EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sistemafc.tallerssh.cu	Checks	9 pruebas
Dominio	sistemafc.tallerssh.cu	Hallazgos	45 totales
Fecha	3 de mayo de 2026 a las 17:09	Problemas	6 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web sistemafc.tallerssh.cu ha resultado en una puntuación de 83/100, lo que equivale a una calificación de grado B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 6 finalizaron con éxito, 2 presentaron advertencias y 1 se identificó como fallo. El sitio demuestra una implementación sólida de cifrado SSL y manejo de cookies, pero carece de políticas de seguridad modernas a nivel de cabeceras HTTP. Aunque la base técnica es estable, la ausencia de protecciones contra inyección de contenido y la exposición de la tecnología del servidor sitúan al sitio en un estado moderadamente vulnerable que requiere atención inmediata.

Resumen de Riesgos

0	3	0	3	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 80 dias
Cabeceras de Seguridad	55	AVISO	4/6 presentes. Faltan: Content-Security-Policy, ...
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	1 cookies, todas con flags correctos
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	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 80 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  80 dias restantes (expira: 2026-07-22T09:43:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-23T09:43:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: AVISO

4/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=()

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://sistemafc.tallerssh.cu/
- 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

1 cookies, todas con flags correctos

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: SISTEMA_COSTOS_SID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: SISTEMA_COSTOS_SID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SISTEMA_COSTOS_SID — SameSite**
  SameSite=strict

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

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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: Falta esta cabecera, la cual es vital para prevenir ataques de Cross-Site Scripting (XSS) e inyecciones de datos maliciosos.

[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones seguras permanentemente, permitiendo posibles ataques de degradación de protocolo.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: Apache, revelando la tecnología utilizada y facilitando el reconocimiento para ataques dirigidos.
[LOW] robots.txt: El archivo no fue encontrado (HTTP 404), lo que impide definir reglas de acceso para rastreadores automáticos.
[LOW] sitemap.xml: No se detectó un mapa del sitio, afectando la visibilidad de la estructura de directorios y la organización lógica del dominio.