EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://taxipremiumpiura.com/	Checks	9 pruebas
Dominio	taxipremiumpiura.com	Hallazgos	15 totales
Fecha	27 de mayo de 2026 a las 16:17	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio taxipremiumpiura.com arroja una puntuación de 73/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, resultando en 1 verificación exitosa y 1 fallo crítico confirmado, mientras que el resto de los módulos presentaron errores técnicos de conexión. La imposibilidad de validar protocolos básicos como SSL/TLS y cabeceras de seguridad impide garantizar la integridad de la navegación. Debido a estas deficiencias en la infraestructura y la falta de archivos de configuración esenciales, se concluye que el sitio es actualmente vulnerable y requiere intervención técnica inmediata.

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
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] Error de conexión SSL/TLS: No se pudo establecer un túnel seguro de comunicación, lo que expone los datos de los usuarios a posibles interceptaciones.
[HIGH] Ausencia de Cabeceras de Seguridad: El servidor no proporciona instrucciones de protección contra ataques de inyección, clickjacking o robo de sesiones.
[HIGH] Tiempo de espera agotado (Timeout): La respuesta del servidor excede los 15 segundos, lo que indica una infraestructura inestable o bloqueos que impiden la auditoría.
[MEDIUM] Configuración de Cookies inaccesible: No se ha podido verificar el uso de atributos de seguridad en las cookies, lo que podría permitir el secuestro de sesiones.
[LOW] Falta de archivos de indexación: El sistema no detectó los archivos robots.txt ni sitemap.xml, esenciales para la correcta gestión de rastreo y seguridad del directorio.