

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://wrap-automated-citizens-studied.trycloudflare.com/	Checks	9 pruebas
Dominio	wrap-automated-citizens-studied.trycloudflare.com	Hallazgos	47 totales
Fecha	9 de mayo de 2026 a las 21:55	Problemas	8 detectados

C

71/100

puntos de seguridad



RESUMEN EJECUTIVO

Tras realizar el analisis de seguridad, el sitio web ha obtenido una puntuacion de 71/100 con una nota final de C. Se ejecutaron 9 checks pasivos que resultaron en 5 validaciones correctas, 3 advertencias y 1 fallo critico relacionado con la gestion del trafico cifrado. Aunque la infraestructura base cuenta con protecciones iniciales, la ausencia de politicas de seguridad avanzadas y la exposicion de rutas administrativas comprometen la integridad del sistema. Se concluye que el sitio es parcialmente vulnerable y requiere intervenciones tecnicas inmediatas para mitigar riesgos de interceptacion de datos e inyecciones de codigo.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 62 dias
Cabeceras de Seguridad	60	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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 62 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
62 dias restantes (expira: 2026-07-10T20:31:34.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-11T19:31:56.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Permissions-Policy

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

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **INFO** **Strict-Transport-Security**
Presente: max-age=15552000; includeSubDomains
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **INFO** **Referrer-Policy**
Presente: no-referrer
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 0/100

Estado: **FALLO**

No hay redirección HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redirección**
HTTP 200 — No redirige a HTTPS
- **INFO** **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=15552000; includeSubDomains
- **BAJO** **HSTS includeSubDomains**
HSTS cubre subdominios
- **INFO** **HSTS max-age**
max-age=15552000 (180 días)
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 200

Detección CMS — 100/100

Estado: **OK**

No se detectó 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 detectó versión de CMS expuesta

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)
- **MEDIO** **Ruta /administrator/**
Panel de login accesible públicamente

- MEDIO** Ruta /user/login
Panel de login accesible publicamente
- 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 (39 bytes)
- INFO** Reglas robots.txt
1 Disallow, 1 Allow
- 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] Redireccion HTTP a HTTPS ausente: El servidor permite conexiones a traves de HTTP sin cifrar, lo que expone a los usuarios a ataques de interceptacion de datos (Man-in-the-Middle).

[HIGH] Content-Security-Policy (CSP) faltante: La falta de esta cabecera permite la ejecucion de scripts no autorizados, elevando el riesgo de ataques Cross-Site Scripting (XSS).

[MEDIUM] Rutas administrativas expuestas: El acceso publico a /administrator/ y /user/login facilita intentos de intrusion mediante ataques de fuerza bruta.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La activacion de este puerto alternativo puede exponer servicios internos o interfaces de gestion que no deberian ser publicas.

[MEDIUM] Permissions-Policy faltante: El sitio no restringe el acceso a APIs sensibles del navegador como camara o microfono, afectando la privacidad de los visitantes.

[LOW] Cabecera Server expuesta: El servidor revela que utiliza tecnologia Cloudflare, lo cual proporciona informacion tecnica valiosa para un atacante en fase de reconocimiento.

[LOW] Sitemap.xml ausente: La falta de un mapa del sitio dificulta la auditoria de contenidos y puede omitir la revision de paginas indexadas por error.