EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.fashionadictas.com/	Checks	9 pruebas
Dominio	www.fashionadictas.com	Hallazgos	64 totales
Fecha	24 de septiembre de 2026 a las 01:40	Problemas	12 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web fashionadictas.com arroja una puntuación de 88/100 con una calificación de nota B. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias de seguridad que requieren atención inmediata. El escaneo revela una base sólida en el cifrado de datos y redirecciones automáticas, aunque se detectaron deficiencias en la configuración de cookies y cabeceras de seguridad. En términos generales, el sitio se considera moderadamente seguro, pero presenta vulnerabilidades específicas que podrían ser explotadas para ataques de interceptación de datos. No se identificaron fallos críticos que comprometan la disponibilidad inmediata, pero la higiene de seguridad de las cookies es el punto más débil detectado.

Resumen de Riesgos

0	6	4	2	52
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 31 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	67	AVISO	_shopify_y: falta HttpOnly; _shopify_y: falta Se...
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 31 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  31 dias restantes (expira: 2026-10-25T04:17:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-27T04:17:34.000Z
- 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://www.fashionadictas.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

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 — 67/100

Estado: AVISO

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

- INFO **Cookies detectadas**
  6 cookie(s) encontrada(s)
- 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
- 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
- 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 (3646 bytes)

- INFO **Reglas robots.txt**
  50 Disallow, 35 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.fashionadictas.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] Cookie _shopify_y: Falta flag HttpOnly que permite acceso vía script (XSS) y flag Secure que permite envío por conexiones no seguras.
[HIGH] Cookie _shopify_s: Carece de flags HttpOnly y Secure, facilitando el secuestro de sesión y la interceptación de identificadores de usuario.
[HIGH] Cookie localization: Ausencia de HttpOnly y Secure, dejando este dato expuesto a scripts maliciosos en el navegador del cliente.
[MEDIUM] Referrer-Policy: La ausencia de esta cabecera impide controlar qué información de origen se comparte con sitios externos al navegar.
[MEDIUM] Permissions-Policy: Falta de configuración para restringir el acceso del navegador a funciones sensibles como cámara, micrófono o geolocalización.
[MEDIUM] HSTS max-age: El tiempo de persistencia de seguridad es de 91 días, lo cual es inferior al estándar recomendado de al menos 180 días.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto alternativo abierto que podría exponer servicios internos o interfaces de administración no deseadas.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante a perfilar el objetivo.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa al directorio admin, facilitando a los atacantes el descubrimiento de rutas de gestión privada.