EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Mtc.treespace.space	Checks	9 pruebas
Dominio	mtc.treespace.space	Hallazgos	49 totales
Fecha	2 de mayo de 2026 a las 05:36	Problemas	16 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en el sitio web ha arrojado una puntuación de 61/100, otorgando una calificación de grado C. Esta evaluación se basó exclusivamente en 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 3 generaron advertencias y 2 fallaron significativamente. Se han identificado riesgos críticos relacionados con la exposición de servicios de infraestructura y la ausencia total de cabeceras de protección en el servidor. Debido a estos hallazgos, el sitio se clasifica actualmente como vulnerable, ya que carece de las defensas básicas contra ataques comunes de interceptación y manipulación de datos.

Resumen de Riesgos

1	7	6	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 77 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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	17	FALLO	XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Se...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 22 (SSH)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 77 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  77 dias restantes (expira: 2026-07-18T16:32:50.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T16:32:51.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.58 (Ubuntu) — 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
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://mtc.treespace.space/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 401

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 — 17/100

Estado: FALLO

XSRF-TOKEN: falta HttpOnly; XSRF-TOKEN: falta Secure; XSRF-TOKEN: falta SameSite; laravel_session: falta Secure; laravel_session: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: XSRF-TOKEN — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: XSRF-TOKEN — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: laravel_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: laravel_session — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: laravel_session — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 22 (SSH), 5432 (PostgreSQL)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto

- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 5432 (PostgreSQL) abierto: La base de datos está expuesta directamente a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Content-Security-Policy faltante: La ausencia de esta cabecera facilita la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options faltante: El sitio no previene ser cargado dentro de frames externos, lo que lo hace vulnerable a ataques de clickjacking.
[HIGH] Strict-Transport-Security (HSTS) no configurado: El servidor no obliga al uso de conexiones cifradas, permitiendo posibles degradaciones de seguridad en la comunicación.
[HIGH] Cookie XSRF-TOKEN insegura: Carece de los flags Secure y HttpOnly, lo que permite que sea interceptada en redes no seguras o accedida mediante scripts.
[HIGH] Cookie laravel_session insegura: No tiene configurado el flag Secure, por lo que la sesión del usuario podría enviarse a través de conexiones no cifradas.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de administración remota es visible para cualquier atacante, aumentando la superficie de exposición del servidor.
[MEDIUM] X-Content-Type-Options faltante: La falta de esta directiva permite que los navegadores ignoren el tipo de contenido enviado, facilitando ataques de tipo MIME-sniffing.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: No se controla la información de navegación compartida ni se restringen las APIs del navegador sensibles.
[MEDIUM] Falta de SameSite en cookies: Tanto XSRF-TOKEN como laravel_session son vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).
[LOW] Cabecera de servidor expuesta: Se revela el uso de Apache/2.4.58 (Ubuntu), proporcionando información valiosa a atacantes sobre el software del sistema.
[LOW] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría estructurada y la indexación correcta de los recursos del sitio.