

Escanear Vulnerabilidades

Informe de Seguridad Web

URL: https://travesiarollers.cl
Dominio: travesiarollers.cl
Fecha: 22 de abril de 2026 a las 01:16

Checks: 9 pruebas
Hallazgos: 46 totales
Problemas: 8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

Tras realizar la auditoría de seguridad en travesiarollers.cl, se ha obtenido una puntuación de 80/100 con una nota de calificación B. El análisis se basó en 9 checks pasivos, de los cuales 7 resultaron satisfactorios, 1 generó advertencias y 1 fue calificado como fallo crítico. Si bien el sitio demuestra una implementación sólida de cifrado SSL y redirecciones seguras, presenta carencias importantes en la configuración de cabeceras de seguridad. Se concluye que el sitio es moderadamente seguro, pero se considera vulnerable ante ataques de inyección de scripts y suplantación de identidad debido a omisiones en la configuración del servidor.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
90 dias restantes (expira: 2026-07-20T19:37:40.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-21T19:37:41.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, 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
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**
Presente: max-age=31536000
- **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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**
HTTP 301 redirige a <https://travesiarollers.cl/>
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000
- **BAJO** **HSTS includeSubDomains**
HSTS no 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

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (1814 bytes)
- INFO **Reglas robots.txt**
9 Disallow, 2 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
<https://www.travesiarollers.cl/sitemap.xml>
- 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 esta cabecera, la cual es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
- [HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
- [MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo que representa un vector de ataque adicional si el servicio allí alojado no está debidamente protegido.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que podría llevar al navegador a interpretar archivos de forma incorrecta y peligrosa.
- [MEDIUM] Referrer-Policy: No existe una política definida, lo que puede provocar la fuga de información sensible en las URL hacia sitios de terceros.
- [MEDIUM] Permissions-Policy: Falta restringir el acceso a APIs del navegador, permitiendo potencialmente el uso no autorizado de funciones como la cámara o el micrófono.
- [MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio, lo cual puede ser un error de configuración o un intento ineficaz de ocultar directorios.
- [LOW] Server header expuesto: El servidor revela que utiliza Cloudflare, proporcionando información técnica que un atacante puede usar para dirigir sus vectores de explotación.