EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://tallerssh.nat.cu	Checks	9 pruebas
Dominio	tallerssh.nat.cu	Hallazgos	51 totales
Fecha	3 de mayo de 2026 a las 12:54	Problemas	16 detectados

C

63/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio tallerssh.nat.cu ha resultado en una puntuación de 63/100, lo que equivale a una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 finalizaron en fallo crítico. A pesar de contar con un cifrado SSL robusto, el servidor presenta carencias graves en la implementación de cabeceras de seguridad y en la protección de cookies de sesión. Debido a la ausencia de mecanismos de defensa modernos contra ataques de inyección y suplantación, el sitio se considera vulnerable.

Resumen de Riesgos

0	7	7	2	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 84 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	17	FALLO	frontend_lang: falta HttpOnly; frontend_lang: fa...
Contenido Mixto	60	AVISO	2 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 84 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  84 dias restantes (expira: 2026-07-26T10:45:29.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-27T10:45:30.000Z
- 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: 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)
- 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://tallerssh.nat.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

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

- INFO **Cookies detectadas**
  2 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

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- 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/ecommerce?utm_source=db&utm_medi...

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (111 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://tallerssh.nat.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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking al permitir que su contenido sea embebido en marcos de otras webs.
[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a usar conexiones HTTPS mediante HSTS, facilitando ataques de degradación de SSL.
[HIGH] Cookie frontend_lang sin flag HttpOnly: Esta vulnerabilidad permite que scripts del lado del cliente accedan a la cookie, facilitando el robo de información en ataques XSS.
[HIGH] Cookies sin flag Secure: Las cookies session_id y frontend_lang se envían sin el flag de seguridad, lo que permite su interceptación en conexiones no cifradas.
[MEDIUM] Cookies sin flag SameSite: La falta de este atributo en las cookies de sesión hace que el sitio sea susceptible a ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] Contenido Mixto detectado: Existen dos recursos cargados mediante HTTP (odoo.com) en una página cifrada con HTTPS, lo que compromete la integridad de la conexión.
[MEDIUM] Falta de X-Content-Type-Options: La ausencia de esta cabecera permite el sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos maliciosos.
[MEDIUM] Falta de Referrer-Policy y Permissions-Policy: No se controla la información de navegación enviada a otros sitios ni se restringen APIs sensibles del navegador como la cámara o el micrófono.
[LOW] Cabecera Server expuesta: Se revela el uso de Werkzeug 2.0.2 y Python 3.10.12, información técnica que ayuda a un atacante a buscar vulnerabilidades específicas.
[LOW] Meta generator expuesto: El código fuente revela directamente que el sitio utiliza el CMS Odoo, facilitando el reconocimiento del sistema.