EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mundotuerka.cl/	Checks	9 pruebas
Dominio	mundotuerka.cl	Hallazgos	44 totales
Fecha	15 de junio de 2026 a las 17:39	Problemas	10 detectados

C

74/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web mundotuerka.cl arroja una puntuación de 74/100 con una calificación final de C. Se ejecutaron 9 comprobaciones pasivas, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos en la configuración. Aunque el cifrado de datos en tránsito es correcto, la exposición de servicios internos y la ausencia de políticas de seguridad en el navegador reducen la protección global. El sitio se considera vulnerable debido a la visibilidad pública de su base de datos y puertos administrativos. Es necesaria una intervención técnica inmediata para mitigar los riesgos de acceso no autorizado identificados.

Resumen de Riesgos

1	4	3	2	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	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 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-08-22T17:33:03.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-24T17:33:04.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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)
- 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://mundotuerka.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

- 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (283 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 3 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://mundotuerka.cl/sitemap.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
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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 está expuesta directamente a internet, permitiendo intentos de conexión externa y ataques de fuerza bruta.
[HIGH] Content-Security-Policy (CSP) ausente: La falta de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no obliga al navegador a usar HTTPS, dejando la conexión susceptible a ataques de degradación de protocolo (Downgrade attacks).
[HIGH] Puerto 21 (FTP) abierto: El protocolo de transferencia de archivos no está cifrado, lo que permite la interceptación de credenciales y datos en la red.
[MEDIUM] Puerto 22 (SSH) abierto: El servicio de acceso remoto es visible, lo que aumenta la superficie de ataque frente a intentos de intrusión al sistema operativo.
[MEDIUM] Referrer-Policy ausente: No se controla qué información de procedencia se envía a otros sitios, pudiendo filtrar rutas internas de la web.
[MEDIUM] Permissions-Policy ausente: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, micrófono o geolocalización.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: Apache, revelando la tecnología utilizada y facilitando la búsqueda de exploits específicos.
[LOW] Ruta sensible en robots.txt: Se menciona la ruta admin en el archivo público, lo que orienta a posibles atacantes sobre la ubicación del panel de administración.