EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://wiotmanager.com	Checks	9 pruebas
Dominio	wiotmanager.com	Hallazgos	45 totales
Fecha	26 de mayo de 2026 a las 16:18	Problemas	14 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio wiotmanager.com arroja una puntuación de 72/100, lo que resulta en una calificación de grado C. El análisis se basó en 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 fallaron críticamente por falta de configuraciones de seguridad esenciales. Aunque el cifrado de datos es correcto, la ausencia total de cabeceras de seguridad y la exposición de rutas administrativas debilitan la estructura del sitio. En conclusión, el sitio web se considera vulnerable a ataques de suplantación de identidad y secuestro de clics debido a una configuración de servidor incompleta.

Resumen de Riesgos

0	4	8	2	31
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 86 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	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	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 86 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  86 dias restantes (expira: 2026-08-20T07:15:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-22T07:15:35.000Z
- 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/1.18.0 (Ubuntu) — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Express — Revela framework/lenguaje
- 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://wiotmanager.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
- INFO **Tecnologias detectadas**
  Express

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 ataques de inyección de contenido y Cross-Site Scripting (XSS).

[HIGH] X-Frame-Options: Falta de protección que permite ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, permitiendo ataques de degradación de conexión.
[MEDIUM] X-Content-Type-Options: El sitio es vulnerable al sniffing de tipos MIME por parte del navegador.
[MEDIUM] Referrer-Policy: No hay control sobre la información de referencia enviada a sitios de terceros.
[MEDIUM] Permissions-Policy: No se restringe el acceso de la aplicación a APIs del navegador como cámara o ubicación.
[MEDIUM] Archivos informativos expuestos: Los archivos /readme.html y /README.txt son accesibles y pueden revelar detalles técnicos del sistema.
[MEDIUM] Paneles de login expuestos: Rutas como /wp-login.php, /administrator/ y /user/login son accesibles públicamente para intentos de intrusión.
[LOW] Exposición de tecnología del servidor: La cabecera Server revela el uso de nginx/1.18.0 (Ubuntu).
[LOW] Exposición de framework: La cabecera X-Powered-By revela el uso de Express, facilitando el reconocimiento a posibles atacantes.
[LOW] Ausencia de archivos de indexación: No se detectaron los archivos robots.txt ni sitemap.xml.