

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://360admin.igssgt.org
Dominio 360admin.igssgt.org
Fecha 25 de mayo de 2026 a las 20:11

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

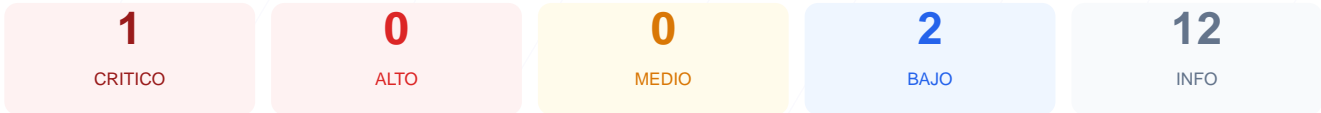
puntos de seguridad



RESUMEN EJECUTIVO

La evaluación de seguridad realizada al sitio web muestra una puntuación de 73/100, lo que otorga una nota C. El análisis consistió en 9 checks pasivos, de los cuales 1 resultó en estado satisfactorio, 0 generaron advertencias y 1 se registró como fallo técnico. Varios procesos de verificación no pudieron completarse debido a errores en la conexión con el servidor, lo que impidió analizar cabeceras y cookies. Debido a la incapacidad de validar el cifrado SSL/TLS y la ausencia de archivos de configuración básicos, el sitio se clasifica como vulnerable en su estado actual.

Resumen de Riesgos



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 — Envío 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 autenticación 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: No se pudo establecer una conexión segura SSL/TLS, lo cual es peligroso porque los datos viajan sin cifrar y pueden ser interceptados.

[LOW] Archivos de rastreo: No se detectaron los archivos robots.txt ni sitemap.xml, lo que impide una gestión correcta de la indexación y puede exponer rutas no deseadas.

[INFO] Cabeceras de seguridad: Error al verificar la presencia de cabeceras de seguridad, dejando al sitio potencialmente expuesto a ataques de clickjacking o inyección si no están configuradas.

[INFO] Seguridad de cookies: No se pudo validar el atributo Secure o HttpOnly en las cookies de sesión debido a los errores de conexión mencionados.