EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://territoria.cl/es/	Checks	9 pruebas
Dominio	territoria.cl	Hallazgos	45 totales
Fecha	21 de septiembre de 2026 a las 14:15	Problemas	11 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado a la plataforma territoria.cl/es/ arroja una puntuacion de 62/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fueron fallos criticos. El sitio presenta una base solida en su cifrado SSL, pero carece de cabeceras de seguridad fundamentales y expone informacion tecnica sensible. Debido a estas deficiencias en la configuracion del servidor y la gestion del CMS, el sitio se considera actualmente vulnerable ante ataques dirigidos.

Resumen de Riesgos

0	4	5	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 45 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 2 expuesta
Seguridad de Cookies	67	AVISO	qtrans_front_language: falta Secure
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 45 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  45 dias restantes (expira: 2026-11-05T10:13:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-07T09:14:50.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://territoria.cl/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 2 expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 67/100

Estado: AVISO

qtrans_front_language: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: qtrans_front_language — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: qtrans_front_language — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: qtrans_front_language — SameSite**
  SameSite=lax

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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
El analisis de seguridad realizado a la plataforma territoria.cl/es/ arroja una puntuacion de 62/100, lo que equivale a una nota C. Se ejecutaron 9 checks pasivos, de los cuales 3 resultaron satisfactorios, 3 generaron advertencias y 3 fueron fallos criticos. El sitio presenta una base solida en su cifrado SSL, pero carece de cabeceras de seguridad fundamentales y expone informacion tecnica sensible. Debido a estas deficiencias en la configuracion del servidor y la gestion del CMS, el sitio se considera actualmente vulnerable ante ataques dirigidos.

---VULNERABILITIES---

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecucion de scripts no autorizados y ataques de inyeccion de contenido como XSS.
[HIGH] Strict-Transport-Security: La ausencia de HSTS permite que un atacante intente degradar la conexion a HTTP para interceptar datos.
[HIGH] Cookie qtrans_front_language: Falta el flag Secure, permitiendo que la cookie se envie por canales no cifrados y sea vulnerable a interceptacion.
[MEDIUM] Version CMS Expuesta: El archivo /readme.html es accesible publicamente y revela que se utiliza WordPress, facilitando la busqueda de exploits especificos.
[MEDIUM] Ruta /wp-login.php: El panel de acceso administrativo esta expuesto, lo que aumenta el riesgo de ataques de fuerza bruta contra las credenciales.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detecto este puerto abierto, el cual suele alojar servicios secundarios o de gestion que podrian no tener las mismas protecciones que el puerto principal.
[MEDIUM] Referrer-Policy: Falta configurar el control de informacion de procedencia, lo que puede filtrar URLs privadas a sitios de terceros.
[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como la camara o el microfono por scripts maliciosos.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, entregando informacion sobre la infraestructura de red a posibles atacantes.
[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos esenciales, lo que indica una falta de control sobre la indexacion y estructura del sitio.