

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://eltoque.com
Dominio eltoque.com
Fecha 21 de mayo de 2026 a las 15:14

Checks 9 pruebas
Hallazgos 44 totales
Problemas 4 detectados

B

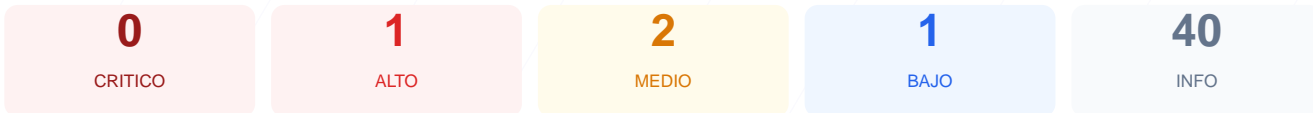
86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio eltoque.com arroja una puntuación técnica de 86/100, lo que corresponde a una calificación de grado B. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, resultando en 6 verificaciones satisfactorias y 3 advertencias, sin detectar fallos críticos que comprometan la disponibilidad inmediata. El sitio web demuestra una base sólida en cuanto a cifrado y protección de datos en tránsito. Sin embargo, se concluye que el sitio es moderadamente seguro pero vulnerable a ataques de inyección y reconocimiento debido a la falta de políticas de seguridad en las cabeceras y la exposición de puertos innecesarios.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
53 dias restantes (expira: 2026-07-13T12:46:43.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-14T11:46:48.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=63072000; includeSubDomains; preload
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **INFO** **Referrer-Policy**
Presente: same-origin
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redirección**
HTTP 301 redirige a https://eltoque.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=63072000; includeSubDomains; preload
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=63072000 (730 días)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Detección CMS — 100/100

Estado: OK

CMS detectado: WordPress

- **INFO** **WordPress**
Detectado via HTML body
- **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** **Tecnologías detectadas**
React, Next.js, Astro

Version CMS Expuesta — 100/100

Estado: OK

No se detectó versión 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, 12 URLs
- 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: Falta — La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso por parte de terceros.

[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: La presencia de este puerto activo sugiere un servidor web alternativo o proxy que podría ser explotado para evadir controles de seguridad estándar.

[MEDIUM] Permissions-Policy: Falta — No se restringe el acceso a las APIs sensibles del navegador, como la cámara, el micrófono o la geolocalización, aumentando el riesgo de privacidad para los usuarios.

[LOW] Server header expuesto: Se detectó el valor Server: cloudflare, lo cual revela información técnica de la infraestructura que facilita el reconocimiento por parte de atacantes.

[LOW] Falta de robots.txt: La carencia de este archivo dificulta la gestión del rastreo de motores de búsqueda y podría permitir la indexación de directorios que deberían permanecer privados.