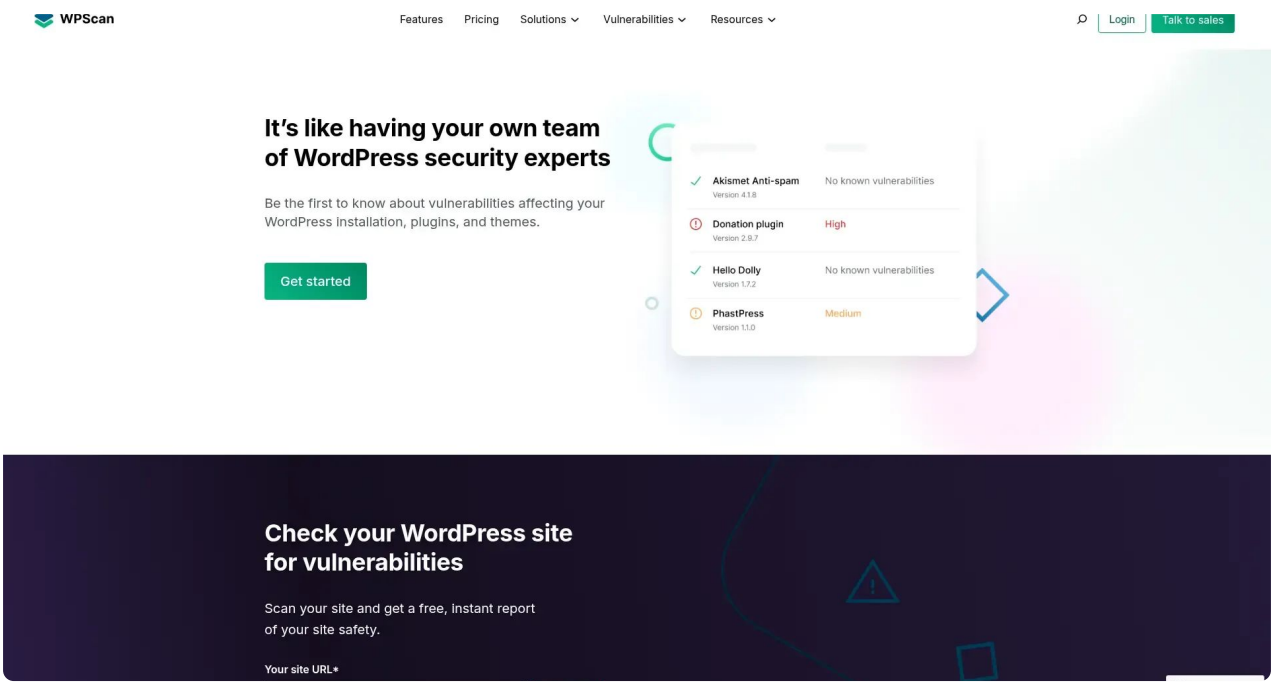

WPScan.com

WPScan es una herramienta de seguridad de caja negra diseñada para administradores de sistemas, desarrolladores y auditores que gestionan sitios WordPress. Permite identificar vulnerabilidades críticas en el núcleo, plugins y temas mediante una base de datos propia verificada por expertos. Es ideal para realizar auditorías técnicas, enumeración de usuarios y pruebas de fuerza bruta, garantizando que la infraestructura web esté protegida contra ataques conocidos antes de que ocurran.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
WPScan es una herramienta de seguridad especializada en el ecosistema WordPress, diseñada para identificar vulnerabilidades en el núcleo (core), plugins y temas. Se trata de un escáner de "caja negra" que simula el punto de vista de un atacante para encontrar fallos de seguridad sin necesidad de acceso al panel de administración. Está dirigida a administradores de sistemas, desarrolladores web, consultores de ciberseguridad y agencias que gestionen parques de sitios basados en WordPress y busquen una auditoría técnica rigurosa.

Principal ventaja profesional
Su base de datos de vulnerabilidades es propia, está verificada manualmente por expertos en seguridad y es considerada el estándar de la industria, alimentando incluso a otras herramientas de seguridad de renombre en el mercado.

Para quién no es
No es una herramienta para usuarios finales sin conocimientos técnicos que busquen un antivirus "instalar y olvidar". Tampoco es adecuada para profesionales que no trabajen específicamente con WordPress o para aquellos que busquen una herramienta de limpieza automática de malware, ya que WPScan solo identifica riesgos, no los repara.

funcionalidades clave
- Escaneo de vulnerabilidades en el núcleo de WordPress, plugins y temas instalados.
- Enumeración de usuarios y ataques de fuerza bruta para probar la robustez de las contraseñas.
- Detección de archivos de configuración expuestos (wp-config.php), volcados de bases de datos y archivos de registro de errores.
- Identificación de directorios de archivos multimedia y listado de directorios de subidas.
- Comprobación de versiones de software obsoletas y referencias a CVE (Common Vulnerabilities and Exposures).
- Modos de escaneo configurables: pasivo, agresivo o mixto según la carga permitida en el servidor.
- Generación de informes en formatos legibles por humanos y en formato JSON para automatización.

Precios
- Versión gratuita: El escáner CLI es de uso gratuito. El acceso a la API es gratuito para uso no comercial y está limitado a 25 peticiones diarias.
- Rango de precios: Precios bajo presupuesto (Enterprise) basados en el volumen de sitios o uso de la API.
- Versiones de pago (Enterprise): Incluye acceso completo a puntuaciones de riesgo CVSS, descripciones detalladas de vulnerabilidades, pruebas de concepto (PoC), alertas por email instantáneas y webhooks para integración con Slack o HTTP.

Perfil del usuario
- Agencias de desarrollo web y mantenimiento WordPress.
- Departamentos de IT en empresas con infraestructuras basadas en WordPress.
- Auditores de seguridad y Pentester.
- Proveedores de alojamiento administrado (Managed WordPress Hosting).

Nivel técnico requerido
- Nivel técnico requerido para su uso: Medio-Alto (manejo de línea de comandos).
- Nivel técnico requerido para su instalación/configuración: Medio (requiere Ruby y gestión de dependencias en sistemas Linux/Mac).
- Necesidades de soporte de departamentos: No requiere soporte externo si se dispone de perfiles técnicos internos.
- Conocimientos necesarios: Manejo de terminal (CLI), conocimientos básicos de arquitectura WordPress y protocolos HTTP.

Ejemplos de uso profesional
- Auditorías preventivas semanales para asegurar que los sitios de clientes no tienen plugins vulnerables.
- Integración en flujos de CI/CD para bloquear despliegues que contengan componentes con fallos de seguridad conocidos.

- Monitorización centralizada mediante Webhooks para recibir alertas cuando aparece una nueva vulnerabilidad crítica afectando a la infraestructura de la empresa.

Uso y distribución
- Versión web: A través de su base de datos online para consultas manuales.
- Versión escritorio: Compatible con sistemas Linux y macOS.
- CLI: Interfaz de línea de comandos principal (Ruby-based).
- Integración mediante plugin: Disponible a través del plugin Jetpack Protect.

Open source
El escáner CLI de WPScan tiene componentes de código abierto, pero su distribución y uso comercial están sujetos a una licencia personalizada de Automattic que requiere pago si se utiliza con fines lucrativos.

Integraciones
- Facilidad de integración: Alta para perfiles técnicos (Full-code vía API).
- API propia: API v3 con endpoints para consultar vulnerabilidades por versión, slug de plugin o tema.
- Ejemplos concretos: Integración nativa con Slack mediante Webhooks, conectores para sistemas de alerta personalizados por HTTP y alimentación de datos para otros plugins de seguridad.

Notas finales
información legal, licencias, contratos
- Desde agosto de 2024, WPScan es propiedad de Automattic Inc.
- El uso comercial de los datos de la vulnerabilidad y la API requiere obligatoriamente una licencia de pago.
- Prohibida la descarga masiva de la base de datos o el uso de los datos para crear productos competidores sin autorización expresa.

Para más información:
- Sitio web oficial: https://wpscan.com
- Precios: https://wpscan.com/pricing
- Documentación de API: https://wpscan.com/docs/api/v3
- Condiciones de servicio: https://wpscan.com/terms
- Github: https://github.com/wpscanteam/wpscan

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
WPScan es una herramienta de auditoría de seguridad externa (Black Box) para infraestructuras WordPress. Es ideal para agencias con carteras de más de 20 sitios, equipos de SecDevOps que integran escaneos en CI/CD y empresas de hosting gestionado. Requiere presupuesto para la licencia comercial si se ofrece como servicio a terceros. Sus puntos clave son la detección precoz de vulnerabilidades en plugins/temas y la simulación de ataques reales de enumeración de usuarios.

Madurez digital requerida
- Usuarios: Esencial dominio de terminal (CLI) y comprensión de vulnerabilidades Web (XSS, SQLi). No apto para usuarios de perfil administrativo o de marketing.
- Empresa: Debe contar con flujos de trabajo de ciberseguridad o mantenimiento preventivo establecidos.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Tiempos de despliegue: Entre 1 y 3 días para una integración básica en entornos locales o servidores de auditoría.
- Evaluación inicial: Auditoría del número de sitios a monitorizar (media de 22 peticiones API por sitio) para determinar el plan de licencia necesario con Automattic.
- Prueba de concepto: Configuración de un entorno con Ruby y ejecución de escaneos manuales contra copias de respaldo para verificar falsos positivos (tasa estimada del 3% por duplicidad de slugs).
- Integración y automatización: Implementación de scripts (Bash/Python) para automatizar escaneos semanales y envío de resultados JSON a sistemas de monitorización centralizada.
- Configuración de alertas: Personalización de Webhooks (Slack/HTTP) para que el equipo técnico reciba notificaciones críticas de forma inmediata.

Necesidades de formación del equipo
- Uso avanzado de la CLI de WPScan y sus diferentes modos de escaneo (passive, aggressive, mixed).
- Interpretación de puntuaciones de riesgo CVSS y vectores de ataque identificados.
- Formación en la resolución manual de los hallazgos (parcheo de plugins, endurecimiento de wp-config.php).

Perfiles necesarios
- Especialista en Ciberseguridad o Pentester para la interpretación de informes.
- Desarrollador Backend/DevOps para la integración en pipelines y automatización de tareas.
- Enfoque externo: Opcionalmente, consultores de seguridad para auditorías profundas trimestrales utilizando la base de datos completa de WPScan.

Retorno de la inversión (ROI)
- Tiempos: Reducción del 40% en el tiempo de identificación de vulnerabilidades específicas de WordPress frente a escáneres genéricos.
- KPIs: Número de vulnerabilidades detectadas antes de ser explotadas, tiempo medio de respuesta (MTTR) ante CVEs críticas y reducción de incidentes de inyección de código.

Otros
- Licenciamiento comercial: Es obligatorio adquirir una licencia de pago si WPScan se utiliza para generar ingresos directos (por ejemplo, como parte de un plan de mantenimiento pagado por clientes).
- Propiedad de Automattic: Al ser parte del ecosistema de Automattic (propietarios de WordPress.com y Jetpack), la herramienta tiene garantizada la actualización constante de su base de datos frente a cualquier cambio en el núcleo de WordPress.

PREGUNTAS FRECUENTES

¿Qué es WPScan y cuál es su función principal?
WPScan es un escáner de seguridad de 'caja negra' especializado en WordPress que identifica vulnerabilidades en el núcleo, plugins y temas. Su función es simular ataques externos para detectar fallos de seguridad sin requerir acceso administrativo al sitio web.

¿Para qué sirve esta herramienta en un entorno profesional?
Se utiliza para realizar auditorías técnicas rigurosas, enumeración de usuarios, ataques de fuerza bruta controlados y detección de archivos críticos expuestos (como wp-config.php), permitiendo a los administradores anticiparse a posibles explotaciones de seguridad.

¿Cuánto cuesta y qué incluye la versión gratuita?
El escáner CLI es gratuito para uso personal. La API ofrece un nivel gratuito limitado a 25 peticiones diarias para uso no comercial. Las versiones Enterprise requieren presupuesto personalizado según el volumen de sitios y ofrecen datos detallados de riesgo CVSS y alertas en tiempo real.

¿Es una solución open source?
Aunque el código del escáner CLI está disponible en GitHub bajo componentes de código abierto, su uso comercial y el acceso a la base de datos de vulnerabilidades están sujetos a una licencia privativa de Automattic que requiere pago para fines lucrativos.

¿Cómo se instala y qué requisitos técnicos tiene?
Requiere un nivel técnico medio-alto. Se instala principalmente como una gema de Ruby en entornos Linux o macOS y se opera a través de la interfaz de línea de comandos (CLI), siendo necesaria la gestión de dependencias en el sistema operativo.

¿Cumple con normativas de privacidad y seguridad?
WPScan se enfoca en la detección de vulnerabilidades técnicas y no almacena datos personales de los visitantes del sitio escaneado. No obstante, al ser propiedad de Automattic, el uso de su API y servicios web se rige por sus políticas de privacidad y términos de servicio actualizados en 2024.

¿Puede WPScan reparar automáticamente las vulnerabilidades encontradas?
No, es una herramienta de diagnóstico, no de remediación. WPScan identifica los riesgos y facilita referencias a CVE (Common Vulnerabilities and Exposures), pero no realiza limpieza de malware ni aplica parches de seguridad de forma automática.

¿Es posible integrarlo en flujos de trabajo automatizados?
Sí, ofrece una alta integración para perfiles técnicos mediante su API v3 y Webhooks. Es común su uso en flujos de CI/CD para bloquear despliegues inseguros y en integraciones con plataformas como Slack para recibir alertas críticas inmediatas.

¿Cuáles son las limitaciones de la base de datos de vulnerabilidades?
La base de datos está verificada manualmente por expertos y es un estándar de la industria, pero su descarga masiva está prohibida. El acceso comercial a estos datos requiere obligatoriamente una licencia de pago y no puede usarse para crear productos competidores.

¿Es una tecnología segura para ejecutar contra mis propios servidores?
Sí, permite configurar modos de escaneo (pasivo, agresivo o mixto) para controlar la carga sobre el servidor. En modo pasivo, el impacto en el rendimiento es mínimo, permitiendo auditorías frecuentes sin afectar la disponibilidad del servicio.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- Obtener siempre autorización previa por escrito del propietario del sitio web antes de realizar escaneos, para evitar infracciones legales relacionadas con el acceso no autorizado a sistemas informáticos.
- Diferenciar estrictamente entre el uso personal/educativo y el uso comercial; este último requiere obligatoriamente una licencia de pago de Automattic.
- No utilizar los datos obtenidos (vulnerabilidades) para crear herramientas o servicios que compitan directamente con WPScan, ya que está prohibido por sus términos.
- Configurar el escáner en modo "pasivo" o moderado para no afectar a la disponibilidad del servicio del cliente y evitar posibles reclamaciones por daños en el servidor.
- Revisar periódicamente las condiciones de la API, ya que tras la adquisición por parte de Automattic, los límites y términos comerciales han sido actualizados.

Privacidad y protección de datos
- Responsabilidades: La empresa que ejecuta el escaneo actúa como Responsable del Tratamiento si maneja datos personales (como enumeración de usuarios). WPScan (Automattic) actúa como proveedor de datos de vulnerabilidades.
- Ubicación de los datos: Los datos de la cuenta y las claves de la API se gestionan en servidores de Automattic Inc., ubicados principalmente en Estados Unidos.
- Transferencia internacional: El uso de la API implica la transferencia de datos (direcciones IP, versiones de software) a EE.UU. Se ampara en el Marco de Privacidad de Datos (Data Privacy Framework) y Cláusulas Contractuales Tipo.
- Derechos ARCO: Los usuarios pueden ejercer sus derechos de acceso, rectificación, cancelación y oposición ante Automattic Inc. a través de sus canales oficiales de privacidad.

Propiedad intelectual
- Propiedad de datos: Los datos de la base de datos de vulnerabilidades de WPScan son propiedad intelectual exclusiva de Automattic Inc. No pueden ser descargados de forma masiva ni redistribuidos.
- Propiedad del resultado: Los informes generados pertenecen a la empresa que realiza la auditoría, pero la información técnica sobre la vulnerabilidad en sí misma sigue estando sujeta a los derechos de autor de la base de datos de origen.
- Licencia de software: El código del escáner CLI está disponible bajo una licencia personalizada (no es GPL estándar). Permite el uso gratuito para individuos, pero exige licencia comercial para empresas o autónomos que ofrezcan servicios a terceros.

Usos y prohibiciones
- Usos prohibidos: Queda terminantemente prohibido el "scraping" de la base de datos de vulnerabilidades, el uso de la herramienta para actividades de hacking no ético o ataques de denegación de servicio.
- Usos admitidos: Auditoría de seguridad propia, consultoría de ciberseguridad para clientes (previa licencia), integración en procesos internos de desarrollo seguro.

Seguridad y certificaciones
- Seguridad: La herramienta utiliza el protocolo HTTPS para todas las consultas a la API y el almacenamiento de claves API se realiza mediante cifrado.
- Certificaciones: Automattic, como empresa matriz, sigue estándares elevados de seguridad, aunque WPScan como herramienta específica no detalla certificaciones SOC2 individuales de forma pública.

Otros
- Impacto legal: Medio. Aunque es una herramienta de diagnóstico, su uso incorrecto contra terceros sin permiso puede derivar en responsabilidades penales en España (Delitos contra el patrimonio y el orden socioeconómico o descubrimiento y revelación de secretos).
- Cambios por adquisición: La integración con Jetpack y el ecosistema de Automattic ha endurecido el control sobre el uso comercial de la API.

Fuentes consultada:
- Contratos: https://wpscan.com/terms
- Privacidad: https://automattic.com/privacy

- Licencias: https://github.com/wpscanteam/wpscan/blob/master/LICENSE
- Documentación API: https://wpscan.com/docs/api/v3

Para más información y herramientas:

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

Inicio Todas las herramientas Categorías