

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://wallcarty.com
Dominio wallcarty.com
Fecha 14 de mayo de 2026 a las 23:25

Checks 9 pruebas
Hallazgos 46 totales
Problemas 16 detectados

D

59/100

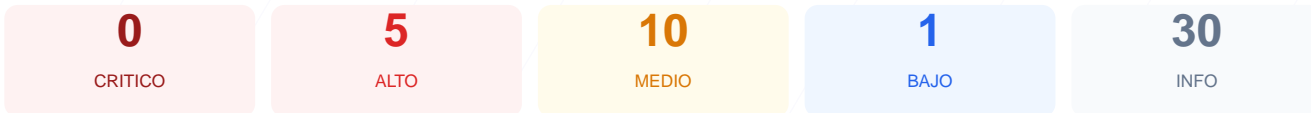
puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al dominio analizado arroja una puntuación de 59/100, lo que corresponde a una calificación de grado D. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallaron críticamente por la ausencia total de medidas de endurecimiento. A pesar de contar con un cifrado SSL válido, la carencia de cabeceras de seguridad y la exposición de rutas administrativas representan un riesgo significativo. Se concluye que el sitio es actualmente vulnerable y requiere correcciones inmediatas para proteger la integridad de la plataforma y sus usuarios.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
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 58 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
58 dias restantes (expira: 2026-07-11T14:54:15.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-12T13:54:17.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-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
- **ALTO** **X-Frame-Options**
Falta — Protege contra clickjacking
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **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 — 0/100

Estado: **FALLO**

No hay redireccion HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redireccion**
HTTP 200 — No redirige a HTTPS
- **ALTO** **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- **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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
Presente (2528 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: Falta esta cabecera crítica que previene ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
- [HIGH] X-Frame-Options: La ausencia de esta directiva permite que el sitio sea cargado en frames, facilitando ataques de clickjacking.
- [HIGH] Strict-Transport-Security: No se implementa HSTS, lo que impide forzar conexiones seguras y deja la comunicación expuesta a ataques de degradación.
- [HIGH] Redirección HTTPS ausente: El servidor permite el acceso mediante HTTP sin redirigir al protocolo seguro, permitiendo la interceptación de datos.
- [MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que los navegadores realicen sniffing de tipos MIME, aumentando el riesgo de ejecución de scripts.
- [MEDIUM] Referrer-Policy: No se controla la información enviada en la cabecera referer al navegar hacia otros dominios.
- [MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a hardware como cámara o micrófono.
- [MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos internos.
- [MEDIUM] Paneles de login accesibles: Se detectaron rutas de administración como /wp-login.php, /administrator/ y /user/login expuestas a intentos de intrusión.
- [MEDIUM] Puerto 8080 abierto: El servicio HTTP-Alt está activo, lo que expande innecesariamente la superficie de ataque del servidor.
- [MEDIUM] Configuración de Robots.txt: El archivo bloquea el rastreo completo del sitio mediante Disallow: /, lo que puede indicar una configuración defensiva mal aplicada.
- [LOW] Server header expuesto: El servidor revela el uso de Cloudflare, entregando información técnica que puede ser utilizada para dirigir ataques específicos.