EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.netflix.com/	Checks	9 pruebas
Dominio	www.netflix.com	Hallazgos	66 totales
Fecha	12 de mayo de 2026 a las 02:20	Problemas	18 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web ha resultado en una puntuación de 78/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron correctamente, 1 generó advertencias y 2 resultaron en fallos críticos. Se han identificado deficiencias en la implementación de cabeceras de seguridad y en el manejo de cookies de sesión, además de la presencia de contenido mixto. Aunque el cifrado de transporte es sólido, la falta de políticas de seguridad de contenido eleva el perfil de riesgo de la plataforma. En conclusión, el sitio se considera moderadamente vulnerable ante ataques de interceptación y scripts maliciosos.

Resumen de Riesgos

0	5	12	1	48
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 283 dias
Cabeceras de Seguridad	50	FALLO	Solo 3/6 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	60	AVISO	flwssn: falta HttpOnly; flwssn: falta Secure; fl...
Contenido Mixto	20	FALLO	5 recursos HTTP en pagina HTTPS
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 283 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  283 dias restantes (expira: 2027-02-18T21:41:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-18T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: envoy — 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
- 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.netflix.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 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**
  React, Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 60/100

Estado: AVISO

flwssn: falta HttpOnly; flwssn: falta Secure; flwssn: falta SameSite; nfvdid: falta HttpOnly; nfvdid: falta Secure; nfvdid: falta SameSite

- INFO **Cookies detectadas**
  5 cookie(s) encontrada(s)
- ALTO **Cookie: flwssn — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: flwssn — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: flwssn — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: nfvdid — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: nfvdid — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: nfvdid — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: SecureNetflixId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: SecureNetflixId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SecureNetflixId — SameSite**
  SameSite=strict
- INFO **Cookie: NetflixId — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: NetflixId — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: NetflixId — SameSite**
  SameSite=lax
- INFO **Cookie: gsid — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: gsid — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: gsid — SameSite**
  SameSite=none

Contenido Mixto — 20/100

Estado: FALLO

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://ir.netflix.com/
- MEDIO **Recurso HTTP (CSS url())**
  http://example.com
- MEDIO **Recurso HTTP (CSS url())**
  http://example.com
- MEDIO **Recurso HTTP (CSS url())**
  http://example.com
- MEDIO **CSS url()**
  ...y 1 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3790 bytes)
- INFO **Reglas robots.txt**
  133 Disallow, 4 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://www.netflix.com/sitemap/index
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de datos.
[HIGH] Cookie flwssn (HttpOnly/Secure): La falta de estas banderas permite que la cookie sea robada mediante scripts o interceptada en conexiones no cifradas.
[HIGH] Cookie nfvdid (HttpOnly/Secure): Al no estar protegida, esta cookie de sesión queda expuesta a ataques de secuestro de sesión y acceso no autorizado.
[MEDIUM] Referrer-Policy: La falta de esta cabecera puede filtrar información sensible de las URLs hacia dominios de terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs críticas del navegador como la cámara o el micrófono, aumentando el riesgo de privacidad.
[MEDIUM] Archivo /readme.html y /README.txt: Estos archivos son accesibles públicamente y pueden exponer detalles técnicos sobre la infraestructura del servidor.
[MEDIUM] Cookie flwssn y nfvdid (SameSite): La ausencia del atributo SameSite hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto: Se detectaron 5 recursos cargándose a través de HTTP, lo que debilita la integridad de la conexión HTTPS y permite ataques de hombre en el medio.
[MEDIUM] Bloqueo en Robots.txt: El archivo bloquea el acceso total al sitio, lo que podría ocultar problemas de indexación o configuraciones erróneas de visibilidad.
[LOW] Server header expuesto: La cabecera revela el uso de la tecnología "envoy", facilitando a un atacante la búsqueda de vulnerabilidades específicas para ese software.