

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://gohiai.com
Dominio gohiai.com
Fecha 22 de mayo de 2026 a las 08:59

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

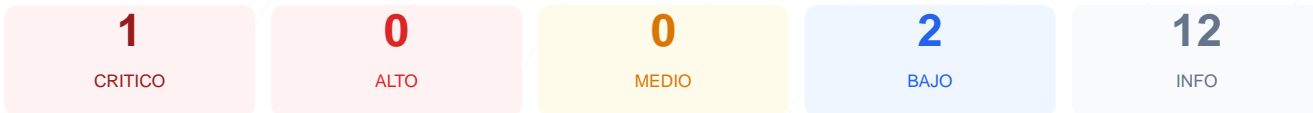
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad del dominio ha arrojado una puntuación de 73/100, lo que resulta en una calificación de grado C. Durante la evaluación pasiva, se ejecutaron 9 verificaciones, detectando fallos críticos en la infraestructura de cifrado y la configuración de cabeceras. El sistema solo superó con éxito la prueba de puertos abiertos, mientras que el resto de los parámetros de red fallaron o no pudieron ser validados. Debido a la incapacidad de confirmar protocolos SSL/TLS y la ausencia de protecciones básicas, se concluye que el sitio es actualmente vulnerable. Es necesario realizar una intervención técnica inmediata para mitigar los riesgos de exposición de datos.

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 SSL/TLS válida, lo que impide el cifrado de la información y expone los datos al interceptado.

[HIGH] Cabeceras de Seguridad: El servidor no entrega cabeceras HTTP de protección, dejando a los usuarios vulnerables ante ataques de inyección y suplantación.

[HIGH] Redirección HTTPS: La falta de redirección forzada hacia un entorno seguro permite comunicaciones inseguras a través de texto plano.

[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo cual facilita el secuestro de sesiones.

[LOW] Ausencia de Robots.txt y Sitemap: Los archivos de control de indexación no son accesibles, lo que complica la gestión de rutas y el rastreo del sitio.

[LOW] Detección de CMS: La imposibilidad de identificar el CMS y su versión impide la gestión de parches de seguridad específicos contra vulnerabilidades conocidas.