

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.purityshop.site/	Checks	9 pruebas
Dominio	www.purityshop.site	Hallazgos	46 totales
Fecha	15 de septiembre de 2026 a las 15:06	Problemas	5 detectados

A

91/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web arroja una puntuación de 91/100 con una calificación final de nota A. Durante el análisis se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, se emitió 1 advertencia técnica y se detectó 1 fallo de configuración. Aunque la infraestructura de cifrado y transporte de datos es excelente, existen omisiones en las políticas de seguridad de contenido y en la exposición de metadatos del servidor. El sitio muestra un nivel de seguridad sólido, pero se considera parcialmente vulnerable a ataques de inyección debido a la falta de cabeceras de seguridad específicas. En conclusión, www.purityshop.site es un sitio seguro para el usuario final, aunque requiere ajustes técnicos preventivos.

Resumen de Riesgos

0	1	0	4	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	75	AVISO	5/6 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	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 60 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
60 dias restantes (expira: 2026-11-14T16:36:41.000Z)
- INFO Fecha de emision
Emitido desde: 2026-08-16T16:36:42.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

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

- BAJO

X-Powered-By expuesto
X-Powered-By: Next.js — Revela framework/lenguaje
- ALTO

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

X-Frame-Options
Presente: DENY
- INFO

Strict-Transport-Security
Presente: max-age=63072000
- 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 308 redirige a https://www.purityshop.site/
- 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
- INFO

Tecnologias detectadas
React, Next.js, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)

- INFO

Archivo /README.txt
No accesible (correcto)
- 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

- BAJO

robots.txt
No encontrado (HTTP 404)
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- 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: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado.

[LOW] Server header expuesto: El servidor revela el valor Server: Vercel, lo cual facilita a un atacante potencial la identificación de la infraestructura para buscar exploits específicos.

[LOW] X-Powered-By expuesto: Se detectó el valor X-Powered-By: Next.js, exponiendo el framework de desarrollo utilizado y reduciendo el esfuerzo necesario para un reconocimiento técnico.

[LOW] robots.txt: La ausencia de este archivo genera un error 404, impidiendo dar instrucciones correctas a los motores de búsqueda sobre el rastreo del sitio.

[LOW] sitemap.xml: No se encontró el mapa del sitio, lo que dificulta la correcta indexación de la estructura web y el análisis de su jerarquía de contenidos.