# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://tasalogistic.com | Checks | 9 pruebas |
| Dominio | tasalogistic.com | Hallazgos | 48 totales |
| Fecha | 22 de mayo de 2026 a las 06:41 | Problemas | 11 detectados |

C

65/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio tasalogistic.com arroja una puntuación de 65/100 con una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 3 advertencias y 2 fallos críticos en la configuración del servidor. La ausencia total de cabeceras de seguridad esenciales y la proximidad del vencimiento del certificado SSL representan los mayores riesgos detectados. Debido a estas deficiencias técnicas que facilitan ataques de interceptación y suplantación, se concluye que el sitio es actualmente vulnerable.

## Resumen de Riesgos

| 0 | 4 | 4 | 3 | 37 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 70 | AVISO | Certificado expira en 14 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 | 83 | AVISO | ARRAffinity: falta SameSite |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| Robots.txt y Sitemap | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 14 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  14 dias restantes (expira: 2026-06-04T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-10T00:00:00.000Z
- 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: nginx — 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://tasalogistic.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

## 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 — 83/100

Estado: AVISO

ARRAffinity: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: ARRAffinity — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ARRAffinity — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ARRAffinity — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: ARRAffinitySameSite — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ARRAffinitySameSite — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ARRAffinitySameSite — SameSite**
  SameSite=none

## 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 — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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**

[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido XSS.
[HIGH] X-Frame-Options: Falta de protección contra ataques de clickjacking, permitiendo que el sitio sea cargado dentro de marcos externos no autorizados.
[HIGH] Strict-Transport-Security: No existe una política HSTS configurada, lo que impide forzar conexiones cifradas y facilita ataques de degradación de protocolo.
[MEDIUM] X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría llevar a la ejecución de archivos con contenido inesperado.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar qué información de navegación se comparte con otros dominios.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador como la cámara o el micrófono, aumentando la superficie de exposición del cliente.
[MEDIUM] Cookie ARRAffinity: El atributo SameSite no está configurado, dejando la sesión vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[LOW] SSL/TLS: El certificado de seguridad actual expirará en 14 días, lo que causará advertencias de seguridad a los usuarios si no se renueva.
[LOW] Server header expuesto: La cabecera revela el uso de tecnología nginx, proporcionando información útil a posibles atacantes para buscar exploits específicos.
[LOW] robots.txt y sitemap.xml: La ausencia de estos archivos dificulta la correcta indexación y auditoría de la estructura del sitio web.