

EscanearVulnerabilidades

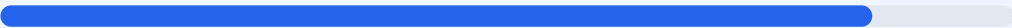
Informe de Seguridad Web

URL	https://www.comrapues.com.py	Checks	9 pruebas
Dominio	www.comrapues.com.py	Hallazgos	49 totales
Fecha	27 de abril de 2026 a las 11:58	Problemas	10 detectados

B

86/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web ha resultado en una puntuación de 86/100 con una calificación de grado B. Se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios, 3 advertencias y 0 fallos críticos. El portal demuestra una implementación sólida en cuanto a cifrado de datos y protocolos de transporte seguro. Sin embargo, se han detectado configuraciones mejorables en las cabeceras de respuesta y la exposición de rutas administrativas. Se concluye que el sitio es generalmente seguro, pero presenta vulnerabilidades de severidad media y alta que deben ser mitigadas.

Resumen de Riesgos

0	1	8	1	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 72 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

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: 2026-07-08T22:44:53.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-09T22:44:54.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- ALTO

Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=15552000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: no-referrer-when-downgrade
- 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.comprapues.com.py/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=15552000 (180 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
React

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO

robots.txt
Presente (1738 bytes)
- INFO

Reglas robots.txt
9 Disallow, 1 Allow
- MEDIO

Bloqueo total
robots.txt bloquea todo el sitio con Disallow: /
- INFO

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

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, aumentando el riesgo de ataques XSS e inyección de contenido.
- [MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo puede ser utilizada para acceder a servicios internos o proxies mal configurados.
- [MEDIUM] Rutas de administración expuestas (/wp-login.php, /administrator/, /user/login): El acceso público a estos paneles facilita ataques de fuerza bruta y reconocimiento de infraestructura.
- [MEDIUM] Archivos informativos accesibles (/readme.html, /README.txt): Estos documentos pueden revelar versiones de software y detalles técnicos que asisten a un atacante en la fase de explotación.
- [MEDIUM] Permissions-Policy: La falta de esta directiva no restringe el uso de APIs sensibles del navegador como la cámara o el micrófono.
- [MEDIUM] Configuración de Robots.txt: El archivo bloquea el rastreo completo del sitio mediante Disallow: /, lo que puede afectar la visibilidad y sugiere una configuración defensiva incompleta.
- [LOW] Cabecera Server expuesta: El servidor revela el uso de la tecnología Cloudflare, lo cual proporciona información técnica útil para perfilar posibles ataques.