EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.muniromeral.cl	Checks	9 pruebas
Dominio	www.muniromeral.cl	Hallazgos	42 totales
Fecha	19 de agosto de 2026 a las 02:36	Problemas	13 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada a muniromeral.cl arrojo una puntuacion de 57/100, lo que equivale a una nota de D. El analisis se baso en 9 checks pasivos, resultando en 5 aprobados, 1 advertencia y 3 fallos criticos de configuracion. Se detectaron servicios de infraestructura expuestos directamente a internet y una ausencia total de politicas de endurecimiento de cabeceras. Debido a la exposicion de la base de datos y la falta de cifrado forzado, el sitio se considera actualmente vulnerable y con un perfil de riesgo elevado.

Resumen de Riesgos

1	6	3	3	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 33 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 33 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  33 dias restantes (expira: 2026-09-20T22:54:24.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-22T22:54:25.000Z
- 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: LiteSpeed — 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- 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

- 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 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- 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
- 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

[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos esta expuesta a internet, permitiendo intentos de conexion externa y ataques de fuerza bruta.
[HIGH] Puerto 21 (FTP) ABIERTO: El servicio de transferencia de archivos no utiliza cifrado, lo que permite la interceptacion de credenciales y datos.
[HIGH] Redireccion HTTPS ausente: El sitio permite conexiones HTTP sin cifrar, facilitando ataques de hombre en el medio para capturar informacion de usuarios.
[HIGH] Content-Security-Policy (CSP) falta: Sin esta cabecera, el sitio es susceptible a ataques de inyeccion de scripts y Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options falta: La ausencia de esta proteccion permite que el sitio sea cargado en marcos externos, facilitando ataques de Clickjacking.
[HIGH] Strict-Transport-Security (HSTS) falta: El servidor no instruye al navegador para usar exclusivamente conexiones seguras, debilitando el SSL.
[MEDIUM] X-Content-Type-Options falta: Permite que el navegador intente adivinar el tipo de contenido, lo que puede llevar a la ejecucion de archivos maliciosos disfrazados.

[MEDIUM] Referrer-Policy falta: No se controla la cantidad de informacion de navegacion que se envia a otros sitios web al seguir enlaces.
[MEDIUM] Permissions-Policy falta: No existen restricciones sobre que funciones del navegador (como camara o ubicacion) pueden ser activadas por el sitio.
[LOW] Server header expuesto (LiteSpeed): Se revela la tecnologia exacta del servidor, facilitando que un atacante busque vulnerabilidades especificas para ese software.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La falta de estos archivos dificulta la auditoria de indexacion y el control de rastreo de motores de busqueda.