

Escanear Vulnerabilidades

Informe de Seguridad Web

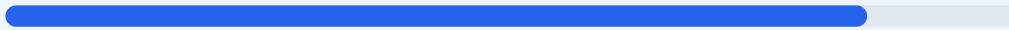
URL https://rovenleather.com
Dominio rovenleather.com
Fecha 24 de abril de 2026 a las 21:02

Checks 9 pruebas
Hallazgos 45 totales
Problemas 6 detectados

B

85/100

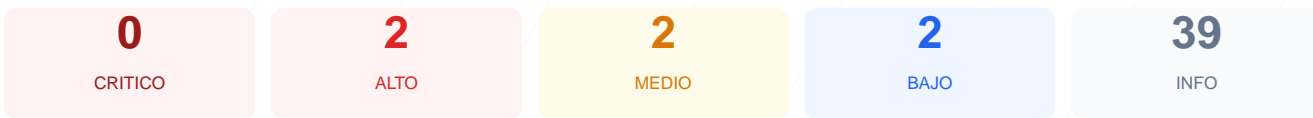
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 85/100, lo que equivale a una nota de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó una advertencia y 1 se marcó como fallo crítico debido a la ausencia de configuraciones de seguridad en el servidor. El cifrado de datos y la gestión de redirecciones seguras son robustos, cumpliendo con los estándares actuales de la industria. Sin embargo, la falta de cabeceras de protección expone a los usuarios a riesgos de inyección de código y suplantación. En conclusión, el sitio es mayoritariamente seguro, pero se considera vulnerable frente a ataques dirigidos de tipo Cross-Site Scripting y Clickjacking.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 64 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	60	AVISO	Falta robots.txt
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 64 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
64 dias restantes (expira: 2026-06-28T02:53:57.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-30T02:53:58.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

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

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: Nuxt — Revela framework/lenguaje
- **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
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **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://rovenleather.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no 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**
Nuxt, Nuxt

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 — 60/100

Estado: AVISO

Falta robots.txt

- INFO **sitemap.xml**
Presente, 11 URLs
- 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 que previene ataques XSS y la ejecución de scripts maliciosos de terceros.

[HIGH] X-Frame-Options: La ausencia de esta política permite que el sitio sea embebido en iframes, facilitando ataques de clickjacking.

[MEDIUM] Referrer-Policy: Falta la configuración para controlar cuánta información de origen se envía al navegar hacia enlaces externos.

[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El servidor revela que utiliza Netlify, lo que proporciona pistas sobre la infraestructura a posibles atacantes.

[LOW] X-Powered-By expuesto: Se detecta el uso del framework Nuxt, exponiendo información sobre el stack tecnológico de la aplicación.

[LOW] Archivo robots.txt ausente: El sitio no cuenta con instrucciones para los motores de búsqueda, lo que genera una advertencia en la gestión del rastreo.