EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ts.savvyds.com	Checks	9 pruebas
Dominio	ts.savvyds.com	Hallazgos	15 totales
Fecha	28 de mayo de 2026 a las 11:52	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis técnico del dominio ts.savvyds.com ha resultado en una puntuación de 73/100, obteniendo una calificación de nota C. Durante la evaluación, se ejecutaron 9 checks pasivos que arrojaron 1 resultado satisfactorio y 1 fallo crítico en la configuración de archivos de navegación, además de múltiples errores de conexión. La imposibilidad de verificar los protocolos de cifrado y las cabeceras de protección básicas sugiere una configuración de servidor deficiente. Por lo tanto, el sitio se clasifica como vulnerable debido a la falta de garantías en la privacidad y seguridad de los datos de los usuarios.

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

[CRITICA] Conexion SSL/TLS: No se pudo establecer una conexion cifrada, lo que impide proteger la informacion contra interceptaciones de terceros.
[CRITICA] Cabeceras de Seguridad: No se detectaron cabeceras esenciales, dejando el sitio expuesto a ataques de Cross-Site Scripting (XSS) y Clickjacking.
[CRITICA] Redireccion HTTPS: El servidor no fuerza el uso de conexiones seguras, permitiendo que los usuarios naveguen por canales vulnerables.
[ALTA] Seguridad de Cookies: La ausencia de verificacion en cookies implica que los identificadores de sesion podrian ser capturados por atacantes.
[BAJA] Robots.txt y Sitemap: Faltan archivos de control de rastreo, lo que afecta la integridad de la indexacion y el control de acceso a directorios.