EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://MRED.CL	Checks	9 pruebas
Dominio	mred.cl	Hallazgos	47 totales
Fecha	4 de junio de 2026 a las 16:04	Problemas	15 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio mred.cl ha resultado en una puntuación de 63/100, lo que otorga una calificación de grado C. La evaluación consistió en 9 checks pasivos, de los cuales 5 resultaron correctos, 1 presentó advertencias y 3 fallaron debido a configuraciones críticas de seguridad. Aunque la transmisión de datos está cifrada, la exposición de servicios de bases de datos y el uso de versiones obsoletas representan un riesgo elevado. Se concluye que el sitio es vulnerable y requiere intervenciones urgentes en la configuración del servidor y el mantenimiento del software.

Resumen de Riesgos

2	6	4	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 90 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 4.40 expuesta, WordPress 2 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	20	FALLO	3 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 90 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  90 dias restantes (expira: 2026-09-02T07:34:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-04T07:34:16.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://mred.cl/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Site Kit by Google 1.180.0
- INFO **Tecnologias detectadas**
  Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 4.40 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 4.40 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 (435 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://mred.cl/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

3 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- CRITICO **Puerto 5432 (PostgreSQL)**
  ABIERTO — 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

[CRITICAL] Puerto 3306 (MySQL): La base de datos está expuesta a internet, permitiendo ataques de fuerza bruta o intentos de acceso no autorizado.
[CRITICAL] Puerto 5432 (PostgreSQL): Servicio de base de datos abierto públicamente, lo que facilita la interceptación o manipulación de datos sensibles.
[HIGH] WordPress versión 4.40 expuesta: El uso de una versión obsoleta permite a los atacantes explotar vulnerabilidades conocidas y documentadas.
[HIGH] Puerto 21 (FTP): Este protocolo transfiere credenciales y archivos en texto plano, siendo vulnerable a la interceptación de datos.
[HIGH] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a clickjacking, permitiendo que un atacante cargue la web en marcos invisibles para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security: El servidor no obliga al navegador a usar siempre conexiones seguras, permitiendo ataques de degradación de protocolo.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela información técnica específica que ayuda a un atacante a planificar un vector de intrusión.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es visible para cualquier usuario, facilitando ataques automatizados contra cuentas de gestión.
[MEDIUM] Referrer-Policy no configurada: Se podría filtrar información de navegación a sitios de terceros mediante las cabeceras de los enlaces.
[MEDIUM] Permissions-Policy faltante: No se restringen las capacidades del navegador para acceder a hardware o APIs sensibles.
[LOW] Server header expuesto: El encabezado revela el uso de nginx, lo que ayuda a perfilar la infraestructura para ataques dirigidos.
[LOW] Meta generator expuesto: El código fuente revela el uso de herramientas específicas como Site Kit by Google y la versión del CMS.
[LOW] Ruta sensible en robots.txt: Se mencionan directorios administrativos que sirven de guía para escaneos maliciosos de rutas privadas.