EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://jellyfin.iptv-box.top	Checks	9 pruebas
Dominio	jellyfin.iptv-box.top	Hallazgos	45 totales
Fecha	16 de mayo de 2026 a las 01:28	Problemas	12 detectados

D

59/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio web arroja una puntuación técnica de 59/100, lo que resulta en una calificación de grado D. Se han ejecutado un total de 9 comprobaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 2 se identificaron como fallos críticos. Aunque la capa de cifrado inicial es correcta, la plataforma carece de configuraciones de endurecimiento esenciales en el servidor web. En su estado actual, el sitio se considera vulnerable debido a la ausencia de protecciones contra ataques comunes de inyección y suplantación.

Resumen de Riesgos

0	5	5	2	33
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 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	100	OK	No se detecto version de CMS 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 88 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  88 dias restantes (expira: 2026-08-12T00:39:10.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-13T23:42:35.000Z
- 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 302 — 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**
  React

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

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 (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Redirección HTTP a HTTPS ausente: El servidor no redirige automáticamente las conexiones inseguras a la versión cifrada, permitiendo el acceso por el puerto 80.
[HIGH] Falta de Strict-Transport-Security (HSTS): No se instruye al navegador para que use exclusivamente HTTPS, facilitando ataques de degradación de seguridad.

[HIGH] Falta de Content-Security-Policy (CSP): La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] Falta de X-Frame-Options: El sitio no previene ser cargado dentro de marcos o iframes, lo que lo hace susceptible a ataques de clickjacking.
[MEDIUM] Falta de X-Content-Type-Options: El navegador podría interpretar archivos con tipos MIME incorrectos, lo que puede derivar en la ejecución de código no deseado.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de navegación que se comparte con sitios terceros al seguir enlaces salientes.
[MEDIUM] Falta de Permissions-Policy: No se restringen las capacidades del navegador, como el acceso a hardware o APIs de geolocalización, desde el contexto web.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo incrementa la superficie de ataque al revelar servicios adicionales o proxys.
[MEDIUM] Robots.txt restrictivo y falta de Sitemap: El archivo de configuración bloquea todo el rastreo y la falta de sitemap.xml dificulta la auditoría de recursos expuestos.
[LOW] Server header expuesto: La cabecera revela el uso de tecnología Cloudflare, lo cual asiste a un atacante en la fase de reconocimiento de la infraestructura.