Dado el Servidor **Web Machine: (N7)** el cual lo podemos encontrar en el siguiente enlace: https://www.vulnhub.com/entry/web-machine-n7,756/#vm

Web Machine: (N7) es una máquina virtual vulnerable diseñada específicamente para que los entusiastas de la seguridad informática practiquen sus habilidades de pentesting, especialmente en el ámbito de la seguridad web. Esta máquina presenta una serie de vulnerabilidades comunes que se encuentran en aplicaciones web reales, ofreciendo un entorno controlado para aprender y experimentar. En el cual podemos encontrar las siguientes vulnerabilidades:

- **Inyección SQL:** Permite a un atacante manipular las consultas a una base de datos.
- **Cross-Site Scripting (XSS):** Permite a un atacante inyectar código malicioso en una página web para robar información o realizar otras acciones no autorizadas.
- **Inyección de comandos:** Permite a un atacante ejecutar comandos en el sistema operativo del servidor.
- **Gestión de sesiones débil:** Puede permitir a un atacante secuestrar sesiones de usuarios autenticados.
- **Otros:** Y muchas más vulnerabilidades que dependerán de la configuración específica de la máquina.

PROCEDIMIENTO

1. **Descarga:** Primero, debes descargar la imagen de la máquina virtual desde el sitio web de VulnHub.
2. **Implementación:** Una vez descargada, tendrás que importar la imagen a una herramienta de virtualización como VirtualBox o VMware.
3. **Enumeración:** Comienza por realizar un escaneo de puertos para identificar los servicios que están en ejecución en la máquina.
4. **Explotación:** Una vez que hayas identificado los servicios vulnerables, podrás utilizar herramientas y técnicas de pentesting para explotar las vulnerabilidades y obtener acceso a la máquina.

Herramientas que se pueden usar para explorar Web Machine(N7):

- **Nmap:** Para realizar escaneos de puertos y descubrir servicios.
- **Burp Suite:** Una suite completa de herramientas para realizar pruebas de seguridad web.
- **OWASP ZAP:** Un escáner de vulnerabilidades web de código abierto.
- **Netcat:** Para interactuar con servicios de red.
- **Otros:** Herramientas como sqlmap, exploit-db, etc., pueden ser útiles para explotar vulnerabilidades específicas.

Recomendaciones:

- Lleva un registro detallado de tus pasos para poder replicar tus hallazgos y aprender de tus errores.
- Resolver los desafíos de una máquina vulnerable puede requerir tiempo y esfuerzo.