

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://roesch.cl
Dominio roesch.cl
Fecha 21 de abril de 2026 a las 16:47

Checks 9 pruebas
Hallazgos 47 totales
Problemas 5 detectados

A

96/100

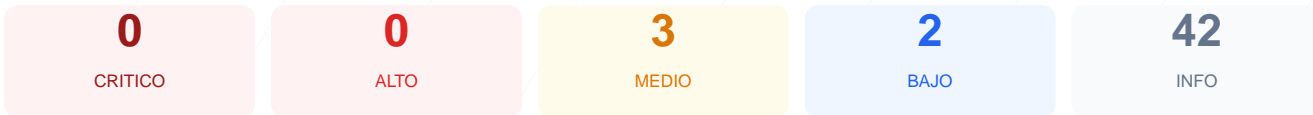
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web roesch.cl arroja una puntuación de 96/100, lo que equivale a una nota de A. Se ejecutaron 9 checks pasivos, de los cuales 8 resultaron correctos y 1 generó una advertencia, sin detectarse fallos críticos. El sitio web demuestra una implementación robusta de cifrado y cabeceras de seguridad fundamentales. En base a los datos obtenidos, se concluye que el sitio es seguro, aunque presenta configuraciones mejorables en la exposición de puertos y políticas de transporte estricto.

Resumen de Riesgos



Resumen de Checks

| | | | |
|------------------------|-----|-------|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 36 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 | 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 36 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
36 dias restantes (expira: 2026-05-27T07:16:43.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-02-26T06:18:15.000Z
- 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 'none'; script-src 'nonce-OzGvIODELft42!su2acQoN' 'unsafe-eval' http...
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=0; includeSubDomains; preload
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: same-origin
- INFO **Permissions-Policy**
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://roesch.cl/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=0; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- MEDIO **HSTS max-age**
max-age=0 (0 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
HTTPS responde con status 403

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 (1848 bytes)
- INFO **Reglas robots.txt**
10 Disallow, 2 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
- INFO **Sitemap en robots.txt**
https://roesch.cl/wp-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

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy abierto puede ser aprovechada para ataques de reconocimiento o acceso a servicios no protegidos.

[MEDIUM] HSTS max-age inadecuado: El valor está configurado en 0 días, lo que invalida la protección contra ataques de degradación de protocolo SSL/TLS.

[MEDIUM] Bloqueo total en robots.txt: Se deniega el rastreo de todo el sitio mediante Disallow: /, lo que puede indicar una configuración de desarrollo o un error de visibilidad.

[LOW] Referencia sensible en robots.txt: La mención directa a rutas como "admin" facilita a potenciales atacantes la identificación de paneles de gestión.

[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, lo cual entrega información técnica sobre la infraestructura de red a terceros.