EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.tiendaleet.com.ar	Checks	9 pruebas
Dominio	www.tiendaleet.com.ar	Hallazgos	52 totales
Fecha	15 de abril de 2026 a las 05:44	Problemas	8 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio tiendaleet.com.ar ha finalizado con una puntuación de 88/100 y una nota de calificación B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, uno generó una advertencia y uno fue calificado como fallo técnico. Los resultados indican una base sólida en el cifrado de datos y gestión de cookies, pero se detectaron omisiones importantes en las directivas de seguridad del servidor. En su estado actual, el sitio se considera mayoritariamente seguro, aunque presenta vulnerabilidades específicas que podrían ser aprovechadas para ataques de manipulación de interfaz.

Resumen de Riesgos

0	1	5	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 74 dias
Cabeceras de Seguridad	60	FALLO	Solo 3/6 presentes. Faltan: X-Frame-Options, Ref...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	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 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-06-28T05:07:23.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-30T04:07:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 60/100

Estado: FALLO

Solo 3/6 presentes. Faltan: X-Frame-Options, Referrer-Policy, Permissions-Policy

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

- INFO **Content-Security-Policy**
  Presente: frame-ancestors 'self' mitiendanube.com *.mitiendanube.com lojavirtualnuvem.com....
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.tiendaleet.com.ar/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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**
  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)

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- 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: __cf_bm — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __cf_bm — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __cf_bm — SameSite**
  SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1455 bytes)
- INFO **Reglas robots.txt**
  38 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://dcdn-us.mitiendanube.com/stores/983/409/themes/common/sitemap.xml.gz
- 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] X-Frame-Options: La ausencia de esta cabecera permite que el sitio sea embebido en marcos externos, facilitando ataques de clickjacking.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto y expuesto, funcionando como un servidor web alternativo que incrementa la superficie de ataque.
[MEDIUM] Ruta /administrator/: El panel de inicio de sesión administrativo es accesible de forma pública, lo que permite intentos de acceso no autorizado.
[MEDIUM] Referrer-Policy: La falta de esta cabecera impide controlar qué información de navegación se comparte con otros dominios al seguir enlaces.
[MEDIUM] Permissions-Policy: Al no estar definida, el sitio no restringe el acceso de las APIs del navegador a funciones sensibles como cámara o micrófono.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / impide la indexación por buscadores, lo cual suele ser un error de configuración en entornos de producción.
[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, entregando información técnica innecesaria sobre la infraestructura a potenciales atacantes.
[LOW] Ruta sensible en robots.txt: Se hace referencia explícita a la palabra admin dentro del archivo, ayudando a identificar directorios que deberían ser privados.