EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.mediservicios.igssgt.org	Checks	9 pruebas
Dominio	www.mediservicios.igssgt.org	Hallazgos	15 totales
Fecha	21 de abril de 2026 a las 20:30	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web https://www.mediservicios.igssgt.org ha arrojado una puntuación de 73/100, lo que corresponde a una calificación de grado C. Durante la evaluación, se ejecutaron 9 checks pasivos de los cuales 1 resultó satisfactorio y 1 se marcó como fallo crítico, mientras que el resto presentó errores de conectividad que impidieron una validación completa. La imposibilidad de verificar parámetros esenciales como el cifrado SSL y las cabeceras de seguridad genera una incertidumbre técnica considerable. Por lo tanto, el sitio se considera vulnerable debido a la falta de transparencia en sus protocolos de protección de datos.

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] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide garantizar que la información enviada por los usuarios viaje de forma cifrada.
[ALTO] Cabeceras de Seguridad: No se pudo verificar la presencia de encabezados HTTP protectores, dejando el sitio expuesto a ataques de intermediario y secuestro de clics.
[ALTO] Redirección HTTPS: La falta de confirmación sobre el forzado de tráfico seguro permite que las sesiones puedan ser interceptadas en redes no confiables.
[BAJO] Robots.txt y Sitemap: Se detectó la ausencia o inaccesibilidad de estos archivos, lo que dificulta el rastreo controlado por parte de motores de búsqueda y expone una gestión deficiente del servidor.
[BAJO] Seguridad de Cookies: No se pudo validar si las cookies de sesión cuentan con los atributos Secure y HttpOnly, necesarios para prevenir el robo de identidad digital.