EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://spotify.com	Checks	9 pruebas
Dominio	spotify.com	Hallazgos	60 totales
Fecha	20 de mayo de 2026 a las 21:38	Problemas	12 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio principal arroja una puntuación de 88/100 con una nota final de B. Se ejecutaron 9 checks pasivos, de los cuales 7 resultaron exitosos, uno generó una advertencia y uno fue calificado como fallo crítico. La infraestructura base de cifrado y transporte es sólida, pero existen deficiencias en la configuración de cabeceras y políticas de cookies. Se concluye que el sitio es seguro para la navegación general, aunque presenta vulnerabilidades específicas que requieren atención inmediata para prevenir ataques dirigidos.

Resumen de Riesgos

0	4	7	1	48
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 202 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
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	sp_t: falta HttpOnly; sp_t: falta HttpOnly; sp_t...
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 202 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  202 dias restantes (expira: 2026-12-08T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-08T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: script-src 'self' 'unsafe-eval' blob: open.spotifycdn.com open-review.spotifycdn...
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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.spotify.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

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

sp_t: falta HttpOnly; sp_t: falta HttpOnly; sp_t: falta SameSite; sp_new: falta HttpOnly; sp_new: falta SameSite; sp_landing: falta SameSite

- INFO **Cookies detectadas**
  5 cookie(s) encontrada(s)
- ALTO **Cookie: sp_t — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: sp_t — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sp_t — SameSite**
  SameSite=none
- INFO **Cookie: sp_landing — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sp_landing — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: sp_landing — SameSite**
  SameSite=none
- ALTO **Cookie: sp_t — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: sp_t — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sp_t — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: sp_new — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: sp_new — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sp_new — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: sp_landing — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: sp_landing — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: sp_landing — SameSite**
  Falta SameSite — Vulnerable a CSRF

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 (592 bytes)
- INFO **Reglas robots.txt**
  15 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://www.spotify.com/sitemap.xml
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Cookie sp_t sin HttpOnly: La falta de este atributo permite que la cookie sea accesible mediante scripts, aumentando el riesgo de robo de sesión vía XSS.
[HIGH] Cookie sp_new sin HttpOnly: Esta cookie de sesión carece de protección contra acceso por Javascript, exponiendo la identidad del usuario.
[MEDIUM] Cookie sp_t sin SameSite: La omisión de este atributo hace que la cookie sea enviada en peticiones de terceros, permitiendo ataques de CSRF.
[MEDIUM] Cookie sp_new sin SameSite: Riesgo de falsificación de solicitudes entre sitios debido a la falta de restricción en el envío de la cookie.
[MEDIUM] Cookie sp_landing sin SameSite: Vulnerabilidad ante ataques de tipo Cross-Site Request Forgery por configuración incompleta.
[MEDIUM] Archivo /readme.html expuesto: Este archivo es accesible públicamente y puede contener metadatos o información técnica sobre la plataforma.
[MEDIUM] Archivo /README.txt expuesto: La visibilidad de este documento técnico puede revelar detalles de la estructura interna del servidor.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar qué información de origen se envía a otros dominios durante la navegación.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara o el micrófono.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología envoy, lo que facilita a atacantes la búsqueda de exploits específicos para esa versión.