EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.flarethla.com	Checks	9 pruebas
Dominio	www.flarethla.com	Hallazgos	41 totales
Fecha	15 de septiembre de 2026 a las 14:31	Problemas	11 detectados

D

57/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha arrojado una puntuación de 57/100, lo que corresponde a una nota D. Se ejecutaron un total de 9 checks pasivos, resultando en 5 verificaciones correctas, 1 advertencia y 3 fallos críticos en la configuración de seguridad. La plataforma carece de las protecciones fundamentales contra ataques de inyección y no garantiza la navegación cifrada de forma obligatoria. Debido a estas carencias en las políticas de respuesta del servidor y la exposición de puertos innecesarios, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	5	4	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 44 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 44 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  44 dias restantes (expira: 2026-10-29T08:43:46.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-31T07:49:03.000Z
- 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

- 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 200 — 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

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] Content-Security-Policy (CSP) ausente: La falta de esta cabecera permite la ejecución de ataques XSS y la inyección de contenido malicioso por parte de terceros.
[HIGH] X-Frame-Options ausente: El sitio no protege contra ataques de clickjacking, permitiendo que la interfaz sea embebida en marcos externos fraudulentos.
[HIGH] Strict-Transport-Security (HSTS) ausente: El servidor no instruye al navegador para usar exclusivamente conexiones HTTPS, facilitando ataques de degradación de SSL.
[HIGH] Redirección HTTP a HTTPS fallida: La comunicación a través del puerto 80 no se redirige automáticamente al protocolo seguro, exponiendo los datos de los usuarios a intercepciones.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un puerto de servidor web alternativo incrementa la superficie de ataque y puede exponer servicios administrativos no protegidos.
[MEDIUM] X-Content-Type-Options ausente: Al no estar configurada, el navegador podría interpretar archivos con tipos MIME incorrectos, derivando en la ejecución de código no deseado.
[MEDIUM] Referrer-Policy ausente: No existe control sobre la información de navegación que se envía a otros dominios, lo que compromete la privacidad del tráfico de salida.

[MEDIUM] Permissions-Policy ausente: El servidor no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El servidor revela el uso de la tecnología Cloudflare, lo que facilita a un atacante potencial el reconocimiento de la infraestructura.
[LOW] sitemap.xml ausente: No se encontró el archivo de mapeo del sitio, lo que dificulta la auditoría de la estructura pública del dominio.