EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://flashsender.org/?gad_source=1&gad_campaignid=23807872473&gclid=CjwKCAjw9NjRBhATEiwA_p2J8TxmzU2DpWNXcpp9GZXk_F-DcppbITkFDyPfZUZ4KNIHLZENjUVRvMhoCexIQAvD_BwE	Checks	9 pruebas
Dominio	flashsender.org	Hallazgos	49 totales
Fecha	20 de junio de 2026 a las 17:40	Problemas	14 detectados

B

78/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del sitio flashsender.org arrojó una puntuación exacta de 78/100, lo que equivale a una nota de B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 2 advertencias y 1 fallo crítico en la configuración de cabeceras. Aunque el sitio demuestra una implementación sólida de cifrado SSL y redirección HTTPS, la carencia de políticas de seguridad proactivas en el servidor es evidente. En conclusión, el sitio web es vulnerable ante ataques de inyección y manipulación de contenido debido a configuraciones de seguridad incompletas.

Resumen de Riesgos

0	2	10	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-08-19T05:50:17.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-21T05:50:18.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, 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
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://flashsender.org/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- 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 (11409 bytes)
- INFO **Reglas robots.txt**
  9 Disallow, 1 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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: La ausencia de esta cabecera permite ataques de inyección de scripts (XSS) y contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking que pueden engañar a los usuarios.
[MEDIUM] X-Content-Type-Options: La falta de esta política permite que los navegadores realicen MIME-type sniffing, facilitando la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que podría filtrar datos de navegación.
[MEDIUM] Permissions-Policy: El sitio no restringe el acceso a APIs del navegador como cámara o micrófono, aumentando el riesgo de privacidad.
[MEDIUM] Archivos Informativos Expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente y pueden revelar detalles técnicos internos.
[MEDIUM] Paneles de Login Expuestos: Rutas críticas como /wp-login.php, /administrator/ y /user/login están abiertas, facilitando intentos de fuerza bruta.
[MEDIUM] Puerto 8080 Abierto: La exposición del puerto HTTP alternativo aumenta innecesariamente la superficie de ataque del servidor.
[MEDIUM] Exposición en Robots.txt: El archivo bloquea todo el contenido y revela una ruta denominada "config", lo que orienta a posibles atacantes hacia directorios sensibles.
[LOW] Cabecera Server Expuesta: Se revela el uso de Cloudflare, proporcionando información valiosa para la fase de reconocimiento de un ataque.