EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.carolinalainez.cl/	Checks	9 pruebas
Dominio	www.carolinalainez.cl	Hallazgos	37 totales
Fecha	29 de abril de 2026 a las 19:03	Problemas	8 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web carolinalainez.cl ha resultado en una puntuación de 75/100, obteniendo una nota de B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 5 finalizaron con éxito, uno presentó advertencias y uno se clasificó como fallo debido a la carencia de protecciones esenciales. A pesar de contar con un cifrado de transporte robusto, la ausencia de cabeceras de seguridad críticas incrementa el riesgo frente a ataques de interceptación y manipulación de contenido. En conclusión, el sitio es funcionalmente seguro para la navegación básica, pero se considera vulnerable ante ataques dirigidos por falta de endurecimiento (hardening) en el servidor.

Resumen de Riesgos

0	4	2	2	29
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 55 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 55 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  55 dias restantes (expira: 2026-06-23T19:26:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-25T19:26:47.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy

- BAJO **Server header expuesto**
  Server: Apache — 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
- INFO **Permissions-Policy**
  Presente: private-state-token-redemption=(self "https://www.google.com" "https://www.gstat...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://carolinalainez.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: All in One SEO (AIOSEO) 4.9.6.2

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

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: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles.
[HIGH] Strict-Transport-Security: La falta de HSTS permite que un atacante degrade la conexión de HTTPS a HTTP para interceptar datos.
[HIGH] HSTS no configurado: El navegador no tiene instrucciones para forzar siempre una conexión segura, dejando una ventana de vulnerabilidad en la redirección inicial.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, lo que podría llevar a la ejecución de archivos no ejecutables.
[MEDIUM] Referrer-Policy: No se controla qué información de procedencia se envía a otros sitios, lo que puede exponer rutas internas privadas.
[LOW] Server header expuesto: El servidor revela que utiliza Apache, información que ayuda a potenciales atacantes a buscar vulnerabilidades específicas para esa tecnología.
[LOW] Meta generator expuesto: El sitio revela el uso de All in One SEO 4.9.6.2, lo que permite a atacantes conocer versiones específicas de plugins de WordPress.