EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://seriesflixhd.win/series-online/	Checks	9 pruebas
Dominio	seriesflixhd.win	Hallazgos	44 totales
Fecha	21 de agosto de 2026 a las 22:53	Problemas	12 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha dado como resultado una puntuación de 51/100, obteniendo una calificación de nota D. Durante el análisis se ejecutaron 9 checks pasivos, de los cuales 4 resultaron satisfactorios, 2 generaron advertencias y 3 fallaron críticamente. La presencia de software de gestión de contenidos severamente desactualizado y la carencia total de cabeceras de protección elevan el riesgo operativo. Se ha determinado que el sitio es actualmente vulnerable ante diversos vectores de ataque conocidos. Por tanto, se requiere una intervención inmediata para mitigar las deficiencias estructurales detectadas.

Resumen de Riesgos

0	6	5	1	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	20	FALLO	WordPress 1.53 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-11-16T08:35:32.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-18T07:37:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, 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
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- 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 — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- 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 — 20/100

Estado: FALLO

WordPress 1.53 expuesta

- ALTO **WordPress version**
  Version 1.53 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (1836 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] WordPress version: Se detectó la versión 1.53 expuesta públicamente, la cual es extremadamente antigua y permite a atacantes explotar múltiples vulnerabilidades críticas y CVEs documentados.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado.
[HIGH] X-Frame-Options: El sitio no cuenta con protección contra Clickjacking, lo que permite que la interfaz sea embebida en marcos maliciosos para engañar a los usuarios.
[HIGH] Strict-Transport-Security: La falta de configuración HSTS impide que el navegador fuerce conexiones seguras, dejando la comunicación vulnerable a ataques de degradación de protocolo.

[HIGH] Redirección HTTP a HTTPS: El sistema permite el acceso mediante el puerto 80 sin redirigir al protocolo cifrado, exponiendo los datos en tránsito a posibles interceptaciones.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto de servidor web alternativo abierto, lo cual aumenta la superficie de ataque y puede exponer servicios administrativos desprotegidos.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos interpretados como scripts.
[MEDIUM] Referrer-Policy: No existe una política definida para el control de la información de referencia, lo que puede provocar la fuga de datos sensibles en las solicitudes salientes.
[MEDIUM] Permissions-Policy: La falta de restricciones en las APIs del navegador permite que funciones sensibles como la cámara o el micrófono no tengan un control de seguridad explícito.
[MEDIUM] Bloqueo total en robots.txt: El archivo de configuración bloquea todo el rastreo del sitio y carece de un sitemap.xml, dificultando las labores legítimas de indexación y auditoría.
[LOW] Server header expuesto: La cabecera revela el uso de infraestructura Cloudflare, proporcionando información técnica que facilita la fase de reconocimiento de un atacante.