EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://worldpaper.com.mx	Checks	9 pruebas
Dominio	worldpaper.com.mx	Hallazgos	19 totales
Fecha	28 de abril de 2026 a las 13:47	Problemas	8 detectados

F

10/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar el análisis técnico de worldpaper.com.mx, se ha determinado una puntuación crítica de 10/100, lo que equivale a una nota de F. Los resultados de los 9 checks pasivos ejecutados revelan fallos estructurales graves, incluyendo un certificado SSL expirado hace años y la exposición de servicios sensibles de base de datos. No se detectaron cabeceras de seguridad ni redirecciones cifradas, dejando la comunicación de los usuarios totalmente desprotegida. Debido a la gravedad de los hallazgos en la infraestructura de red y transporte de datos, se concluye que el sitio es altamente vulnerable y no cumple con los estándares mínimos de seguridad web.

Resumen de Riesgos

2	3	1	2	11
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- ALTO **Dias hasta expiracion**
  -2754 dias restantes (expira: 2018-10-13T19:49:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2017-10-13T19:49:07.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 301 — No redirige a 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 — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — 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] Certificado SSL inválido: El certificado de seguridad expiró hace 2754 días (octubre de 2018), invalidando cualquier intento de conexión cifrada.
[CRITICAL] Puerto 3306 (MySQL) abierto: La base de datos se encuentra expuesta directamente a internet, lo que permite ataques de fuerza bruta y posible extracción de información sensible.
[HIGH] Redirección HTTPS inexistente: El servidor utiliza una redirección HTTP 301 que no fuerza el tráfico hacia una versión segura, exponiendo los datos en tránsito.
[HIGH] Puerto 21 (FTP) abierto: El uso de este puerto para transferencia de archivos sin cifrar permite que atacantes intercepten credenciales y contenido.
[HIGH] Cabeceras de seguridad ausentes: La falta de verificación en cabeceras HTTP impide proteger al sitio contra ataques de inyección, XSS y Clickjacking.
[MEDIUM] Puerto 22 (SSH) abierto: Aunque permite administración segura, mantener este puerto visible desde cualquier IP aumenta innecesariamente la superficie de ataque.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos indica una carencia de configuración en la estructura del sitio y errores de acceso al servidor.