EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://impresiones.tallerssh.cu	Checks	9 pruebas
Dominio	impresiones.tallerssh.cu	Hallazgos	59 totales
Fecha	3 de mayo de 2026 a las 13:04	Problemas	21 detectados

C

66/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio impresiones.tallerssh.cu arroja una puntuación de 66/100, lo que corresponde a una calificación de nota C. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 2 advertencias por configuraciones incompletas y 2 fallos críticos en la seguridad de cabeceras y cookies. Aunque el cifrado de datos es correcto, la ausencia de políticas de protección contra ataques de inyección y el manejo inseguro de sesiones incrementan el riesgo operativo. En su estado actual, el sitio se considera vulnerable ante ataques comunes de la capa de aplicación. Es fundamental implementar las protecciones faltantes para alcanzar un nivel de seguridad aceptable.

Resumen de Riesgos

0	10	9	2	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 71 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	17	FALLO	frontend_lang: falta HttpOnly; frontend_lang: fa...
Contenido Mixto	60	AVISO	3 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 71 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  71 dias restantes (expira: 2026-07-13T02:52:20.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-14T02:52:21.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- BAJO **Server header expuesto**
  Server: Werkzeug/2.0.2 Python/3.10.12 — 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)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- 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://impresiones.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
- BAJO **Meta generator**
  Expone: Odoo
- INFO **Tecnologias detectadas**
  Next.js

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 — 17/100

Estado: FALLO

frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; session_id: falta Secure; session_id: falta SameSite; frontend_lang: falta HttpOnly; frontend_lang: falta Secure; frontend_lang: falta SameSite; session_id: falta Secure; session_id: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: frontend_lang — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: frontend_lang — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: frontend_lang — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: session_id — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: session_id — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: session_id — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

3 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://impresiones.tallerssh.cu/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.odoo.com?utm_source=db&utm_medium=website
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.odoo.com/app/website?utm_source=db&utm_medium...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (118 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  http://impresiones.tallerssh.cu/sitemap.xml
- 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, lo que permite la ejecución de scripts maliciosos y facilita ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: La ausencia de esta directiva expone al sitio a ataques de clickjacking, permitiendo que la web sea cargada en marcos externos.
[HIGH] Strict-Transport-Security: No se ha configurado HSTS, por lo que el navegador no obliga a realizar conexiones siempre seguras vía HTTPS.
[HIGH] Cookie frontend_lang sin flag HttpOnly: Esta cookie de aplicación es accesible mediante scripts de cliente, permitiendo el robo de información en ataques XSS.
[HIGH] Cookie frontend_lang sin flag Secure: La información se transmite sin cifrar si el usuario accede por error mediante el protocolo HTTP.
[HIGH] Cookie session_id sin flag Secure: El identificador de sesión es vulnerable a interceptación en redes locales o conexiones no seguras.
[MEDIUM] Cookies sin flag SameSite: Tanto session_id como frontend_lang carecen de esta protección, facilitando ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy: No existe una política que controle cuánta información de la URL de origen se comparte con sitios de terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso de las APIs del navegador a componentes sensibles como la cámara o el micrófono.
[MEDIUM] Contenido Mixto detectado: El sitio carga recursos mediante enlaces HTTP directos, lo que degrada la integridad de la conexión cifrada HTTPS.
[LOW] Cabecera Server expuesta: Se revela el uso de Werkzeug/2.0.2 y Python/3.10.12, proporcionando datos valiosos para que un atacante busque exploits específicos.
[LOW] Meta generator expuesto: El código fuente confirma el uso de la plataforma Odoo, permitiendo identificar vectores de ataque conocidos para dicho sistema.