EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.desatascosjumbo.com	Checks	9 pruebas
Dominio	www.desatascosjumbo.com	Hallazgos	47 totales
Fecha	2 de junio de 2026 a las 04:21	Problemas	12 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación técnica de 68/100, lo que resulta en una calificación de grado C. Durante la evaluación se ejecutaron un total de 9 comprobaciones pasivas, obteniendo 6 resultados satisfactorios, 1 advertencia y 2 fallos críticos en la configuración. A pesar de contar con un cifrado de conexión adecuado, la ausencia de cabeceras de seguridad y la exposición de versiones desactualizadas representan un riesgo significativo. Se concluye que el sitio es actualmente vulnerable a ataques de inyección, clickjacking y explotación de vulnerabilidades conocidas en su CMS.

Resumen de Riesgos

0	5	4	3	35
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 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 5.8.1 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-07-18T03:27:48.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-19T03:27:49.000Z
- 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 — 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.desatascosjumbo.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: WordPress 5.8.1
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 5.8.1 expuesta

- ALTO **WordPress version**
  Version 5.8.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)

- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (67 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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] WordPress version: La versión 5.8.1 del CMS está expuesta públicamente, lo que facilita a atacantes la búsqueda de CVEs y exploits conocidos para tomar el control del sitio.
[HIGH] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts no autorizados, facilitando ataques de XSS y robo de datos.
[HIGH] X-Frame-Options: Al no estar configurada, el sitio puede ser cargado en marcos externos, permitiendo ataques de clickjacking para engañar a los usuarios.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS mediante HSTS, lo que permite ataques de degradación de protocolo y manipulación de tráfico.
[HIGH] HSTS (Strict-Transport-Security): El navegador no tiene instrucciones para forzar conexiones seguras de forma permanente.
[MEDIUM] WordPress login: La ruta /wp-login.php es accesible para cualquier usuario, permitiendo intentos de acceso no autorizado mediante fuerza bruta.
[MEDIUM] X-Content-Type-Options: Falta la protección contra el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos disfrazados de elementos legítimos.
[MEDIUM] Referrer-Policy: No se controla la información que el navegador envía a otros sitios al hacer clic en enlaces externos.
[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs del navegador como la cámara, el micrófono o la geolocalización.
[LOW] Server header expuesto: El servidor revela el uso de nginx, proporcionando información valiosa a posibles atacantes sobre la infraestructura base.
[LOW] Meta generator: La etiqueta meta expone explícitamente que se utiliza WordPress 5.8.1.
[LOW] Ruta sensible en robots.txt: El archivo menciona el directorio admin, lo que ayuda a mapear áreas restringidas del servidor.