EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.projectrack.cl	Checks	9 pruebas
Dominio	www.projectrack.cl	Hallazgos	51 totales
Fecha	16 de abril de 2026 a las 20:25	Problemas	10 detectados

A

94/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada en el sitio web obtuvo una puntuación de 94/100 y una calificación final de nota A. Se ejecutaron un total de 9 checks pasivos, resultando en 7 validaciones exitosas, 2 advertencias y 0 fallos críticos. El análisis destaca una excelente implementación de cifrado SSL y cabeceras de seguridad, aunque se identificaron riesgos moderados por exposición de información técnica. Los resultados permiten concluir que el sitio es seguro en su configuración base, pero presenta vulnerabilidades de reconocimiento que deben ser corregidas para evitar ataques dirigidos.

Resumen de Riesgos

0	0	7	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 41 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 41 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  41 dias restantes (expira: 2026-05-27T23:43:05.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-26T23:43:06.000Z
- 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 'self' https:; script-src 'self' 'unsafe-inline' https:; style-src '...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera='none'; microphone='none'; geolocation='none'; payment='none'

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.projectrack.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

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
- INFO **Tecnologias detectadas**
  React

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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 (121221 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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

[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, lo cual facilita a un atacante identificar la tecnología de protección y buscar vulnerabilidades específicas para dicha infraestructura.
[MEDIUM] Archivo /readme.html accesible: Este archivo es accesible públicamente y puede revelar información técnica, versiones del sistema y detalles de configuración que ayudan a perfilar el sitio.
[MEDIUM] Archivo /README.txt accesible: Al igual que el archivo HTML, este documento expone metadatos del sistema que no deberían estar disponibles para usuarios externos.
[MEDIUM] Paneles de login expuestos: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, lo que permite intentos de acceso no autorizado y ataques de fuerza bruta.
[MEDIUM] Bloqueo total en robots.txt: El archivo robots.txt bloquea la indexación de todo el sitio mediante la directiva Disallow: /, lo cual puede ser un error de configuración o indicar un entorno de desarrollo expuesto.
[LOW] Rutas sensibles en robots.txt: Se mencionan términos como admin y config, lo que entrega pistas directas a atacantes sobre la ubicación de directorios críticos.
[MEDIUM] Puerto 8080 abierto: La apertura de este puerto alternativo aumenta la superficie de ataque, pudiendo alojar servicios mal configurados o proxys vulnerables.