EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://lbh.rpcontrol.cl	Checks	9 pruebas
Dominio	lbh.rpcontrol.cl	Hallazgos	46 totales
Fecha	25 de abril de 2026 a las 04:08	Problemas	9 detectados

B

86/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio lbh.rpcontrol.cl ha finalizado con una puntuación de 86/100 y una calificación de grado B. Se realizaron un total de 9 comprobaciones pasivas, obteniendo 5 resultados satisfactorios y 4 advertencias, sin detectarse fallos críticos de seguridad inmediatos. No se ejecutó una fase de pentest activo en este escaneo, por lo que los resultados se limitan a la configuración externa y cabeceras. Aunque el cifrado de datos es sólido, la falta de políticas de transporte estricto y la exposición de servicios en puertos alternativos representan riesgos moderados. Se concluye que el sitio es generalmente seguro, pero se encuentra en un estado vulnerable a ataques de intermediario y reconocimiento de infraestructura.

Resumen de Riesgos

0	2	3	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
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	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 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-13T02:37:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-14T02:37:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'none'; script-src 'nonce-qc2ExeLWyYNooK37MhpoGp' 'unsafe-eval' http...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://lbh.rpcontrol.cl/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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)
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- 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 (55955 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
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- 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

[HIGH] Strict-Transport-Security: La cabecera HSTS no está configurada, lo que impide forzar conexiones HTTPS seguras de forma obligatoria en el navegador.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Se detectó un servidor web alternativo o proxy accesible, lo cual incrementa la superficie de ataque del sistema.
[MEDIUM] Archivo /README.txt accesible: Este archivo se encuentra expuesto públicamente y podría revelar información técnica sobre la arquitectura o versiones del sistema.
[MEDIUM] Bloqueo total en robots.txt: El archivo utiliza una instrucción Disallow que bloquea todo el sitio, lo que puede ser una configuración errónea o un intento ineficaz de ocultar directorios.
[LOW] Cabecera Server expuesta: El servidor revela el uso de la tecnología Cloudflare, entregando información útil para que un atacante planifique vectores específicos.
[LOW] Rutas sensibles en robots.txt: El archivo de rastreo menciona explícitamente directorios como admin y config, facilitando la identificación de puntos de entrada críticos.
[LOW] Falta de sitemap.xml: No se encontró el mapa del sitio estructurado, lo que dificulta la auditoría de contenidos y la correcta indexación.
[INFO] Respuesta HTTPS 403: El acceso directo a través de HTTPS devuelve un código de estado prohibido, sugiriendo restricciones de acceso o configuraciones de servidor pendientes.