

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Reservasnevados.com	Checks	9 pruebas
Dominio	reservasnevados.com	Hallazgos	47 totales
Fecha	6 de octubre de 2026 a las 03:10	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a Reservasnevados.com arroja una puntuación exacta de 79/100, obteniendo una nota final de B. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se generaron 2 advertencias y se identificó 1 fallo crítico en la configuración de tráfico. Aunque la implementación del cifrado SSL es robusta, la ausencia de una redirección forzada hacia el protocolo seguro representa un riesgo significativo para la privacidad de los datos. El estado de la plataforma se concluye como vulnerable debido a la exposición de rutas administrativas y archivos de información técnica que facilitan el reconocimiento por parte de atacantes.

Resumen de Riesgos

0	1	6	1	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 43 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 43 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
43 dias restantes (expira: 2026-11-18T07:07:33.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-08-20T06:07:39.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- BAJO **Server header expuesto**
Server: cloudflare — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: upgrade-insecure-requests; default-src 'self' https: data: blob:; script-src 'se...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=31536000; includeSubDomains
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- INFO

Permissions-Policy
Presente: camera=(), microphone=(), geolocation=(), usb=()

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 200 — No redirige a HTTPS
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=31536000; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=31536000 (365 dias)
- INFO

Respuesta HTTPS
HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO

Archivo /readme.html
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php
Panel de login accesible publicamente

- MEDIO

Ruta /administrator/
Panel de login accesible publicamente
- MEDIO

Ruta /user/login
Panel de login accesible publicamente
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO

Cookies detectadas
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO

Contenido mixto
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (67 bytes)
- INFO

Reglas robots.txt
1 Disallow, 0 Allow
- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO

Puerto 8080 (HTTP-Alt)
ABIERTO — Servidor web alternativo / proxy
- INFO

Puerto 27017 (MongoDB)
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

- [HIGH] Falta de redirección HTTP a HTTPS: El sitio permite conexiones mediante HTTP sin cifrar, lo que expone los datos de los usuarios a ataques de interceptación.
- [MEDIUM] Archivos de documentación expuestos: Las rutas /readme.html y /README.txt son accesibles, lo que podría revelar versiones internas y detalles del software base.
- [MEDIUM] Paneles de administración accesibles: Se detectó acceso público a rutas de login como /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.
- [MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de este servidor alternativo incrementa la superficie de ataque y puede contener servicios no supervisados.
- [LOW] Cabecera de servidor expuesta: El campo Server revela el uso de Cloudflare, proporcionando información sobre la infraestructura tecnológica a posibles atacantes.
- [LOW] Ausencia de sitemap.xml: La falta de este archivo dificulta la correcta gestión y control de la indexación del contenido del sitio.