EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fuenzalidaremates.cl	Checks	9 pruebas
Dominio	www.fuenzalidaremates.cl	Hallazgos	50 totales
Fecha	28 de mayo de 2026 a las 19:08	Problemas	8 detectados

A

96/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta un desempeño de seguridad sobresaliente con una puntuación exacta de 96/100 y una calificación de A. Durante la evaluación se ejecutaron 9 comprobaciones pasivas, de las cuales 8 resultaron correctas y 1 generó una advertencia, sin registrarse fallos críticos. El análisis destaca un cumplimiento perfecto en cifrado SSL, cabeceras de seguridad y redirecciones HTTPS. A pesar de la exposición de ciertos archivos informativos y un puerto alternativo, no se detectaron brechas que comprometan la integridad inmediata de los datos. En conclusión, el sitio se considera seguro y bien configurado bajo los estándares de auditoría pasiva.

Resumen de Riesgos

0	0	7	1	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	100	OK	robots.txt y sitemap.xml presentes
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: 2026-08-25T20:10:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-27T20:10:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https:; style-src 'self' '...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.fuenzalidaremates.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- 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
- INFO **Tecnologias detectadas**
  React

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1822 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://gestionfuenzalidaremates.cl/fr/sitemap.xml
- 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

[LOW] Server header expuesto: El encabezado revela el uso de Cloudflare, lo cual facilita a un atacante identificar la tecnología de protección y buscar vectores específicos para evadirla.
[MEDIUM] Archivo /readme.html accesible: Este archivo está disponible públicamente y puede ser utilizado para obtener detalles técnicos sobre la plataforma o versiones de software subyacente.
[MEDIUM] Archivo /README.txt accesible: La exposición de este documento permite a terceros leer metadatos e información de configuración del sistema.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es visible, lo que permite ataques de fuerza bruta dirigidos contra las credenciales de gestión.
[MEDIUM] Ruta /administrator/ expuesta: La interfaz de administración se encuentra accesible, aumentando la superficie de ataque para intentos de acceso no autorizado.
[MEDIUM] Ruta /user/login expuesta: La disponibilidad pública de este endpoint de autenticación facilita el reconocimiento de formularios de entrada por parte de scripts maliciosos.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el sitio, lo cual, además de afectar el SEO, revela una política de ocultación manual que suele atraer el interés de atacantes.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un servidor web alternativo o proxy en este puerto representa un vector de entrada adicional que podría no tener las mismas protecciones que el puerto principal.