

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://magnifica-manager-spa.netlify.app/	Checks	9 pruebas
Dominio	magnifica-manager-spa.netlify.app	Hallazgos	45 totales
Fecha	20 de julio de 2026 a las 05:00	Problemas	4 detectados

A

91/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio magnifica-manager-spa.netlify.app ha arrojado una puntuación de 91/100, lo que equivale a una nota de grado A. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 7 verificaciones exitosas, 1 advertencia y 1 fallo detectado. La plataforma presenta una base sólida en cuanto a cifrado de datos y configuraciones de transporte seguro, aunque carece de ciertas cabeceras de seguridad preventivas. Se han identificado omisiones menores en archivos de configuración de indexación que no comprometen directamente la integridad de los datos. En conclusión, el sitio se clasifica como seguro, siempre que se atiendan las recomendaciones para mitigar riesgos de inyección de contenido.

Resumen de Riesgos

0	1	0	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 243 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 243 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
243 dias restantes (expira: 2027-03-19T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-16T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

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

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: DENY
- INFO

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

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

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

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

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://magnifica-manager-spa.netlify.app/
- INFO

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

Tecnologias detectadas
Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)

● 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

● BAJO **robots.txt**
No encontrado (HTTP 404)

● BAJO **sitemap.xml**
No encontrado (HTTP 404)

● BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

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

[HIGH] Content-Security-Policy: Falta esta cabecera fundamental, lo que deja al sitio vulnerable ante ataques de Cross-Site Scripting (XSS) e inyecciones de datos.

[LOW] Server header expuesto: La cabecera revela el uso de Netlify, proporcionando información técnica sobre la infraestructura que podría ser aprovechada en un reconocimiento de objetivos.

[LOW] robots.txt: El archivo no fue encontrado (404), lo que impide definir reglas de acceso para rastreadores automáticos.

[LOW] sitemap.xml: La ausencia de este archivo dificulta la indexación estructurada y el reconocimiento de la jerarquía del sitio por parte de servicios externos.