EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://steaminventoryhelper.com/steam-desktop-authenticator	Checks	9 pruebas
Dominio	steaminventoryhelper.com	Hallazgos	41 totales
Fecha	22 de abril de 2026 a las 18:36	Problemas	9 detectados

C

62/100

puntos de seguridad

RESUMEN EJECUTIVO

El sitio web analizado presenta un nivel de seguridad intermedio, obteniendo una puntuación exacta de 62/100 con una nota de calificación C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron críticamente. El análisis revela deficiencias importantes en la configuración de cabeceras de seguridad y en la redirección forzosa de tráfico cifrado. Debido a la ausencia de políticas de protección contra inyecciones y la exposición de puertos alternativos, se concluye que el sitio es actualmente vulnerable a ataques de nivel intermedio. La infraestructura requiere una intervención inmediata para mitigar riesgos asociados a la interceptación de datos y ataques de scripts.

Resumen de Riesgos

0	4	3	2	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 51 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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 51 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  51 dias restantes (expira: 2026-06-12T23:32:47.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-14T23:32:48.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, 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
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: same-origin
- 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 403 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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 403)
- 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: Esta cabecera no se encuentra configurada, lo que facilita ataques de Cross-Site Scripting (XSS) y de inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo posibles degradaciones de protocolo por parte de atacantes.
[HIGH] Redirección HTTP a HTTPS: El sitio no redirige automáticamente el tráfico inseguro y devuelve un error 403, lo que compromete la integridad de la conexión inicial del usuario.
[MEDIUM] X-Content-Type-Options: Al no estar presente, el navegador podría interpretar archivos con un tipo MIME incorrecto, aumentando el riesgo de ataques de sniffing.
[MEDIUM] Permissions-Policy: La ausencia de esta cabecera significa que no se están restringiendo las APIs del navegador, como el acceso a la cámara o micrófono, desde el contexto web.
[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un puerto de servicio alternativo abierto que podría ser utilizado como vector de ataque o acceso a servicios no protegidos.
[LOW] Server header expuesto: La cabecera del servidor revela el uso de Cloudflare, proporcionando información técnica sobre la infraestructura que puede ser usada para reconocimiento.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado (error 403), lo que dificulta la auditoría de la estructura pública del dominio.