

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://anonymous-cloud.com/	Checks	9 pruebas
Dominio	anonymous-cloud.com	Hallazgos	44 totales
Fecha	21 de septiembre de 2026 a las 08:43	Problemas	12 detectados

C

68/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 68/100, lo que resulta en una calificación de grado C. Durante la auditoría se ejecutaron 9 checks pasivos, de los cuales 5 fueron satisfactorios, 2 generaron advertencias y 2 resultaron en fallos críticos. Aunque la plataforma cuenta con una base sólida en el cifrado de datos, la ausencia total de cabeceras de seguridad modernas compromete la integridad del servicio. En su estado actual, el sitio se considera vulnerable a ataques dirigidos contra el navegador de los usuarios y a técnicas de suplantación.

Resumen de Riesgos

0 CRITICO	4 ALTO	4 MEDIO	4 BAJO	32 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	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 88 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
88 dias restantes (expira: 2026-12-18T09:21:28.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-19T08:21:30.000Z
- 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: Express — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://anonymous-cloud.com/
- 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
Express

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

robots.txt
No encontrado (HTTP 404)
- 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes lo carguen en marcos invisibles para engañar al usuario.

[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar siempre conexiones seguras, lo que permite ataques de degradación de protocolo (Man-in-the-Middle).

[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que facilita la ejecución de scripts maliciosos camuflados.

[MEDIUM] Falta de Referrer-Policy: No existe control sobre la información de navegación que se envía a sitios externos a través de los enlaces.

[MEDIUM] Falta de Permissions-Policy: El servidor no restringe el acceso a funciones sensibles del navegador como la cámara, el micrófono o la ubicación.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque y sugiere la presencia de servicios de administración o proxies desprotegidos.

[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, lo que facilita a los atacantes el reconocimiento de la infraestructura de red.

[LOW] Cabecera X-Powered-By expuesta: Indica que el sitio utiliza el framework Express, permitiendo la búsqueda de vulnerabilidades específicas para esa tecnología.

[LOW] Archivos de indexación faltantes: La ausencia de robots.txt y sitemap.xml indica una configuración de servidor incompleta y dificulta la gestión de rastreo.