EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tarifagiveaway.com/	Checks	9 pruebas
Dominio	tarifagiveaway.com	Hallazgos	49 totales
Fecha	14 de julio de 2026 a las 16:02	Problemas	13 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 65/100, lo que equivale a una calificación de C. Durante la evaluación, se ejecutaron 9 checks pasivos que resultaron en 5 aciertos, 2 advertencias y 2 fallos críticos en la configuración. Aunque el cifrado SSL es adecuado, se identificaron carencias significativas en la implementación de cabeceras de seguridad y en la protección de las cookies del sistema. Debido a la ausencia de políticas de defensa modernas y la exposición de puertos no estándar, el sitio se considera vulnerable a ataques de intermediario y secuestro de sesiones. Es imperativo abordar estas debilidades para mejorar la postura defensiva de la plataforma y proteger la integridad de los usuarios.

Resumen de Riesgos

0	6	5	2	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 75 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	33	FALLO	NEXT_LOCALE: falta HttpOnly; NEXT_LOCALE: falta ...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 75 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  75 dias restantes (expira: 2026-09-27T15:55:56.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-29T14:58:27.000Z
- 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: Next.js — 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://tarifagiveaway.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**
  React, Next.js, Next.js

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 — 33/100

Estado: FALLO

NEXT_LOCALE: falta HttpOnly; NEXT_LOCALE: falta Secure

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- ALTO **Cookie: NEXT_LOCALE — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: NEXT_LOCALE — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- INFO **Cookie: NEXT_LOCALE — SameSite**
  SameSite=lax

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2132 bytes)
- INFO **Reglas robots.txt**
  19 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**
  https://acme.com/sitemap.xml
- 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 facilita ataques de XSS e inyección de contenido malicioso al no restringir el origen de los recursos.
[HIGH] Falta de X-Frame-Options: Permite ataques de clickjacking, lo que podría engañar a los usuarios para realizar acciones no deseadas en el sitio.
[HIGH] Falta de Strict-Transport-Security: No se fuerza el uso de HTTPS en el navegador, permitiendo posibles ataques de degradación de protocolo.
[HIGH] Cookie NEXT_LOCALE sin HttpOnly: La cookie es accesible mediante scripts de cliente, aumentando drásticamente el riesgo de robo de identidad en ataques XSS.
[HIGH] Cookie NEXT_LOCALE sin Secure: La información se transmite por canales no cifrados, permitiendo que un atacante intercepte la cookie en redes inseguras.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: El servicio expone un vector de ataque adicional que suele estar menos monitorizado que los puertos estándar.
[MEDIUM] Falta de X-Content-Type-Options: Permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de scripts maliciosos disfrazados.
[MEDIUM] Falta de Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría filtrar rutas internas privadas.
[MEDIUM] Falta de Permissions-Policy: El sitio no limita el acceso del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / impide la indexación y sugiere que el sitio podría estar exponiendo estructuras internas por error.
[LOW] Server header expuesto: Se revela el uso de Cloudflare, lo cual asiste a los atacantes en la fase de reconocimiento de la infraestructura.
[LOW] X-Powered-By expuesto: Se confirma el uso de Next.js como framework, permitiendo búsquedas de vulnerabilidades específicas para esta tecnología.