EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://LIMCHILE.CL	Checks	9 pruebas
Dominio	limchile.cl	Hallazgos	16 totales
Fecha	4 de junio de 2026 a las 16:05	Problemas	2 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación exacta de 84/100 con una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 1 resultado satisfactorio y 1 advertencia, mientras que el resto de los módulos no devolvieron datos por tiempo de espera. Aunque el cifrado de datos es robusto, la exposición de puertos administrativos críticos representa un vector de ataque directo. Debido a estos hallazgos, se concluye que el sitio es actualmente vulnerable a nivel de infraestructura. Es imperativo corregir la visibilidad de los servicios de red para alcanzar un estado de seguridad óptimo.

Resumen de Riesgos

0	1	1	0	14
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Puertos Abiertos	60	AVISO	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-08-12T00:45:18.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-14T00:45:19.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — 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

[HIGH] Puerto 21 (FTP): El puerto está abierto y permite la transferencia de archivos sin cifrar, lo que expone credenciales y datos sensibles a interceptaciones.
[MEDIUM] Puerto 22 (SSH): El servicio de acceso remoto está expuesto públicamente, facilitando posibles ataques de fuerza bruta contra el servidor.