EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.servicios.igssgt.org	Checks	9 pruebas
Dominio	www.servicios.igssgt.org	Hallazgos	15 totales
Fecha	21 de abril de 2026 a las 20:31	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre la plataforma arroja una puntuación de 73/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 1 resultado satisfactorio y 1 fallo crítico documentado, mientras que el resto de las pruebas no pudieron completarse por errores de conexión. La imposibilidad de establecer un túnel SSL/TLS impide garantizar la confidencialidad de los datos transmitidos por los usuarios. Debido a la falta de cifrado y la ausencia de cabeceras de seguridad verificables, el sitio se considera vulnerable en su estado actual. Es imperativo corregir la configuración del servidor para mitigar riesgos de interceptación de tráfico.

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

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de la información y facilita ataques de intermediario (Man-in-the-Middle).
[LOW] Archivo robots.txt ausente: El sistema no pudo acceder al archivo de directivas para buscadores, lo que afecta el control de indexación y privacidad de rutas internas.
[LOW] Archivo sitemap.xml ausente: La falta de este archivo dificulta la auditoría de la estructura del sitio y el reconocimiento de endpoints legítimos.
[HIGH] Cabeceras de seguridad no detectadas: La imposibilidad de verificar headers de protección sugiere que el sitio carece de políticas contra ataques de inyección y clickjacking.
[MEDIUM] Inconsistencia en la seguridad de cookies: No se pudo validar el uso de atributos de seguridad en las cookies, lo que pone en riesgo la integridad de las sesiones de usuario.