EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://zonaradios.cl	Checks	9 pruebas
Dominio	zonaradios.cl	Hallazgos	50 totales
Fecha	15 de mayo de 2026 a las 07:02	Problemas	6 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 85/100 con una calificación final de grado B. Se ejecutaron 9 verificaciones pasivas de seguridad, de las cuales 7 resultaron aprobadas, 1 presentó advertencias y 1 fue calificada como fallo crítico. La infraestructura demuestra una implementación robusta en el cifrado de datos y redirecciones seguras, aunque presenta deficiencias importantes en la protección de cabeceras y gestión de cookies. En su estado actual, el sitio se considera seguro para la navegación general, pero vulnerable ante ataques dirigidos de inyección de scripts y secuestro de sesiones.

Resumen de Riesgos

0	3	1	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	33	FALLO	csrftoken: falta HttpOnly; csrftoken: falta Secu...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-08-07T01:16:43.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-09T01:16:44.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://zonaradios.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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**
  Next.js

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 — 33/100

Estado: FALLO

csrftoken: falta HttpOnly; csrftoken: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: csrftoken — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: csrftoken — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: csrftoken — SameSite**
  SameSite=lax

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 (103 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://zonaradios.cl/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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 crítica que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Cookie csrftoken (HttpOnly): La cookie carece del flag HttpOnly, lo que permite que sea accesible mediante scripts del navegador y facilita el robo de sesiones.
[HIGH] Cookie csrftoken (Secure): La cookie no tiene habilitado el flag Secure, permitiendo que se envíe a través de conexiones no cifradas en ciertos escenarios.
[MEDIUM] Permissions-Policy: Ausencia de políticas para restringir el acceso del navegador a APIs sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de nginx, proporcionando información técnica que un atacante podría usar para buscar vulnerabilidades específicas del software.
[LOW] Ruta sensible en robots.txt: Se identifica una referencia al directorio "admin", lo cual expone rutas administrativas potenciales a atacantes y rastreadores.