EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://customer-187-175-52-241.uninet-ide.com.mx	Checks	9 pruebas
Dominio	customer-187-175-52-241.uninet-ide.com.mx	Hallazgos	15 totales
Fecha	11 de septiembre de 2026 a las 02:31	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado sobre el activo digital ha resultado en una puntuacion de 73/100, lo que otorga una nota C segun los estandares de evaluacion. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 1 resulto correcto, 0 generaron advertencias y 1 fue categorizado como fallo critico debido a la imposibilidad de verificar parametros de seguridad esenciales. La ausencia de visibilidad en el cifrado de datos y las cabeceras de proteccion impide garantizar la integridad del sitio. En consecuencia, el sitio se considera vulnerable y presenta un riesgo operativo elevado para el intercambio de informacion. No se dispone de datos de profundidad tecnica adicional debido a que el pentest activo no fue ejecutado.

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

[CRITICO] Conexion SSL/TLS: No se pudo establecer ni verificar una conexion cifrada, lo que expone los datos a interceptaciones de terceros.
[CRITICO] Cabeceras de Seguridad: No fue posible detectar encabezados HTTP de proteccion, dejando el servidor vulnerable a ataques de inyeccion y clickjacking.
[CRITICO] Redireccion HTTPS: El sitio no garantiza el redireccionamiento automatico a una version segura, permitiendo conexiones potenciales a traves de canales no cifrados.
[CRITICO] Seguridad de Cookies: No se pudo validar la presencia de atributos de seguridad en las cookies, lo que facilita el robo de sesiones de usuario.
[BAJO] Archivos de Indexacion: Se confirmo la ausencia de robots.txt y sitemap.xml, lo que compromete la gestion adecuada del rastreo por parte de motores de busqueda.