# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://sshive.io | Checks | 9 pruebas |
| Dominio | sshive.io | Hallazgos | 43 totales |
| Fecha | 28 de abril de 2026 a las 22:56 | Problemas | 12 detectados |

**D**

57/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 57/100, lo que resulta en una calificación de grado D. Se ejecutaron 9 comprobaciones pasivas, de las cuales 5 resultaron exitosas, 1 generó una advertencia y 3 fallaron debido a configuraciones de seguridad críticas ausentes. A pesar de contar con un cifrado de conexión válido, la infraestructura carece de las protecciones básicas necesarias para mitigar ataques modernos de interceptación y manipulación de datos. Por lo tanto, se concluye que el sitio es actualmente vulnerable y requiere acciones correctivas inmediatas para alcanzar un nivel de seguridad aceptable.

## Resumen de Riesgos

| 0 | 5 | 4 | 3 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 48 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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-15T17:56:28.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-17T17:56:29.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Nuxt — Revela framework/lenguaje
- 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 404 — 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**
  Nuxt, Nuxt

## 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] Fallo en Redirección HTTPS: La conexión no redirige automáticamente el tráfico HTTP hacia HTTPS, permitiendo comunicaciones no cifradas.
[HIGH] Ausencia de Strict-Transport-Security (HSTS): El sitio no instruye a los navegadores para usar exclusivamente conexiones seguras, facilitando ataques de degradación de protocolo.
[HIGH] Ausencia de Content-Security-Policy (CSP): No existe una política definida para controlar las fuentes de contenido, lo que expone el sitio a ataques de Cross-Site Scripting (XSS).
[HIGH] Ausencia de X-Frame-Options: La falta de esta cabecera permite que el sitio sea embebido en iframes externos, facilitando ataques de Clickjacking.

[MEDIUM] Puerto 8080 (HTTP-Alt) Abierto: La exposición de servicios en puertos alternativos aumenta la superficie de ataque y puede revelar proxies o servicios internos vulnerables.
[MEDIUM] Ausencia de X-Content-Type-Options: El sitio es susceptible a ataques de MIME-type sniffing, permitiendo que archivos maliciosos sean ejecutados como scripts.
[MEDIUM] Ausencia de Referrer-Policy: No se limita la información de referencia enviada a otros sitios, lo que puede comprometer la privacidad del usuario.
[MEDIUM] Ausencia de Permissions-Policy: El navegador no tiene restricciones sobre el uso de hardware o APIs sensibles por parte de scripts del sitio.
[LOW] Cabecera Server Expuesta: El valor "cloudflare" revela información sobre la infraestructura de red utilizada por el servidor.
[LOW] Cabecera X-Powered-By Expuesta: Se detectó el uso del framework Nuxt, lo que proporciona pistas sobre la tecnología base para posibles ataques dirigidos.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la correcta gestión de la indexación y visibilidad en motores de búsqueda.