EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://Pollaya.com	Checks	9 pruebas
Dominio	pollaya.com	Hallazgos	51 totales
Fecha	18 de junio de 2026 a las 05:14	Problemas	15 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado en Pollaya.com arroja una puntuación de 72/100 con una calificación de nota C. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con fallos críticos. Aunque el sitio cuenta con una base sólida en cuanto a cifrado SSL y redirecciones seguras, presenta deficiencias importantes en la configuración de cabeceras de seguridad y exposición de información técnica. La visibilidad de la versión del CMS y la apertura de puertos no estándar elevan la superficie de ataque. En su estado actual, el sitio se considera vulnerable a ataques de nivel intermedio que podrían comprometer la integridad de la sesión del usuario o facilitar el reconocimiento para exploits específicos.

Resumen de Riesgos

0	3	9	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 73 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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 6.8.5 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 73 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  73 dias restantes (expira: 2026-08-30T16:42:12.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-01T16:02:39.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- 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 — 100/100

Estado: OK
HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://pollaya.com/
- 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
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 6.8.5
- INFO **Tecnologias detectadas**
  Next.js, ASP.NET

Version CMS Expuesta — 20/100

Estado: FALLO
WordPress 6.8.5 expuesta

- ALTO **WordPress version**
  Version 6.8.5 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  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 (169 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- INFO **Sitemap en robots.txt**
  https://pollaya.com/sitemap_index.xml
- 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] Content-Security-Policy: La ausencia de esta cabecera impide prevenir ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en frames externos.
[HIGH] Versión de WordPress expuesta: La versión 6.8.5 es visible públicamente, lo que permite a atacantes identificar y explotar CVEs conocidos para esa versión específica.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite ataques de MIME-type sniffing, donde el navegador interpreta archivos de forma incorrecta.
[MEDIUM] Referrer-Policy: No se controla la información de referencia enviada a otros sitios, lo que puede fugar datos de navegación sensibles.
[MEDIUM] Permissions-Policy: No se restringe el acceso a APIs del navegador, dejando expuestas funciones como cámara o micrófono ante posibles vulnerabilidades de scripts.
[MEDIUM] Archivos informativos expuestos: El acceso público a /readme.html y /README.txt facilita la obtención de metadatos sobre la instalación del CMS.
[MEDIUM] Rutas de administración accesibles: Los paneles /wp-login.php, /administrator/ y /user/login están abiertos, facilitando intentos de fuerza bruta.
[MEDIUM] Puerto 8080 (HTTP-Alt): El puerto se encuentra abierto, funcionando como un servidor web alternativo o proxy que amplía la superficie de exposición.
[LOW] Cabecera Server expuesta: Se revela el uso de Cloudflare, proporcionando pistas sobre la infraestructura de red utilizada.
[LOW] X-Powered-By expuesto: El servidor informa el uso de ASP.NET, revelando el framework de desarrollo subyacente.
[LOW] Meta generator detectado: El código fuente incluye la etiqueta que identifica explícitamente el uso de WordPress 6.8.5.