

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://www.ayudaparajosepascual.com  
Dominio www.ayudaparajosepascual.com  
Fecha 25 de abril de 2026 a las 20:41

Checks 9 pruebas  
Hallazgos 47 totales  
Problemas 9 detectados

# B

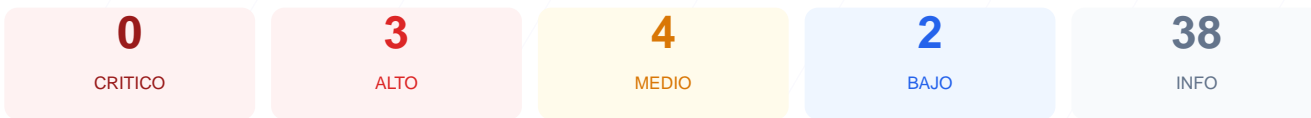
## 76/100

puntos de seguridad

### RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio web arroja una puntuacion de 76/100 con una calificacion de grado B. Se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 presentaron fallos criticos relacionados con la exposicion de informacion y falta de endurecimiento del servidor. No se realizo un pentest activo, por lo que el analisis se limita a la superficie visible y configuraciones de red. El sitio cuenta con una base solida de cifrado, pero se considera vulnerable a ataques de inyeccion y clickjacking debido a la ausencia de cabeceras de seguridad esenciales. Se recomienda una intervencion tecnica inmediata para mitigar los riesgos identificados en la infraestructura WordPress.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 61 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 6.9.4 expuesta, WordPress 2 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	100	OK	2 puerto(s) abierto(s), todos esperados

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 61 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
61 dias restantes (expira: 2026-06-25T15:31:42.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-03-27T15:31:43.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-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
- **ALTO** **X-Frame-Options**  
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**  
Presente: max-age=31536000
- **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 — 100/100

---

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- **INFO** **HTTP !' HTTPS redireccion**  
HTTP 301 redirige a <https://www.ayudaparajosepascual.com/>
- **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

CMS detectado: WordPress

- **INFO** **WordPress**  
Detectado via HTML body
- **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 6.9.4 expuesta, WordPress 2 expuesta

- **ALTO** **WordPress version**  
Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- **MEDIO** **Archivo /readme.html**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS

- 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 (180 bytes)
- INFO **Reglas robots.txt**  
1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**  
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**  
<https://ayudaparajosepascual.com/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 lo que permite ataques de cross-site scripting (XSS) e inyeccion de contenido malicioso.

[HIGH] X-Frame-Options: La ausencia de esta directiva hace que el sitio sea susceptible a ataques de clickjacking, permitiendo que sea cargado en marcos externos no autorizados.

[HIGH] WordPress version: La version 6.9.4 se encuentra expuesta publicamente, facilitando a atacantes la identificacion de vulnerabilidades conocidas (CVEs) para dicha version.

[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecucion de archivos no ejecutables como scripts.

[MEDIUM] Referrer-Policy: No se controla la informacion de referencia enviada, lo que podria filtrar datos de navegacion privados hacia otros dominios.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la camara, el microfono o la geolocalizacion desde el cliente.

[MEDIUM] Archivo /readme.html: Este archivo es accesible publicamente y puede revelar detalles especificos de la instalacion del CMS y sus dependencias.

[LOW] Server header expuesto: La cabecera revela el uso de tecnologia nginx, proporcionando informacion util para el reconocimiento de la infraestructura por parte de terceros.

[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas de administracion, lo que orienta a posibles atacantes sobre la ubicacion de paneles de control.