EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://demo.missr.cl	Checks	9 pruebas
Dominio	demo.missr.cl	Hallazgos	42 totales
Fecha	29 de mayo de 2026 a las 01:36	Problemas	10 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre la plataforma ha dado como resultado una puntuacion de 62/100, lo que otorga una calificacion de nota C. Durante el analisis se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presento advertencias y 3 fallaron en aspectos criticos. Aunque existe un certificado de cifrado valido, se detectaron deficiencias graves en la configuracion de las cabeceras de seguridad y en la gestion del trafico cifrado. Debido a la falta de politicas de seguridad en el navegador y una redireccion defectuosa a HTTPS, se concluye que el sitio es vulnerable ante ataques de interceptacion de datos y ejecucion de scripts maliciosos.

Resumen de Riesgos

0	4	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 85 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 85 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  85 dias restantes (expira: 2026-08-21T14:08:11.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-23T13:08:21.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — La ausencia de esta cabecera permite ataques de scripts cruzados (XSS) e inyeccion de contenido malicioso en el navegador del usuario.
[HIGH] Strict-Transport-Security: Falta — Al no estar configurado el mecanismo HSTS, los usuarios pueden ser forzados a usar conexiones no cifradas vulnerables a interceptacion.
[HIGH] HTTP a HTTPS redireccion: HTTP 403 — El servidor no redirige automaticamente el trafico inseguro hacia el protocolo seguro, bloqueando el acceso en su lugar.
[MEDIUM] X-Content-Type-Options: Falta — Esta carencia permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecucion de archivos maliciosos disfrazados.
[MEDIUM] Permissions-Policy: Falta — El sitio no restringe el acceso a funciones sensibles del dispositivo del usuario como camara, microfono o geolocalizacion a traves de la API del navegador.

[MEDIUM] Puerto 8080 (HTTP-Alt): ABIERTO — La presencia de un servidor web alternativo o proxy abierto aumenta innecesariamente la superficie de ataque del sistema.
[LOW] Server header expuesto: Server: cloudflare — La exposicion de la tecnologia del servidor facilita a un atacante potencial la busqueda de vulnerabilidades especificas de la infraestructura.
[LOW] robots.txt: No encontrado — La falta de este archivo impide una gestion adecuada de la indexacion por parte de los motores de busqueda.
[LOW] sitemap.xml: No encontrado — La ausencia de un mapa del sitio refleja una falta de configuracion estandar en el despliegue del servidor web.