EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.grupovadillo.com	Checks	9 pruebas
Dominio	www.grupovadillo.com	Hallazgos	47 totales
Fecha	28 de julio de 2026 a las 14:44	Problemas	6 detectados

B

88/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 88/100 con una calificación de nota B. Durante la auditoría se ejecutaron 9 checks pasivos, resultando en 7 verificaciones exitosas, 1 advertencia y 1 fallo crítico detectado. El sitio demuestra una implementación sólida en cuanto a cifrado de datos y cabeceras de protección, pero presenta debilidades en el mantenimiento del software base y la exposición de servicios de red. Se concluye que el sitio es mayoritariamente seguro para el usuario final, pero vulnerable ante ataques dirigidos debido a la exposición de información técnica y puertos críticos.

Resumen de Riesgos

0	2	2	2	41
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 58 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 6.1.6 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	2 puerto(s) potencialmente riesgoso(s): 21 (FTP)...

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: 2026-09-24T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-11T00:00:00.000Z
- 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: Apache — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: DENY
- 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=self

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.grupovadillo.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
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.1.6 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.1.6 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 (759 bytes)
- INFO **Reglas robots.txt**
  5 Disallow, 14 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://www.grupovadillo.com/sitemap_index.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

2 puerto(s) potencialmente riesgoso(s): 21 (FTP), 22 (SSH)

- ALTO **Puerto 21 (FTP)**
  ABIERTO — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

[ALTA] Versión de WordPress expuesta: La versión 6.1.6 es visible públicamente, lo que permite a atacantes identificar y explotar vulnerabilidades conocidas (CVEs) de esta versión específica.
[ALTA] Puerto 21 (FTP) abierto: Este puerto permite la transferencia de archivos sin cifrado, facilitando la interceptación de credenciales y datos sensibles en la red.
[MEDIA] Puerto 22 (SSH) abierto: El acceso remoto seguro está expuesto, lo que incrementa el riesgo de intentos de intrusión mediante ataques de fuerza bruta.
[MEDIA] Archivo /readme.html accesible: Este archivo es público y puede confirmar la versión exacta del CMS y otros detalles técnicos de la instalación.
[BAJA] Cabecera de servidor expuesta: El servidor revela el uso de Apache, proporcionando información valiosa a los atacantes para perfilar la infraestructura tecnológica.
[BAJA] Ruta sensible en robots.txt: El archivo incluye una referencia directa a la ruta de administración, ayudando a los atacantes a localizar paneles de acceso restringidos.