

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://miportal.hph.cl:8892/
Dominio miportal.hph.cl
Fecha 1 de junio de 2026 a las 14:09

Checks 9 pruebas
Hallazgos 12 totales
Problemas 0 detectados

A

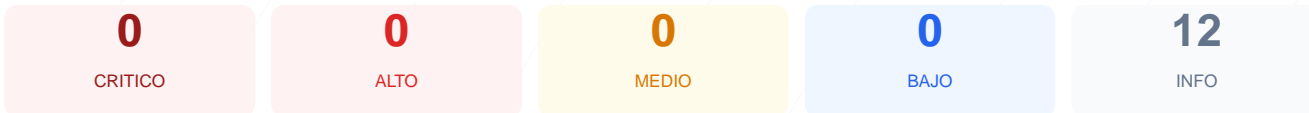
100/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio https://miportal.hph.cl:8892/ ha otorgado una puntuación de 100/100 con una nota final de A. Se ejecutaron un total de 9 checks pasivos, obteniendo 1 resultado exitoso y 0 fallos registrados, aunque diversos módulos presentaron tiempos de espera agotados. No se llevó a cabo un pentest activo, por lo que el análisis se limita a la superficie de exposición externa inmediata. En base a los parámetros técnicos evaluados satisfactoriamente, el sitio se considera seguro. Es fundamental realizar una revisión técnica de la conectividad para validar los puntos que no pudieron ser analizados por latencia.

Resumen de Riesgos



Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
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	100	OK	No se detectaron puertos abiertos

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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 — Envío de correo
- INFO **Puerto 80 (HTTP)**
Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
Cerrado — 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

No se detectaron vulnerabilidades durante los checks pasivos realizados. El sistema de escaneo no reportó fallos, advertencias ni vulnerabilidades de tipo CWE. Debido a la ausencia de un pentest activo, no se descubrieron endpoints de API, subdominios expuestos o cabeceras faltantes adicionales en este informe.