EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tradelabjournal.com/	Checks	9 pruebas
Dominio	www.tradelabjournal.com	Hallazgos	44 totales
Fecha	12 de mayo de 2026 a las 15:53	Problemas	8 detectados

B

76/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio tradelabjournal.com ha resultado en una puntuación de 76/100 con una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios, se generó 1 advertencia por puertos expuestos y se identificaron 2 fallos críticos en la configuración de cabeceras y archivos de indexación. Aunque la infraestructura de cifrado y redirección HTTPS es robusta, la ausencia casi total de cabeceras de seguridad modernas eleva el riesgo de ataques dirigidos al cliente. Se concluye que el sitio web presenta un estado de seguridad aceptable pero vulnerable a ataques de inyección y secuestro de clics debido a omisiones en la configuración del servidor.

Resumen de Riesgos

0	2	4	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-06-22T23:17:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-24T23:17:11.000Z
- 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: cloudflare — 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=63072000
- 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 308 redirige a https://www.tradelabjournal.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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**
  React, 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 **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, lo cual suele indicar la presencia de servidores web alternativos o interfaces de gestión potencialmente vulnerables.

[MEDIUM] X-Content-Type-Options: La falta de esta instrucción permite que el navegador realice sniffing de tipos MIME, facilitando la ejecución de archivos con contenido malicioso disfrazado.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que podría exponer datos de navegación privados.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como la cámara, micrófono o geolocalización a través de esta cabecera.
[LOW] Server header expuesto: Se revela la tecnología de servidor Cloudflare, facilitando la fase de reconocimiento para un atacante.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado (HTTP 404), afectando la transparencia de la estructura del dominio.