EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tiendanube.com/	Checks	9 pruebas
Dominio	www.tiendanube.com	Hallazgos	49 totales
Fecha	7 de mayo de 2026 a las 13:57	Problemas	14 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el activo arroja una puntuación de 56/100, lo que equivale a una nota de D. Se ejecutaron un total de 9 checks pasivos, resultando en 3 verificaciones satisfactorias, 4 advertencias por configuraciones mejorables y 2 fallos críticos de seguridad. La auditoría revela una ausencia total de cabeceras de seguridad esenciales y la exposición de información sensible del sistema de gestión de contenidos. Debido a la combinación de una versión de software desactualizada y la falta de protecciones contra ataques web comunes, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0	5	6	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 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	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 1 expuesta
Seguridad de Cookies	67	AVISO	__cf_bm: falta SameSite
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-06-24T07:58:34.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-26T06:58:35.000Z
- 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: cloudflare — 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://www.tiendanube.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

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- 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: WPML ver:4.9.2 stt:42,66,69,68,67;
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 1 expuesta

- ALTO **WordPress version**
  Version 1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 67/100

Estado: AVISO

__cf_bm: falta SameSite

- INFO **Cookies detectadas**
  1 cookie(s) encontrada(s)
- INFO **Cookie: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: __cf_bm — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (405 bytes)
- INFO **Reglas robots.txt**
  11 Disallow, 0 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.tiendanube.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- 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

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] WordPress version: La versión 1 del CMS se encuentra expuesta públicamente, lo que facilita a atacantes la búsqueda y explotación de CVEs conocidos.
[HIGH] Content-Security-Policy: Falta esta cabecera crítica que previene ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: Ausencia de protección contra ataques de clickjacking, permitiendo que el sitio sea embebido en marcos externos no autorizados.
[HIGH] Strict-Transport-Security: La cabecera HSTS no está configurada, por lo que el servidor no obliga al navegador a mantener siempre una conexión segura.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, lo cual representa un riesgo al ser utilizado habitualmente para servicios de administración o proxies alternativos.
[MEDIUM] Recurso HTTP (Mixed Content): Se detectó un enlace a una hoja de estilo (gmpg.org) mediante protocolo inseguro HTTP dentro de una página HTTPS.
[MEDIUM] Cookie Security: La cookie __cf_bm carece del atributo SameSite, lo que incrementa el riesgo de ataques de falsificación de petición en sitios cruzados (CSRF).
[MEDIUM] X-Content-Type-Options: No se previene el MIME-type sniffing, lo que podría permitir que archivos cargados sean interpretados de forma malintencionada por el navegador.
[MEDIUM] Referrer-Policy: Falta el control sobre cuánta información de referencia se envía al navegar hacia otros dominios.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la ubicación, cámara o micrófono.
[LOW] Meta generator: El código fuente expone detalles específicos del plugin WPML, ayudando a perfilar la infraestructura interna.
[LOW] Server header expuesto: El encabezado revela el uso de tecnología Cloudflare, proporcionando datos útiles para la fase de reconocimiento de un atacante.
[LOW] Ruta sensible en robots.txt: Se hace referencia directa a rutas de administración, lo que orienta a posibles atacantes hacia paneles de acceso restringido.