

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://www.grupo-int.com
Dominio www.xn--grupoint-wn3d.com
Fecha 28 de julio de 2026 a las 14:43

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

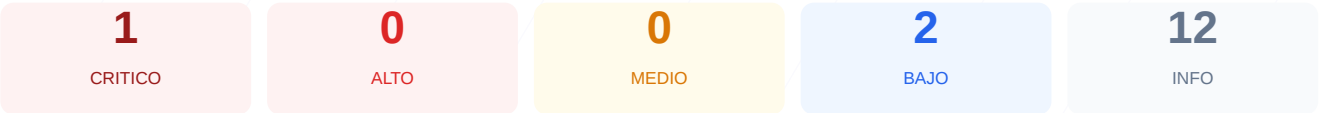
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arroja una puntuación exacta de 73/100 con una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 1 aprobado y 1 fallo crítico identificado según los parámetros de la auditoría. La imposibilidad de validar protocolos básicos como SSL/TLS y las cabeceras de seguridad sugiere deficiencias estructurales importantes en la configuración del servidor. No se llevó a cabo un pentest activo, limitando el alcance de este informe a la exposición pública inmediata y pasiva del sitio. En conclusión, el sitio web se considera actualmente como vulnerable debido a la ausencia de medidas de protección y cifrado fundamentales.

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 autentificacion 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

[CRÍTICO] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de datos entre el usuario y el servidor.

[CRÍTICO] Cabeceras de Seguridad: Ausencia total de cabeceras HTTP de protección, exponiendo el sitio a ataques de inyección y suplantación.

[CRÍTICO] Redirección HTTPS: El sitio no fuerza el uso de protocolos seguros, permitiendo la interceptación de tráfico en texto plano.

[CRÍTICO] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo que facilita el robo de sesiones.

[BAJO] Archivos de Rastreo: Faltan los archivos robots.txt y sitemap.xml, lo que indica una configuración de servidor incompleta y falta de control sobre buscadores.