

Escanear Vulnerabilidades

Informe de Seguridad Web

URL: https://quantumcart.store/
Dominio: quantumcart.store
Fecha: 18 de junio de 2026 a las 02:05

Checks: 9 pruebas
Hallazgos: 45 totales
Problemas: 6 detectados

A

96/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 96/100, lo que equivale a una nota A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 8 resultaron satisfactorios y solo 1 presentó fallos críticos de configuración. Se han detectado rutas administrativas expuestas y archivos de información técnica accesibles que podrían facilitar el reconocimiento por parte de atacantes. A pesar de estos hallazgos, la implementación de cifrado y cabeceras de seguridad es excelente. En conclusión, el sitio es seguro para su uso operativo, aunque requiere ajustes menores para mitigar riesgos de enumeración.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 83 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	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 83 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
83 dias restantes (expira: 2026-09-09T05:36:18.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-06-11T05:36:19.000Z
- 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: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
Presente: default-src 'self'; base-uri 'self'; connect-src 'self'; font-src 'self' data; ...
- INFO **X-Frame-Options**
Presente: DENY
- INFO **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
Presente: camera=(), microphone=(), geolocation=()

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://quantumcart.store/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
HSTS 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

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

[LOW] Server header expuesto: El encabezado revela el uso de nginx, permitiendo a potenciales atacantes identificar la tecnologia del servidor y buscar vulnerabilidades especificas de la version.

[MEDIUM] Archivo /readme.html accesible: Este archivo se encuentra disponible publicamente y puede revelar información técnica sobre la estructura o versiones del sitio.

[MEDIUM] Archivo /README.txt accesible: Documento accesible que suele contener datos de instalación o configuración que no deberían ser públicos.

[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es visible, lo que aumenta el riesgo de ataques de fuerza bruta o de diccionario.

[MEDIUM] Ruta /administrator/ expuesta: Interfaz de administración accesible desde internet, lo que representa un vector de ataque directo hacia el control del sitio.

[MEDIUM] Ruta /user/login expuesta: Punto de autenticación de usuarios expuesto que podría ser explotado si no cuenta con protecciones de tasa de límite o segundo factor.

[MEDIUM] Ausencia de Robots.txt y Sitemap: El sitio carece de instrucciones para motores de búsqueda, lo que impide una indexación controlada y puede exponer directorios no deseados.