




Reporte

 Propietario	 Ayala Arroyo Raúl
 Etiquetas	

Servicios y Versiones Detectados

El escaneo realizado con Nmap en el host `192.168.100.13` detectó los siguientes servicios y versiones en los puertos abiertos:

1. Puerto 80/tcp (HTTP):

- **Servicio:** Apache HTTP
- **Versión:** Apache httpd 2.4.62 (Debian)

2. Puerto 443/tcp (HTTPS):

- **Servicio:** Apache HTTP (SSL)
- **Versión:** Apache httpd 2.4.62 (Debian)

Resultados del Escaneo de Vulnerabilidades

El comando `nmap -sV --script=vuln 192.168.100.13` fue utilizado para buscar vulnerabilidades conocidas en los servicios detectados. A continuación se presentan los resultados y una breve explicación:

- **Apache HTTP Server (Versión 2.4.62 en Debian):**
 - **HTTP (`80/tcp`):**
 - **http-server-header:** Muestra la versión del servidor (Apache/2.4.62 en Debian).
 - **http-stored-xss:** No se encontraron vulnerabilidades de XSS almacenadas.
 - **http-dombased-xss:** No se detectaron vulnerabilidades XSS basadas en DOM.
 - **http-csrf:** No se encontraron vulnerabilidades CSRF.

- **http-enum:** Se encontraron las siguientes rutas:
 - `/wordpress/` : Indica la presencia de un blog en WordPress.
 - `/info.php` : Archivo que posiblemente contiene información del servidor.
 - `/wordpress/wp-login.php` : Página de inicio de sesión de WordPress.
- **HTTPS (`443/tcp`):**
 - **http-server-header:** Muestra la versión del servidor (Apache/2.4.62 en Debian).
 - **http-stored-xss:** No se encontraron vulnerabilidades de XSS almacenadas.
 - **http-dombased-xss:** No se detectaron vulnerabilidades XSS basadas en DOM.
 - **http-csrf:** No se encontraron vulnerabilidades CSRF.
 - **http-enum:** Rutas detectadas:
 - `/wordpress/` : Blog de WordPress.
 - `/info.php` : Archivo de información potencial.
 - `/wordpress/wp-login.php` : Página de inicio de sesión de WordPress.

Búsqueda de Vulnerabilidades en Bases de Datos Públicas

Para cada servicio y versión detectada, es recomendable buscar en bases de datos públicas de vulnerabilidades para obtener información adicional. A continuación, se presentan algunos enlaces útiles para investigar las vulnerabilidades específicas de **Apache HTTP 2.4.62** y **WordPress**:

1. Apache HTTP Server 2.4.62

NVD (National Vulnerability Database)

La **National Vulnerability Database (NVD)** es una base de datos pública y completa de vulnerabilidades mantenida por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. La NVD asigna identificadores CVE (Common Vulnerabilities and Exposures) a cada

vulnerabilidad y les otorga puntuaciones basadas en el CVSS (Common Vulnerability Scoring System) para indicar la gravedad de cada una. Al buscar **Apache HTTP Server 2.4.62** en la NVD, puedes encontrar vulnerabilidades específicas de esta versión y sus posibles soluciones o parches, lo cual es crucial para evaluar y mitigar riesgos en entornos de producción.

CVE Details para Apache HTTP Server

CVE Details es una plataforma que organiza las vulnerabilidades por productos, incluyendo su puntaje CVSS, tipo de ataque y el impacto. Proporciona información detallada sobre cada CVE, incluyendo enlaces a recursos y soluciones. Este sitio permite una búsqueda específica para Apache HTTP Server, donde puedes revisar vulnerabilidades relacionadas con la versión 2.4.62 y ver detalles sobre los exploits conocidos, impactos potenciales y enlaces a los parches necesarios.

Exploit Database

Exploit Database es un repositorio de exploits que permite a los profesionales de seguridad ver ejemplos específicos de cómo pueden explotarse ciertas vulnerabilidades en diferentes productos y versiones. Para **Apache HTTP Server**, puedes buscar exploits específicos de la versión 2.4.62 y encontrar detalles técnicos sobre cómo se aprovechan las fallas de seguridad, además de posibles medidas de mitigación. Es una excelente fuente para entender las técnicas que los atacantes podrían usar y preparar defensas efectivas.

2. WordPress (para el blog detectado en `/wordpress/`)

Vulnerabilidades de WordPress en Exploit Database

La sección de **WordPress en Exploit Database** contiene una lista de exploits conocidos para varias versiones de WordPress y sus complementos. Dado que WordPress es una de las plataformas de gestión de contenido más utilizadas, los atacantes suelen buscar vulnerabilidades en sus temas y complementos. Exploit Database es útil para descubrir exploits conocidos que pueden afectar a una instalación de WordPress, especialmente si no está actualizada, y ver ejemplos de código que los atacantes podrían usar para comprometer el sistema.

Vulnerabilidades de WordPress en CVE Details

CVE Details también tiene una sección específica para WordPress, donde puedes buscar vulnerabilidades de esta plataforma por versión. Esta base de datos categoriza las vulnerabilidades por tipo de ataque, como inyecciones SQL, XSS (Cross-Site Scripting), y más. Al buscar WordPress en CVE Details, obtienes un panorama de vulnerabilidades categorizadas con sus respectivos impactos y, en muchos casos, enlaces a soluciones o mitigaciones.

Vulners - WordPress

Vulners es una plataforma de búsqueda de vulnerabilidades que compila información de varias bases de datos, incluyendo CVE, Exploit Database, y otras fuentes. En la sección de WordPress, puedes buscar vulnerabilidades específicas de versiones de WordPress y de sus complementos. Vulners es especialmente útil porque muestra una lista consolidada de todas las vulnerabilidades, proporcionando enlaces directos a los recursos de cada vulnerabilidad, con recomendaciones para mitigarlas y reducir los riesgos.

Resumen de Posibles Vulnerabilidades

1. Apache HTTP Server 2.4.62

- **Inyección de Comandos:** Permite a un atacante ejecutar comandos arbitrarios en el servidor.
- **Explotación de Módulos:** Módulos como `mod_ssl` pueden introducir vulnerabilidades si no están bien configurados o actualizados.
- **Cross-Site Scripting (XSS):** Puede afectar a aplicaciones web en Apache si no se aplican configuraciones de seguridad adecuadas.
- **Desbordamiento de Búfer:** Riesgo de ejecución de código malicioso si hay un fallo de memoria.
- **Fuga de Información:** Configuraciones incorrectas pueden exponer información sensible sobre el sistema.

Fuentes para explorar vulnerabilidades: [NVD](#), [CVE Details](#), [Exploit Database](#).

2. WordPress (en `/wordpress/`)

- **Inyección SQL:** Complementos inseguros pueden permitir ataques de SQL Injection.
- **XSS:** Plugins y temas pueden ser vulnerables a XSS, permitiendo scripts maliciosos en el navegador del usuario.
- **Control de Acceso Insuficiente:** Permisos mal configurados pueden dar acceso a usuarios no autorizados.
- **Plugins y Temas No Actualizados:** Plugins obsoletos son una vía común de ataque.
- **Autenticación Débil:** Sin medidas adicionales, la página `wp-login.php` es vulnerable a ataques de fuerza bruta.

Fuentes para explorar vulnerabilidades en WordPress: [Exploit Database](#), [CVE Details](#), [Vulners](#).

Recomendaciones

- **Actualizar Apache HTTP Server:** Verificar que el servidor esté en su versión más reciente y que incluya parches de seguridad.
- **Asegurar WordPress:**
 - Mantener actualizados WordPress, temas y complementos.
 - Implementar medidas de seguridad adicionales, como el uso de autenticación de dos factores en el acceso al panel de administración.
 - Limitar el acceso al archivo `info.php` o eliminarlo si no es necesario, ya que podría exponer información del sistema.