EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.grupoint.com	Checks	9 pruebas
Dominio	www.grupoint.com	Hallazgos	19 totales
Fecha	28 de julio de 2026 a las 14:45	Problemas	4 detectados

F

37/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras la auditoría técnica realizada, el sitio grupoint.com ha obtenido una puntuación de 37/100, lo que equivale a una calificación de grado F. Se ejecutaron un total de 9 checks pasivos, de los cuales únicamente 1 resultó exitoso, identificándose 2 fallos críticos directos y múltiples errores de configuración que impidieron la validación de otros parámetros. La infraestructura actual presenta deficiencias graves en la implementación de protocolos de cifrado y seguridad en el transporte de datos. Por todo lo anterior, se concluye que el sitio es altamente vulnerable y no ofrece garantías de privacidad para sus usuarios.

Resumen de Riesgos

1	1	0	2	15
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 0/100

Estado: FALLO

Certificado SSL no valido

- CRITICO **Certificado valido**
  El certificado SSL NO es valido
- INFO **Dias hasta expiracion**
  70 dias restantes (expira: 2026-10-06T21:22:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-08T21:22:16.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

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

2 puerto(s) abierto(s), todos esperados

- 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)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — 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] Certificado SSL no válido: El certificado de seguridad actual no es válido o no ha sido reconocido, lo que permite la interceptación de datos entre el navegador y el servidor.
[HIGH] Redirección HTTPS ausente: El sitio permite el acceso mediante el protocolo HTTP sin forzar el paso a una conexión cifrada, manteniendo la comunicación expuesta en texto plano.
[LOW] Ausencia de archivos robots.txt y sitemap.xml: No se detectaron estos archivos de configuración, lo que afecta la visibilidad en motores de búsqueda y el control del rastreo del sitio.
[ERROR] Fallo general en cabeceras de seguridad: No se pudo verificar la presencia de protecciones contra ataques de tipo Clickjacking, XSS o inyección, lo que sugiere una configuración de servidor deficiente.