

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://santopazaccesorios.com/
Dominio santopazaccesorios.com
Fecha 7 de mayo de 2026 a las 13:46

Checks 9 pruebas
Hallazgos 49 totales
Problemas 8 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el sitio web ha dado como resultado una puntuación de 87/100, lo que equivale a una nota B. Se completaron exitosamente 9 checks pasivos, identificando 8 componentes correctamente configurados y 1 fallo crítico en la implementación de políticas de seguridad. El sitio presenta una base robusta en cuanto a cifrado y gestión de certificados, pero muestra debilidades significativas en la protección contra ataques de inyección y manipulación de interfaz. En conclusión, el sitio se considera seguro en su infraestructura de red, pero vulnerable a ataques dirigidos a los usuarios finales debido a la ausencia de cabeceras de seguridad esenciales.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 54 dias
Cabeceras de Seguridad	35	FALLO	Solo 2/6 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 54 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
54 dias restantes (expira: 2026-06-30T13:12:06.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-01T13:12:07.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 35/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: openresty — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: Express — Revela framework/lenguaje
- **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=15552000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniff
- **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 301 redirige a https://santopazaccesorios.com/
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=15552000; includeSubDomains
- **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**
Next.js, Express

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (624 bytes)
- INFO **Reglas robots.txt**
8 Disallow, 1 Allow
- MEDIO **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
<https://santopazaccesorios.com/sitemap.xml>
- 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 scripts no autorizados, aumentando el riesgo de ataques Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Al no estar presente, el sitio es vulnerable a ataques de Clickjacking donde un atacante puede cargar la web en un marco invisible para engañar al usuario.

[MEDIUM] Referrer-Policy: La falta de esta directiva impide controlar la información de procedencia que el navegador envía a terceros, lo que podría comprometer la privacidad.

[MEDIUM] Permissions-Policy: No se han restringido las APIs del navegador, lo que permite potencialmente el acceso de scripts a funciones como la cámara o el micrófono.

[MEDIUM] Configuración de Robots.txt: El archivo bloquea la indexación de todo el sitio y expone la ruta admin, lo que facilita el reconocimiento de paneles de gestión a posibles atacantes.

[LOW] Server header expuesto: El servidor revela el uso de Openresty, proporcionando información técnica que ayuda a un atacante a buscar vulnerabilidades específicas del software.

[LOW] X-Powered-By expuesto: Se detecta el uso del framework Express, lo cual facilita la identificación de la tecnología utilizada en el desarrollo del sitio.