EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.stripchat.com	Checks	9 pruebas
Dominio	www.stripchat.com	Hallazgos	51 totales
Fecha	7 de septiembre de 2026 a las 14:17	Problemas	6 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma ha dado como resultado una puntuación de 83/100, lo que otorga una calificación final de grado B. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno presentó advertencias y uno fue calificado como fallo crítico. Se observa una implementación excelente en cuanto a cifrado de datos y gestión de identidad, aunque existen carencias importantes en las políticas de seguridad del lado del cliente. En conclusión, el sitio web se considera mayoritariamente seguro, pero presenta vulnerabilidades moderadas que podrían ser explotadas para ataques de inyección si no se corrigen a corto plazo.

Resumen de Riesgos

0	1	4	1	45
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 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	2 cookies, todas con flags correctos
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 89 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  89 dias restantes (expira: 2026-12-05T04:37:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-06T03:37:46.000Z
- 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-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: deny
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- 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.stripchat.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 406

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

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

2 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none
- 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 (699 bytes)
- INFO **Reglas robots.txt**
  7 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://stripchat.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: La ausencia de esta cabecera impide definir qué fuentes de contenido son confiables, facilitando ataques de Cross-Site Scripting (XSS) e inyección de datos.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó este puerto abierto, el cual suele utilizarse para servicios de administración o proxies, representando un vector de ataque si no está debidamente protegido.
[MEDIUM] X-Content-Type-Options: Al faltar esta directiva, el navegador puede intentar interpretar el contenido de forma distinta a la declarada, permitiendo la ejecución de código malicioso mediante MIME-sniffing.
[MEDIUM] Referrer-Policy: La falta de esta política puede provocar la filtración de información sensible sobre la procedencia de los usuarios hacia sitios de terceros.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador, lo que podría permitir que scripts de terceros accedan a funciones como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, proporcionando información técnica que ayuda a un atacante a perfilar la infraestructura tecnológica del sitio.