EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://app.todolotiene.com/	Checks	9 pruebas
Dominio	app.todolotiene.com	Hallazgos	46 totales
Fecha	5 de mayo de 2026 a las 04:28	Problemas	5 detectados

A

94/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio arrojó una puntuación de 94/100 con una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 generaron advertencias técnicas. Los estándares de cifrado y las cabeceras de seguridad muestran una implementación sólida, aunque existen vectores de información expuestos en la infraestructura. En conclusión, el sitio se considera seguro para la operación, aunque requiere ajustes menores en la configuración del servidor y visibilidad de puertos para mitigar riesgos de reconocimiento.

Resumen de Riesgos

0	0	3	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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 sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-07-15T11:00:26.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-16T10:00:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'nonce-LXHgSWdY9jK3bBydobdbYb' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=2592000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://app.todolotiene.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=2592000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=2592000 (30 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1738 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy abierto puede ser utilizada por atacantes para intentar acceder a paneles de administración o servicios internos.
[MEDIUM] Configuración HSTS insuficiente: El valor max-age está configurado en 30 días, lo cual es inferior al estándar de la industria de 180 días, reduciendo la ventana de protección de transporte estricto.
[MEDIUM] Bloqueo total en robots.txt: El archivo instruye a los buscadores a no indexar ninguna sección del sitio, lo cual puede ser una medida de seguridad por oscuridad pero también indica una superficie de ataque no deseada para el tráfico público.
[LOW] Cabecera Server expuesta: El servidor revela el uso de Cloudflare, lo que permite a un actor malintencionado identificar la tecnología de protección y buscar vulnerabilidades específicas de dicho proveedor.
[LOW] Ausencia de sitemap.xml: El archivo de mapa del sitio no fue encontrado o el acceso está prohibido (403), lo que dificulta la auditoría de rutas legítimas y la indexación controlada.