EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Shein.com	Checks	9 pruebas
Dominio	shein.com	Hallazgos	70 totales
Fecha	4 de julio de 2026 a las 11:35	Problemas	12 detectados

A

90/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja un resultado sobresaliente, obteniendo una puntuación exacta de 90/100 y una calificación de A. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias y 2 generaron advertencias importantes por falta de configuraciones defensivas. No se identificaron fallos críticos de seguridad en los elementos analizados, destacando un cifrado de transporte impecable. Por lo tanto, se concluye que el sitio es seguro para su uso general, aunque presenta debilidades técnicas en la protección de sesiones y cabeceras que deben ser subsanadas.

Resumen de Riesgos

0	3	8	1	58
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	70	AVISO	4/6 presentes. Faltan: X-Frame-Options, Permissi...
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	63	AVISO	AT: falta SameSite; armorUuid: falta HttpOnly; a...
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 53 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  53 dias restantes (expira: 2026-08-25T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-25T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 70/100

Estado: AVISO

4/6 presentes. Faltan: X-Frame-Options, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors *.shein.com https://www.shein.com.hk https://www.shein.com.vn ht...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=7776000000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- 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://shein.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=7776000000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=7776000000 (90000 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

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 — 63/100

Estado: AVISO

AT: falta SameSite; armorUuid: falta HttpOnly; armorUuid: falta Secure; armorUuid: falta SameSite; sessionID_shein: falta SameSite; sessionID_shein: falta SameSite; sessionID_shein: falta SameSite; sessionID_shein: falta SameSite; sessionID_shein: falta SameSite

- INFO **Cookies detectadas**
  8 cookie(s) encontrada(s)
- INFO **Cookie: AT — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: AT — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: AT — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: armorUuid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: armorUuid — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: armorUuid — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sessionID_shein — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sessionID_shein — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sessionID_shein — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sessionID_shein — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sessionID_shein — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sessionID_shein — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sessionID_shein — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sessionID_shein — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sessionID_shein — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sessionID_shein — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sessionID_shein — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sessionID_shein — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sessionID_shein — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sessionID_shein — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sessionID_shein — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: _cfuvid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: _cfuvid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: _cfuvid — SameSite**
  SameSite=none

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 (279 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 2 Allow
- INFO **Sitemap en robots.txt**
  https://www.shein.com/sitemap-index.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] X-Frame-Options: Esta cabecera de seguridad no está presente, lo que permite que el sitio sea cargado dentro de iframes en dominios externos, facilitando ataques de Clickjacking.
[HIGH] Cookie armorUuid sin flag HttpOnly: El atributo HttpOnly está ausente, permitiendo que scripts de terceros accedan a la cookie a través de document.cookie, aumentando el riesgo de robo de sesión mediante XSS.
[HIGH] Cookie armorUuid sin flag Secure: La falta de este atributo permite que la cookie sea enviada a través de conexiones HTTP no cifradas, lo que expone el identificador a ataques de interceptación de red.
[MEDIUM] Permissions-Policy: La ausencia de esta cabecera impide restringir el uso de APIs sensibles del navegador, como la cámara, el micrófono o la geolocalización, por parte de scripts o terceros.
[MEDIUM] Atributo SameSite faltante en cookies: Las cookies AT, armorUuid y sessionID_shein carecen de la directiva SameSite, lo que las hace vulnerables a ataques de falsificación de petición en sitios cruzados (CSRF).

[LOW] Cabecera Server expuesta: El servidor revela el uso de tecnología Cloudflare, lo cual proporciona información útil a un atacante sobre la infraestructura y capas de seguridad intermedias.