EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://flexxshit.com/	Checks	9 pruebas
Dominio	flexxshit.com	Hallazgos	66 totales
Fecha	29 de abril de 2026 a las 16:41	Problemas	13 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado en el sitio web ha arrojado una puntuacion exacta de 88/100, lo que corresponde a una nota B. Durante la evaluacion se ejecutaron 9 checks pasivos, resultando en 6 verificaciones exitosas, 3 advertencias y 0 fallos criticos. El sistema demuestra una implementacion robusta de cifrado SSL y proteccion de contenido, aunque presenta debilidades tecnicas en la configuracion de cookies y cabeceras de respuesta. En conclusion, el sitio es mayoritariamente seguro, pero se considera vulnerable a ataques de secuestro de sesion y fugas de informacion debido a configuraciones de servidor mejorables.

Resumen de Riesgos

0	6	5	2	53
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 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	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 79 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  79 dias restantes (expira: 2026-07-17T20:00:02.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-18T20:00:03.000Z
- 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://flexxshit.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 — 67/100

Estado: AVISO

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

- INFO **Cookies detectadas**
  6 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: _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 (6790 bytes)

- INFO **Reglas robots.txt**
  152 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://flexxshit.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 flags HttpOnly y Secure: Las cookies localization, _shopify_y y _shopify_s no tienen activas estas protecciones, lo que permite que sean robadas mediante scripts maliciosos o interceptadas en conexiones no cifradas.
[MEDIUM] Falta de cabecera Referrer-Policy: El sitio no controla que informacion de referencia se envia al navegar hacia otros dominios, lo que puede comprometer la privacidad del usuario.
[MEDIUM] Falta de cabecera Permissions-Policy: No se restringen las capacidades del navegador, como el acceso a la camara o el microfono, aumentando el riesgo en caso de inyeccion de scripts.
[MEDIUM] HSTS max-age insuficiente: El tiempo de persistencia de la conexion segura es de 91 dias, cuando la recomendacion de seguridad estandar es de un minimo de 180 dias.
[MEDIUM] Puerto 8080 abierto: Se detecto un servicio HTTP alternativo activo, lo que expande la superficie de ataque y puede exponer servicios administrativos o de desarrollo.
[MEDIUM] Bloqueo total en robots.txt: El archivo bloquea el rastreo de todo el sitio, lo que puede ser un error de configuracion o una medida que afecta la visibilidad, ademas de exponer la ruta admin.
[LOW] Cabecera Server expuesta: Se revela el uso de la tecnologia Cloudflare, lo cual facilita a un atacante potencial la fase de reconocimiento de la infraestructura.