EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tarifas.707studios-film.workers.dev/#inicio	Checks	9 pruebas
Dominio	tarifas.707studios-film.workers.dev	Hallazgos	41 totales
Fecha	9 de septiembre de 2026 a las 10:51	Problemas	11 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el sitio web arroja una puntuación de 57/100, lo que corresponde a una calificación de grado D. Se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, se emitió 1 advertencia y se identificaron 3 fallos críticos en la configuración. La ausencia total de cabeceras de seguridad y la falta de una política de redirección cifrada comprometen la integridad de la plataforma. Debido a estas deficiencias técnicas, se concluye que el sitio es actualmente vulnerable y requiere intervenciones inmediatas para alcanzar niveles de protección aceptables.

Resumen de Riesgos

0	5	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 89 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	20	FALLO	Faltan robots.txt y sitemap.xml
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: 2026-12-07T21:30:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-09-08T20:31:34.000Z
- 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

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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- 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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de inyección de código y Cross-Site Scripting (XSS), facilitando la ejecución de scripts maliciosos.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, donde un atacante puede inducir al usuario a realizar acciones no deseadas mediante marcos invisibles.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, dejando la comunicación expuesta a ataques de degradación de protocolo.
[HIGH] Redirección HTTP a HTTPS: El servidor responde por el puerto 80 sin redirigir al tráfico cifrado, lo que permite que la información viaje de forma vulnerable.
[MEDIUM] X-Content-Type-Options: La falta de esta protección permite el MIME-type sniffing, lo que puede llevar a que archivos de texto sean interpretados como código ejecutable por el navegador.
[MEDIUM] Referrer-Policy: No se controla la cantidad de información que el navegador envía al navegar desde este sitio hacia otros enlaces externos.
[MEDIUM] Permissions-Policy: No existe una restricción sobre el uso de APIs del navegador, como la cámara, el micrófono o la geolocalización, dentro del contexto del sitio.

[MEDIUM] Puerto 8080 (HTTP-Alt): Se ha detectado este puerto abierto, el cual suele utilizarse para servicios secundarios o de administración que podrían no tener las mismas protecciones que el puerto principal.
[LOW] Server header expuesto: La cabecera revela el uso de Cloudflare, lo que facilita a un atacante potencial el reconocimiento de la infraestructura tecnológica utilizada.
[LOW] sitemap.xml y robots.txt no encontrados: La falta de estos archivos dificulta la correcta indexación y el control sobre qué partes del sitio deben ser exploradas por motores de búsqueda.