EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mediacionprivadaonline.cl/	Checks	9 pruebas
Dominio	mediacionprivadaonline.cl	Hallazgos	46 totales
Fecha	23 de julio de 2026 a las 04:07	Problemas	15 detectados

C

70/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 70/100 con una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 3 generaron advertencias y 1 se identificó como fallo crítico debido a la ausencia de cabeceras de protección. Aunque el cifrado de datos es correcto, la configuración del servidor presenta brechas que facilitan ataques de interceptación y suplantación de identidad. Se concluye que el sitio es vulnerable ante vectores de ataque web comunes que podrían comprometer la integridad de la navegación de los usuarios.

Resumen de Riesgos

0	4	10	1	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-10-20T05:35:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-22T04:37:52.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — 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)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- 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 308 redirige a https://mediacionprivadaonline.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

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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- 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 (2346 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en iframes, facilitando ataques de clickjacking.
[HIGH] Strict-Transport-Security: No se detectó la política HSTS, lo que impide que el navegador fuerce siempre conexiones seguras HTTPS.
[HIGH] HSTS (Strict-Transport-Security): El servidor no obliga al uso de HTTPS de forma estricta, permitiendo posibles degradaciones de seguridad.
[MEDIUM] X-Content-Type-Options: Falta la configuración para evitar que el navegador realice sniffing de tipos MIME, lo que podría ejecutar scripts disfrazados.
[MEDIUM] Referrer-Policy: No existe control sobre la información de referencia enviada a otros sitios, lo que puede filtrar URLs privadas.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden revelar información técnica sobre la infraestructura.
[MEDIUM] Rutas de login expuestas: Las rutas /wp-login.php, /administrator/ y /user/login son accesibles, facilitando ataques de fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que incrementa la superficie de ataque del servidor.
[MEDIUM] robots.txt: El archivo bloquea la indexación total del sitio, lo cual es una configuración inusual que puede ocultar errores de estructura.
[MEDIUM] Falta de sitemap.xml: La ausencia de este archivo dificulta la auditoría completa de las páginas existentes en el dominio.
[LOW] Server header expuesto: Se revela el uso de Cloudflare, proporcionando información inicial a potenciales atacantes sobre la pila tecnológica.