

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://moringmex.netlify.app/
Dominio moringmex.netlify.app
Fecha 4 de mayo de 2026 a las 19:05

Checks 9 pruebas
Hallazgos 44 totales
Problemas 8 detectados

B

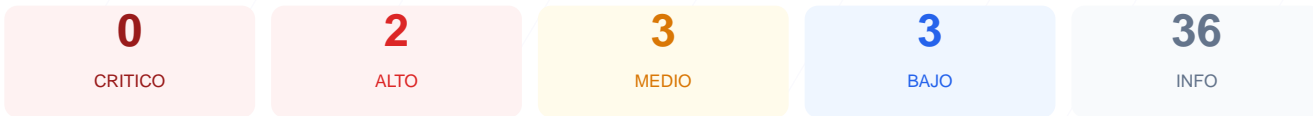
80/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio moringmex.netlify.app ha resultado en una puntuación de 80/100, lo que equivale a una nota B. Se ejecutaron 9 checks pasivos, de los cuales 7 finalizaron con éxito y 2 presentaron fallos críticos relacionados con la configuración del servidor. El cifrado de datos y las redirecciones son correctos, pero la ausencia de cabeceras de seguridad fundamentales deja la plataforma expuesta a ataques conocidos. Aunque el sitio muestra una base técnica sólida, se considera vulnerable debido a la falta de políticas de protección en el navegador. Por tanto, se requiere una intervención inmediata en los parámetros de respuesta HTTP para mitigar riesgos de inyección y suplantación.

Resumen de Riesgos



Resumen de Checks

| | | | |
|------------------------|-----|-------|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 319 dias |
| Cabeceras de Seguridad | 20 | FALLO | Solo 1/6 presentes. Faltan: Content-Security-Pol... |
| 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 319 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
319 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 — 20/100

Estado: FALLO

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

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyeccion de contenido
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains; preload
- **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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://moringmex.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

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: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea embebido en marcos externos no autorizados.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-type sniffing, lo que podría llevar a la ejecución de scripts camuflados como archivos de datos.

[MEDIUM] Referrer-Policy: No existe una política definida para controlar la información de procedencia que se envía a otros dominios durante la navegación.

[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, dejando expuestas funciones como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El encabezado revela el uso de Netlify como tecnología de servidor, facilitando el reconocimiento a posibles atacantes.

[LOW] Archivos de indexación faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta el control de rastreo y la visibilidad en buscadores.