EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://api.wisdomtreeprimeapp.com	Checks	9 pruebas
Dominio	api.wisdomtreeprimeapp.com	Hallazgos	44 totales
Fecha	29 de abril de 2026 a las 22:01	Problemas	8 detectados

B

79/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio api.wisdomtreeprimeapp.com arroja una puntuación de 79/100 con una calificación final de grado B. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, de las cuales 6 resultaron exitosas, una generó una advertencia y dos fallaron debido a configuraciones ausentes. Aunque el cifrado de datos es sólido, la carencia de cabeceras de seguridad críticas debilita la postura defensiva del servidor. En su estado actual, el sitio web se considera moderadamente seguro, pero presenta vulnerabilidades que podrían ser explotadas mediante ataques de inyección y manipulación de interfaz.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 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	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 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-06-28T16:39:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T15:39:21.000Z
- 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: 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=15552000; includeSubDomains; preload
- 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://api.wisdomtreeprimeapp.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 404

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 — 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 no autorizados, aumentando el riesgo de ataques XSS y robo de datos.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y expone un servidor web alternativo o proxy, lo cual amplía la superficie de ataque innecesariamente.
[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la filtración de información sensible a través de las cabeceras de referencia en peticiones externas.
[MEDIUM] Permissions-Policy: No se restringe el acceso a funciones sensibles del navegador como la cámara o el micrófono, dejando la puerta abierta a abusos de API.
[LOW] Server header expuesto: Se detectó el uso de Cloudflare a través de la cabecera del servidor, lo que facilita a un atacante el reconocimiento de la infraestructura tecnológica.
[LOW] Ausencia de robots.txt y sitemap.xml: El servidor responde con errores 404 para estos archivos, lo que indica una falta de gestión en la visibilidad y el rastreo del sitio.