EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mundocopextel.com	Checks	9 pruebas
Dominio	mundocopextel.com	Hallazgos	15 totales
Fecha	27 de abril de 2026 a las 13:24	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio mundocopextel.com arroja una puntuación de 73/100, otorgando una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en un solo acierto y múltiples fallos críticos que impidieron la verificación de parámetros esenciales. La imposibilidad de validar el cifrado SSL y las cabeceras de seguridad fundamentales sugiere una configuración técnica deficiente o restrictiva. Debido a estas carencias en la infraestructura de protección básica, se concluye que el sitio es actualmente vulnerable. La plataforma no garantiza un entorno seguro para la transferencia de información sensible.

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 datos y expone la comunicación a interceptaciones.
[HIGH] Cabeceras de Seguridad: No se detectaron cabeceras de protección, facilitando ataques de tipo Cross-Site Scripting (XSS) e inyección de código.
[HIGH] Redirección HTTPS: El servidor no fuerza el uso de protocolos seguros, permitiendo que los usuarios naveguen por canales vulnerables.
[MEDIUM] Seguridad de Cookies: Ausencia de atributos de seguridad en las cookies, lo que pone en riesgo la integridad de las sesiones de usuario.
[MEDIUM] Contenido Mixto: La falta de verificación de recursos sugiere que elementos inseguros podrían estarse cargando en páginas supuestamente protegidas.
[LOW] Configuración de Rastreo: El fallo en robots.txt y sitemap.xml dificulta la gestión del tráfico de bots y la indexación controlada del sitio.