

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://neversal.com
Dominio neversal.com
Fecha 27 de mayo de 2026 a las 20:44

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

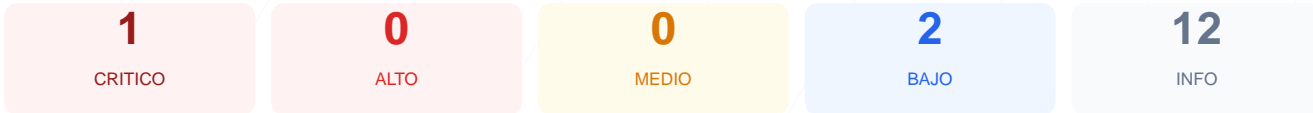
73/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web neversal.com ha arrojado una puntuación de 73/100, lo que corresponde a una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 1 validación correcta, 0 advertencias y 1 fallo crítico que impidió la verificación de múltiples parámetros esenciales. La imposibilidad de establecer una conexión SSL/TLS y la ausencia de cabeceras de seguridad representan un riesgo significativo para la integridad de los datos. Con base en los resultados obtenidos, se concluye que el sitio es actualmente vulnerable y no cumple con los estándares mínimos de seguridad web.

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

- [CRITICO] Conexión SSL/TLS: No se pudo establecer una conexión cifrada, lo que permite la interceptación de datos en tránsito entre el usuario y el servidor.
- [CRITICO] Cabeceras de Seguridad: No se pudieron verificar los encabezados de protección, lo que sugiere una falta de defensas contra ataques de inyección y cross-site scripting.
- [CRITICO] Redirección HTTPS: El sitio no garantiza el uso de protocolos seguros, exponiendo a los usuarios a conexiones no cifradas.
- [BAJO] Robots.txt y Sitemap: Se detectó la falta de archivos de indexación, lo que afecta la visibilidad en motores de búsqueda y la estructura de rastreo.
- [CRITICO] Seguridad de Cookies: No se pudo verificar el estado de las cookies, incrementando el riesgo de secuestro de sesiones si no se utilizan los atributos Secure y HttpOnly.