EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.pentavida.cl/	Checks	9 pruebas
Dominio	www.pentavida.cl	Hallazgos	47 totales
Fecha	11 de junio de 2026 a las 00:21	Problemas	5 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web arroja una puntuación técnica de 88/100, obteniendo una calificación final de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, se identificó 1 advertencia y se registró 1 fallo crítico de seguridad. Aunque la infraestructura de cifrado y las cabeceras de protección son robustas, la exposición de software desactualizado representa un riesgo latente. En su estado actual, el sitio se considera mayormente seguro, pero vulnerable ante ataques dirigidos que exploten vulnerabilidades conocidas en versiones antiguas del CMS.

Resumen de Riesgos

0	1	2	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 171 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 5.5.3 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 171 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  171 dias restantes (expira: 2026-11-28T14:21:01.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-13T14:21:01.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: frame-src 'self' *.pentavida.cl pentavida.cl *.google.com google.com *.livechati...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=4838400; includeSubdomains;
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: same-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyros...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.pentavida.cl/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=4838400; includeSubdomains;
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- MEDIO **HSTS max-age**
  max-age=4838400 (56 dias) — Recomendado minimo 180 dias
- 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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.5.3 expuesta

- ALTO **WordPress version**
  Version 5.5.3 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 — 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 (330 bytes)
- INFO **Reglas robots.txt**
  8 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.pentavida.cl/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] WordPress version: la versión 5.5.3 se encuentra expuesta públicamente, lo que facilita a los atacantes la identificación de exploits y CVEs específicos para este núcleo.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: la presencia de un servidor web alternativo o proxy en este puerto aumenta la superficie de ataque y posibles accesos no autorizados.
[MEDIUM] HSTS max-age: la configuración actual de 56 días es inferior al estándar recomendado de 180 días, reduciendo el periodo de protección de transporte estricto.
[LOW] Server header expuesto: se revela el uso de Cloudflare como tecnología de servidor, lo cual asiste a los atacantes en la fase de reconocimiento.
[LOW] Ruta sensible en robots.txt: el archivo hace referencia directa a rutas de administración, guiando a posibles atacantes hacia paneles sensibles del sitio.