EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://monteavilaeditores.com/	Checks	9 pruebas
Dominio	monteavilaeditores.com	Hallazgos	47 totales
Fecha	29 de agosto de 2026 a las 18:34	Problemas	13 detectados

C

68/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de seguridad realizado sobre el dominio monteavilaeditores.com ha arrojado una puntuacion de 68/100, lo que equivale a una nota de C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 genero una advertencia y 2 finalizaron con errores criticos. Aunque el sitio cuenta con cifrado basico y una gestion correcta de archivos de indexacion, presenta deficiencias severas en la configuracion de cabeceras de seguridad y exposicion de versiones de software. En su estado actual, el sitio se considera vulnerable a ataques de inyeccion, suplantacion y explotacion de vulnerabilidades conocidas en el CMS.

Resumen de Riesgos

0	5	5	3	34
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 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, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.12.0 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	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 58 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  58 dias restantes (expira: 2026-10-27T03:18:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-07-29T03:18:16.000Z
- 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/1.29.8 — 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://monteavilaeditores.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, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Redux 4.5.13
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.12.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.12.0 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)

- 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 (325 bytes)
- INFO **Reglas robots.txt**
  6 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://monteavilaeditores.com/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Cerrado — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecucion de scripts maliciosos y ataques de inyeccion de contenido como XSS.
[HIGH] Falta de X-Frame-Options: El sitio es vulnerable a ataques de clickjacking, permitiendo que atacantes carguen la web en frames externos para engañar al usuario.
[HIGH] Falta de Strict-Transport-Security: No se fuerza la conexion HTTPS mediante HSTS, lo que facilita ataques de degradacion de protocolo (SSL Stripping).
[HIGH] Version de WordPress expuesta: La deteccion publica de la version 6.12.0 permite a los atacantes identificar y explotar CVEs especificos para ese motor.
[MEDIUM] Falta de X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, facilitando ataques de MIME-sniffing.
[MEDIUM] Falta de Referrer-Policy: No existe control sobre la informacion de procedencia enviada en las peticiones, lo que puede filtrar URLs privadas a sitios de terceros.
[MEDIUM] Falta de Permissions-Policy: El sitio no restringe el uso de funciones sensibles del navegador como la camara, el microfono o la geolocalizacion.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela informacion tecnica del CMS que deberia ser privada para evitar el reconocimiento por parte de atacantes.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es publico, lo que aumenta el riesgo de ataques de fuerza bruta contra las credenciales.
[LOW] Cabecera Server expuesta: El servidor revela el uso de nginx/1.29.8, informacion que ayuda a los atacantes a realizar ataques dirigidos a dicha arquitectura.
[LOW] Meta generator expuesto: Se detecto la presencia de Redux 4.5.13, revelando detalles adicionales sobre la estructura interna y plugins instalados.
[LOW] Ruta sensible en robots.txt: La referencia directa a directorios admin en el archivo de rastreo facilita el mapeo de rutas protegidas para agentes maliciosos.