

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://flashusdt.io/
Dominio flashusdt.io
Fecha 20 de junio de 2026 a las 17:35

Checks 9 pruebas
Hallazgos 44 totales
Problemas 12 detectados

C

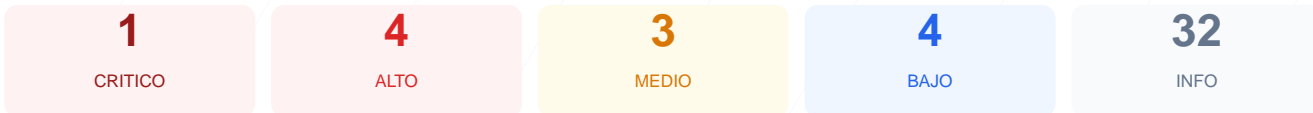
73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web flashusdt.io ha resultado en una puntuación de 73/100 con una calificación de grado C. Durante el proceso se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron clasificados como fallos. Aunque el cifrado de datos es robusto, la exposición de servicios críticos en puertos abiertos y la ausencia de cabeceras de seguridad fundamentales comprometen la integridad del servidor. Se concluye que el sitio es actualmente vulnerable a ataques de interceptación y acceso no autorizado a bases de datos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 49 dias
Cabeceras de Seguridad	25	FALLO	Solo 1/6 presentes. Faltan: X-Frame-Options, Str...
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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 49 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
49 dias restantes (expira: 2026-08-08T15:24:28.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-10T15:24:29.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 1/6 presentes. Faltan: X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**
Presente: upgrade-insecure-requests
- **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://flashusdt.io/>
- **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**
Next.js, PHP/8.2.30

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

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 3306 (MySQL)

- **ALTO** **Puerto 21 (FTP)**
ABIERTO — 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
- **CRITICO** **Puerto 3306 (MySQL)**
ABIERTO — 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
- **INFO** **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- **INFO** **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL): El servicio de base de datos está expuesto públicamente, lo que permite intentos de conexión externa y ataques de fuerza bruta.

[HIGH] Puerto 21 (FTP): Este puerto permite la transferencia de archivos sin cifrar, facilitando la interceptación de credenciales por parte de terceros.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, permitiendo ataques de degradación de protocolo (SSL Stripping).

[HIGH] X-Frame-Options: La ausencia de esta cabecera hace al sitio susceptible a ataques de Clickjacking, donde un atacante puede camuflar la interfaz.

[MEDIUM] X-Content-Type-Options: Al no estar configurada, el navegador podría intentar interpretar archivos de forma incorrecta, facilitando ataques de ejecución de código.

[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros dominios, lo que puede filtrar datos de navegación privados.

[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs sensibles del navegador como la cámara o el micrófono desde el contexto web.

[LOW] Exposición de tecnología: Las cabeceras Server y X-Powered-By revelan el uso de LiteSpeed y PHP/8.2.30, facilitando la búsqueda de exploits específicos.

[LOW] Ausencia de archivos de gestión: No se detectaron robots.txt ni sitemap.xml, lo cual afecta la indexación y el control de rastreo de los motores de búsqueda.