EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.municipalidadnancagua.cl/	Checks	9 pruebas
Dominio	www.municipalidadnancagua.cl	Hallazgos	44 totales
Fecha	2 de mayo de 2026 a las 00:23	Problemas	13 detectados

C

60/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación de 60/100, lo que equivale a una calificación de nota C. Se ejecutaron un total de 9 controles pasivos, de los cuales 4 resultaron exitosos, 2 generaron advertencias y 3 fallaron críticamente. El análisis revela una ausencia total de cabeceras de seguridad esenciales y la exposición de versiones desactualizadas del sistema de gestión de contenidos. Debido a la combinación de software expuesto y la falta de protecciones en el servidor, se concluye que el sitio es actualmente vulnerable a ataques de inyección y suplantación.

Resumen de Riesgos

0	5	5	3	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 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	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-07-14T06:02:37.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-15T06:02:38.000Z
- 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

- 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 301 redirige a https://www.municipalidadnancagua.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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.portaltransparencia.cl/PortalPdT/pdtta?codOrganis...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.portaltransparencia.cl/PortalPdT/web/guest/direct...

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 — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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
- 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

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de ataques XSS y la inyección de contenido malicioso.
[HIGH] X-Frame-Options: No configurada, dejando el sitio vulnerable a ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: Ausente, lo que impide que el navegador fuerce siempre conexiones seguras mediante HSTS.
[HIGH] WordPress version: La versión 6.9.4 se encuentra expuesta públicamente, permitiendo a posibles atacantes identificar y explotar CVEs específicos conocidos.
[MEDIUM] X-Content-Type-Options: Falta la configuración para evitar que el navegador interprete archivos con tipos MIME incorrectos (sniffing).
[MEDIUM] Referrer-Policy: No se detectó esta cabecera, lo que compromete la privacidad de los datos de navegación enviados a otros sitios.

[MEDIUM] Permissions-Policy: Ausente, lo que significa que no hay restricciones sobre el uso de APIs del navegador como cámara o micrófono.
[MEDIUM] Recurso HTTP (Contenido Mixto): Se detectaron dos hojas de estilo cargando desde enlaces inseguros de portaltransparencia.cl dentro del sitio HTTPS.
[LOW] Meta generator: La etiqueta expone directamente el uso de WordPress 6.9.4, facilitando el reconocimiento para ataques automatizados.
[LOW] robots.txt: No se encontró el archivo en el servidor, dificultando el control de los rastreadores de búsqueda.
[LOW] sitemap.xml: El archivo no está presente, lo que afecta la indexación y visibilidad de la estructura del sitio.