

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://greynimbus.com
Dominio greynimbus.com
Fecha 10 de agosto de 2026 a las 15:12

Checks 9 pruebas
Hallazgos 43 totales
Problemas 14 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 73/100 con una calificación final de nota C. Se ejecutaron un total de 9 controles pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos críticos. Aunque la capa de cifrado base es correcta, la exposición de servicios de infraestructura y la ausencia de cabeceras de protección incrementan el perfil de riesgo. Se concluye que el sitio es actualmente vulnerable debido a configuraciones de servidor inseguras que comprometen la integridad de la base de datos y la privacidad del usuario.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
81 dias restantes (expira: 2026-10-30T21:58:02.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-01T21:58:03.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO Server header expuesto
Server: LiteSpeed — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: upgrade-insecure-requests
- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://greynimbus.com/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 20/100

Estado: FALLO
Faltan robots.txt y sitemap.xml

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

Puertos Abiertos — 60/100

Estado: AVISO
2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- **ALTO** **Puerto 21 (FTP)**
ABIERTO — 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
- **CRITICO** **Puerto 3306 (MySQL)**
ABIERTO — 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] Puerto 3306 (MySQL): El puerto de la base de datos está abierto al acceso público, lo que permite intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP): Servicio de transferencia de archivos activo y accesible, el cual transmite credenciales y datos sin cifrado, facilitando la interceptación de información.
[HIGH] X-Frame-Options: Cabecera ausente, lo que permite que el sitio sea cargado en iframes externos facilitando ataques de secuestro de clics o clickjacking.
[HIGH] Strict-Transport-Security: La política HSTS no está configurada, permitiendo que un atacante pueda forzar la degradación de la conexión de HTTPS a HTTP.

[MEDIUM] X-Content-Type-Options: Falta esta cabecera, lo que permite al navegador intentar interpretar el contenido de forma distinta a la declarada (MIME-sniffing).

[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros dominios, lo que podría filtrar rutas internas privadas.

[MEDIUM] Permissions-Policy: Ausencia de restricciones para APIs del navegador como cámara, micrófono o geolocalización.

[MEDIUM] Rutas de administración y archivos expuestos: Acceso público a /wp-login.php, /administrator/, /user/login, /readme.html y /README.txt, lo que facilita el reconocimiento del sistema.

[LOW] Server header expuesto: El servidor revela el uso de la tecnología LiteSpeed, facilitando la búsqueda de vulnerabilidades específicas para esa versión.