EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://online.bancochile.cl	Checks	9 pruebas
Dominio	online.bancochile.cl	Hallazgos	12 totales
Fecha	10 de abril de 2026 a las 22:04	Problemas	9 detectados

F

20/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio online.bancochile.cl ha arrojado una puntuación de 20/100, lo que equivale a una nota de F. Los resultados de los 9 checks pasivos ejecutados revelan fallos críticos de conectividad y una exposición alarmante de la infraestructura interna, detectándose múltiples puertos de servicios sensibles abiertos a internet. La imposibilidad de verificar cabeceras de seguridad y la configuración de cookies debido a constantes tiempos de espera sugiere una configuración de red inestable o mal gestionada. Tras evaluar los hallazgos, se concluye que el sitio es altamente vulnerable y presenta un riesgo significativo para la integridad de los datos.

Resumen de Riesgos

6	1	2	0	3
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	20	FALLO	9 puertos riesgosos abiertos

Puertos Abiertos — 20/100

Estado: FALLO

9 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — Acceso remoto seguro
- CRITICO **Puerto 23 (Telnet)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — Base de datos PostgreSQL expuesta

- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- CRITICO **Puerto 27017 (MongoDB)**
  ABIERTO — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 23 (Telnet): El servicio de acceso remoto Telnet está abierto y transmite información sin cifrar, lo que permite el robo de credenciales.
[CRITICAL] Puerto 3306 (MySQL): La base de datos MySQL se encuentra expuesta directamente, permitiendo intentos de acceso externo y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP): El protocolo de escritorio remoto de Windows está accesible, siendo el principal vector de entrada para ataques de ransomware.
[CRITICAL] Puerto 5432 (PostgreSQL): Exposición de base de datos relacional que podría comprometer la información almacenada mediante explotación de vulnerabilidades.
[CRITICAL] Puerto 6379 (Redis): El servicio de caché está abierto y, al carecer frecuentemente de autenticación por defecto, permite la extracción de datos sensibles en memoria.
[CRITICAL] Puerto 27017 (MongoDB): La base de datos NoSQL está accesible desde el exterior, facilitando la exfiltración masiva de registros de usuarios.
[HIGH] Puerto 21 (FTP): El protocolo de transferencia de archivos carece de cifrado, exponiendo archivos y claves de acceso durante el tránsito.
[MEDIUM] Puerto 22 (SSH): El acceso por terminal remota está habilitado, aumentando la superficie de ataque frente a intentos de intrusión por fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt): Servicio web alternativo detectado que podría alojar consolas de administración o proxies con configuraciones de seguridad débiles.
[ERROR] Fallos de verificación: Se detectaron errores por timeout que impidieron validar cabeceras HTTP, seguridad de cookies y presencia de contenido mixto.