EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Www.pjud.cl	Checks	9 pruebas
Dominio	www.pjud.cl	Hallazgos	54 totales
Fecha	11 de abril de 2026 a las 00:03	Problemas	13 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio pjud.cl ha arrojado una puntuación de 72/100, lo que corresponde a una calificación de grado C. Se ejecutaron un total de 9 chequeos pasivos, de los cuales 5 resultaron satisfactorios y 4 presentaron fallos de diversa gravedad. A pesar de contar con un cifrado SSL robusto y cabeceras de seguridad correctamente configuradas, se detectaron deficiencias críticas en la gestión de cookies y obsolescencia de software. Debido a la exposición de una versión de WordPress vulnerable y la presencia de contenido mixto, el sitio se considera vulnerable bajo los estándares actuales de ciberseguridad.

Resumen de Riesgos

0	4	6	3	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 170 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	No se detecto un CMS conocido
Version CMS Expuesta	20	FALLO	WordPress 1.1 expuesta
Seguridad de Cookies	17	FALLO	csrfToken: falta Secure; csrfToken: falta SameSi...
Contenido Mixto	20	FALLO	12 recursos 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 170 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  170 dias restantes (expira: 2026-09-27T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-13T00:00:00.000Z
- 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: Apache — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests;
- 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: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=self

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.pjud.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 — 20/100

Estado: FALLO

WordPress 1.1 expuesta

- ALTO **WordPress version**
  Version 1.1 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 — 17/100

Estado: FALLO

csrfToken: falta Secure; csrfToken: falta SameSite; f5_cspm: falta HttpOnly; f5_cspm: falta Secure; f5_cspm: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: csrfToken — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: csrfToken — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: csrfToken — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: f5_cspm — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: f5_cspm — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: f5_cspm — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 20/100

Estado: FALLO

12 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.poderjudicialtv.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.poderjudicialtv.cl/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://ojv.pjud.cl/kpitec-ojv-web/tramite_facil?tramite=rece...
- MEDIO **href (link/stylesheet)**
  ...y 9 mas del mismo tipo

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] WordPress versión 1.1 expuesta: Se detectó una versión extremadamente obsoleta del CMS, lo que permite a atacantes buscar y explotar CVEs conocidos para comprometer el servidor.
[HIGH] Cookie f5_cspm falta HttpOnly: La ausencia de este flag permite que la cookie sea accesible mediante scripts del lado del cliente, aumentando significativamente el riesgo de ataques XSS.
[HIGH] Cookies csrfToken y f5_cspm falta Secure: Estas cookies se envían a través de conexiones no cifradas, lo que permite la interceptación de datos de sesión en redes inseguras.
[MEDIUM] Cookies csrfToken y f5_cspm falta SameSite: La carencia de este atributo hace que las sesiones de los usuarios sean susceptibles a ataques de falsificación de solicitudes en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto detectado: Existen 12 recursos que se cargan mediante HTTP en una página servida por HTTPS, lo que debilita la integridad de la conexión y permite ataques de degradación.
[LOW] Cabecera Server expuesta: El servidor revela que utiliza Apache, proporcionando información valiosa a posibles atacantes sobre la tecnología subyacente.
[LOW] Ausencia de archivos de indexación: No se encontraron robots.txt ni sitemap.xml, lo que impacta negativamente en la administración del sitio y su visibilidad controlada.