

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL: https://securitypyme.com/  
Dominio: securitypyme.com  
Fecha: 12 de mayo de 2026 a las 15:48

Checks: 9 pruebas  
Hallazgos: 45 totales  
Problemas: 11 detectados

# B

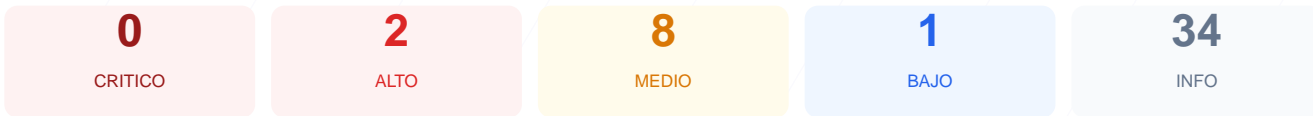
## 80/100

puntos de seguridad

### RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el dominio analizado arroja una puntuación de 80/100, lo que equivale a una nota de B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 7 resultados satisfactorios y 2 fallos críticos relacionados con la configuración de cabeceras y archivos de sistema. Aunque el cifrado y la redirección de tráfico son correctos, la ausencia de políticas de seguridad en el navegador incrementa el riesgo de ataques dirigidos. En conclusión, el sitio web es mayoritariamente sólido en su infraestructura base, pero se considera vulnerable ante ataques de inyección y suplantación por falta de endurecimiento en sus configuraciones.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 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	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 72 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
72 dias restantes (expira: 2026-07-23T16:55:10.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-24T16:55:11.000Z
- 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: Vercel — 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=63072000
- **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 308 redirige a https://securitypyme.com/
- **INFO** **HSTS (Strict-Transport-Security)**  
HSTS activo: max-age=63072000
- **BAJO** **HSTS includeSubDomains**  
HSTS no cubre subdominios
- **INFO** **HSTS max-age**  
max-age=63072000 (730 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

## Version CMS Expuesta — 100/100

---

Estado: OK

No se detecto version de CMS expuesta

- **MEDIO** **Archivo /readme.html**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- **MEDIO** **Archivo /README.txt**  
Archivo accesible publicamente — Puede revelar version e informacion del CMS
- **MEDIO** **Ruta /wp-login.php**  
Panel de login accesible publicamente

- MEDIO** Ruta /administrator/  
Panel de login accesible publicamente
- MEDIO** Ruta /user/login  
Panel de login accesible publicamente
- INFO** Version CMS  
No se detecta ninguna version expuesta

## 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- INFO** security.txt  
Presente en /.well-known/security.txt — Buena practica

## 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: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: La falta de esta política hace que el sitio sea susceptible a ataques de clickjacking, donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría intentar interpretar el contenido de forma distinta a la declarada, permitiendo la ejecución de código malicioso mediante MIME-sniffing.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría exponer datos de navegación privados.

[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.

[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, lo que podría revelar detalles técnicos sobre la estructura interna.

[MEDIUM] Rutas administrativas accesibles: Se detectó acceso público a múltiples paneles de gestión como /wp-login.php, /administrator/ y /user/login, aumentando el riesgo de ataques de fuerza bruta.

[LOW] Server header expuesto: El encabezado Server revela el uso de tecnología Vercel, proporcionando información útil para un atacante en la fase de reconocimiento.

[LOW] Ausencia de archivos de indexación: La falta de robots.txt y sitemap.xml dificulta la gestión del rastreo por parte de motores de búsqueda y la exclusión de áreas privadas.