EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://garciacarrion.com/pages/don-simon?srsltid=AfmBOoqPUdCdSuLSHPvrbx0yn9tpMeb0eElFpxdjFvQPqGtnMDXkK	Checks	9 ejecutados
Dominio	garciacarrion.com	Hallazgos	69 totales
Fecha	18 de abril de 2026 a las 10:51	Problemas	15 detectados

B

87/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web arroja una puntuación de 87/100, lo que equivale a una nota de B. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias debido a configuraciones incompletas. Se han detectado debilidades importantes en la gestión de cookies y en la exposición de servicios en puertos alternativos. A pesar de contar con un cifrado SSL robusto, la plataforma presenta vulnerabilidades en la privacidad de las sesiones que impiden calificarla como totalmente segura. En conclusión, el sitio es mayoritariamente seguro pero vulnerable a ataques de interceptación de datos y scripting si no se aplican las correcciones recomendadas.

Resumen de Riesgos

0	8	5	2	54
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 76 dias
Cabeceras de Seguridad	75	AVISO	4/6 presentes. Faltan: Referrer-Policy, Permissi...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: Shopify
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	62	AVISO	localization: falta HttpOnly; localization: falt...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 76 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  76 dias restantes (expira: 2026-07-03T13:36:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-04T13:36:35.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

4/6 presentes. Faltan: Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=7889238
- 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://garciacarrion.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=7889238
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=7889238 (91 dias) — Recomendado minimo 180 dias
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Shopify

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  Detectado via HTML body
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  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 — 62/100

Estado: AVISO

localization: falta HttpOnly; localization: falta Secure; cart_currency: falta HttpOnly; cart_currency: falta Secure; _shopify_y: falta HttpOnly; _shopify_y: falta Secure; _shopify_s: falta HttpOnly; _shopify_s: falta Secure

- INFO **Cookies detectadas**
  7 cookie(s) encontrada(s)
- ALTO **Cookie: localization — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: localization — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: localization — SameSite**
  SameSite=lax
- ALTO **Cookie: cart_currency — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: cart_currency — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: cart_currency — SameSite**
  SameSite=lax
- ALTO **Cookie: _shopify_y — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: _shopify_y — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: _shopify_y — SameSite**
  SameSite=lax
- ALTO **Cookie: _shopify_s — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: _shopify_s — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: _shopify_s — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_essential — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_essential — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_essential — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_analytics — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_analytics — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_analytics — SameSite**
  SameSite=lax
- INFO **Cookie: _shopify_marketing — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _shopify_marketing — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _shopify_marketing — SameSite**
  SameSite=lax

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 (6658 bytes)
- INFO **Reglas robots.txt**
  148 Disallow, 0 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://garciacarrion.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] Cookies sin flag HttpOnly: Las cookies localization, cart_currency, _shopify_y y _shopify_s carecen de esta protección, permitiendo que scripts maliciosos accedan a ellas mediante ataques XSS.
[HIGH] Cookies sin flag Secure: Las cookies mencionadas no obligan a su transmisión exclusiva por canales cifrados, lo que facilita el robo de información en redes no seguras.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de un puerto alternativo puede revelar servicios de administración o proxies que no deberían estar accesibles públicamente.
[MEDIUM] Ausencia de cabecera Referrer-Policy: No se define una política para controlar qué información de navegación se comparte con sitios externos al hacer clic en enlaces.
[MEDIUM] Ausencia de cabecera Permissions-Policy: El sitio no restringe el uso de APIs sensibles del navegador como la cámara, el micrófono o la geolocalización.
[MEDIUM] Configuración HSTS insuficiente: El tiempo de vida de la directiva de transporte seguro es de 91 días, por debajo del estándar recomendado de 180 días.
[MEDIUM] Información sensible en robots.txt: El archivo bloquea la indexación total del sitio y revela la ubicación de la ruta admin, facilitando el reconocimiento a posibles atacantes.

[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare como tecnología de servidor, lo que ayuda a un atacante a perfilar la infraestructura técnica.