50/100

Estado: AVISO

El sitio no usa HTTPS, no aplica chequeo de contenido mixto

- ALTO **Protocolo**
  El sitio no usa HTTPS

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

[CRÍTICO] Conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que permite la interceptación de datos entre el usuario y el servidor.
[ALTO] Protocolo Inseguro: El sitio opera exclusivamente bajo HTTP, lo que expone a los visitantes a ataques de hombre en el medio (MitM).
[ALTO] Cabeceras de Seguridad: No se detectaron cabeceras HTTP de protección, dejando el sitio vulnerable a ataques de inyección, XSS y clickjacking.
[ALTO] Seguridad de Cookies: La ausencia de cifrado impide verificar si las cookies de sesión cuentan con los atributos Secure y HttpOnly.
[BAJO] Robots.txt y Sitemap: El servidor no dispone de archivos de indexación, lo que indica una configuración de servidor incompleta o defectuosa.