EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://argtour.com	Checks	9 pruebas
Dominio	argtour.com	Hallazgos	49 totales
Fecha	18 de septiembre de 2026 a las 02:44	Problemas	7 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web argtour.com arroja una puntuación de 88/100 con una calificación de grado B. Se ejecutaron un total de 9 comprobaciones pasivas, de las cuales 7 resultaron satisfactorias, una generó una advertencia y una fue clasificada como fallo crítico. El sitio demuestra una implementación robusta de cifrado SSL y cabeceras de seguridad, pero falla significativamente al exponer información técnica interna del CMS. Aunque el entorno es generalmente estable, la visibilidad de versiones específicas permite que un atacante identifique vectores de explotación dirigidos. En conclusión, el sitio es mayormente seguro pero presenta vulnerabilidades de exposición de datos que deben ser mitigadas.

Resumen de Riesgos

0	1	3	3	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 63 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.1.1 expuesta, WordPress 2 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	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 63 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  63 dias restantes (expira: 2026-11-20T12:44:13.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-08-22T11:44:27.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

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

- INFO **Content-Security-Policy**
  Presente: block-all-mixed-content
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: no-referrer-when-downgrade
- INFO **Permissions-Policy**
  Presente: geolocation=*, midi=*, sync-xhr=(self "https://argtour.com" "https://www.argtour...

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://argtour.com/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no 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

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 7.1.1
- INFO **Tecnologias detectadas**
  Next.js, Astro

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.1.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.1.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Archivo /README.txt**
  No accesible (correcto)

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 (2974 bytes)
- INFO **Reglas robots.txt**
  18 Disallow, 7 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://argtour.com/sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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: Exposición pública de la versión 7.1.1 de WordPress, lo que permite a atacantes buscar vulnerabilidades conocidas (CVE) para esta versión específica.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, revelando un servidor web alternativo o proxy que aumenta la superficie de ataque del servidor.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y confirma la versión exacta y componentes del CMS instalado.
[MEDIUM] Bloqueo total en robots.txt: El archivo utiliza la directiva Disallow: / para bloquear todo el sitio, lo cual es una configuración anómala que puede ocultar contenido o indicar errores de despliegue.
[LOW] Meta generator: Presencia de etiquetas HTML que exponen el uso de WordPress 7.1.1 ante herramientas de escaneo automatizado.
[LOW] Ruta sensible en robots.txt: El archivo referencia la ruta "admin", proporcionando pistas directas sobre la estructura de directorios privados a agentes maliciosos.
[LOW] Server header expuesto: La cabecera de respuesta revela el uso de Cloudflare, entregando información sobre la infraestructura de red y seguridad perimetral.