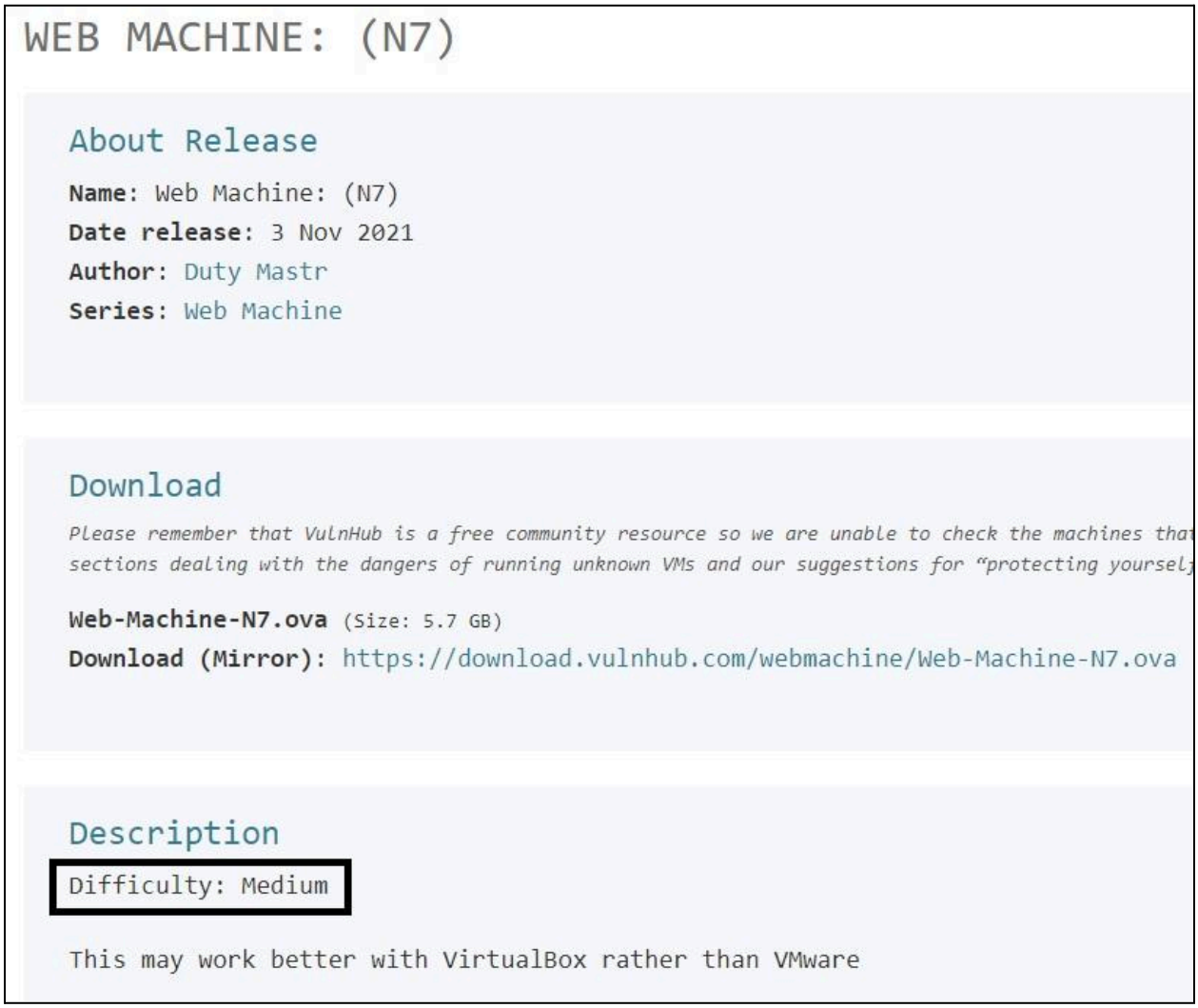
Rafael Aguiar Muñoz



WEB MACHINE: (N7)

About Release

Name: Web Machine: (N7)
Date release: 3 Nov 2021
Author: Duty Mastr
Series: Web Machine

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that
sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yoursel

Web-Machine-N7.ova (Size: 5.7 GB)
Download (Mirror): https://download.vulnhub.com/webmachine/Web-Machine-N7.ova

Description

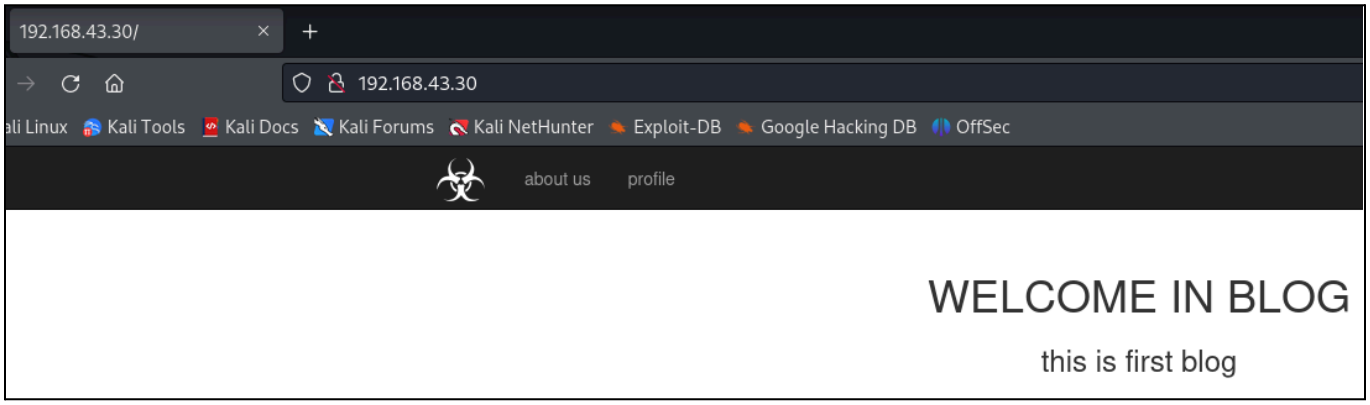
Difficulty: Medium

This may work better with VirtualBox rather than VMware

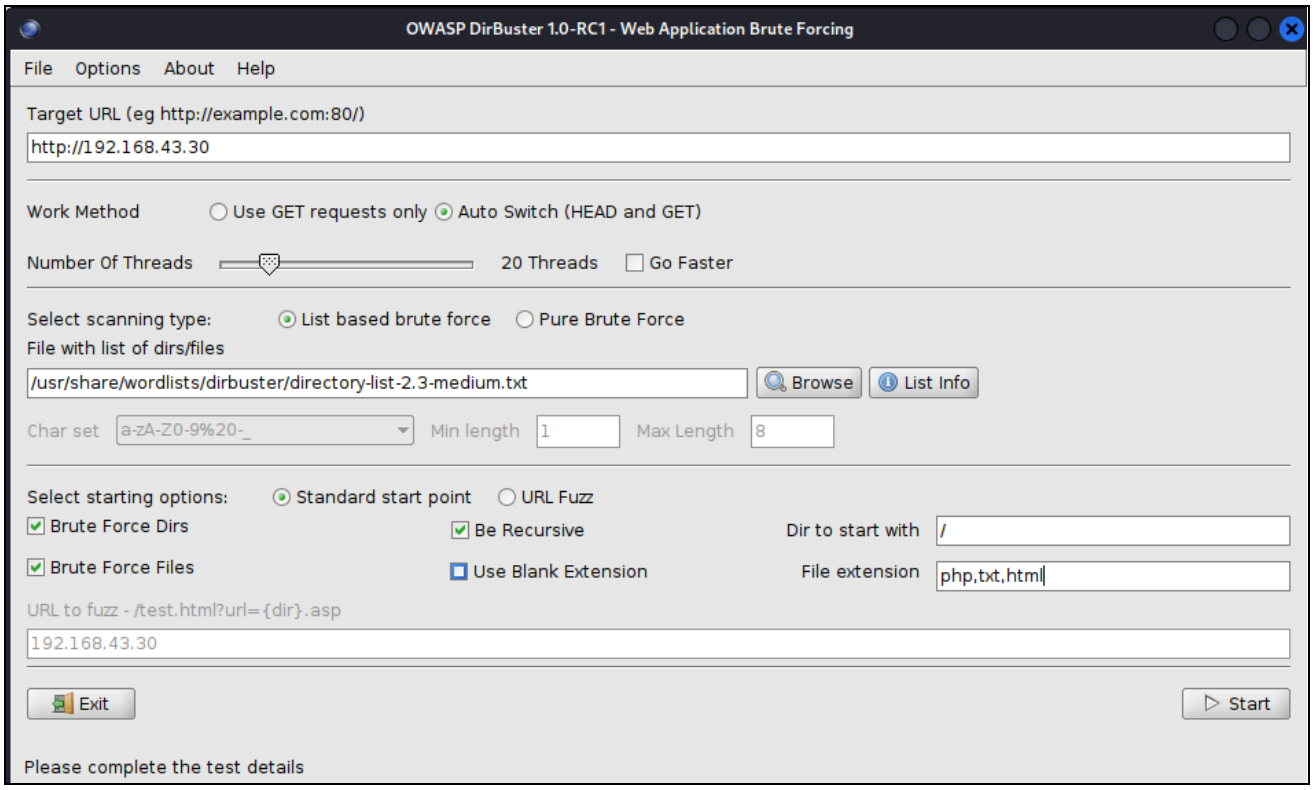
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -A -Pn 192.168.43.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 05:26 EST
Nmap scan report for 192.168.43.30
Host is up (0.0037s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.46 ((Debian))
|_http-server-header: Apache/2.4.46 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:ED:BD:C7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.70 ms 192.168.43.30
```

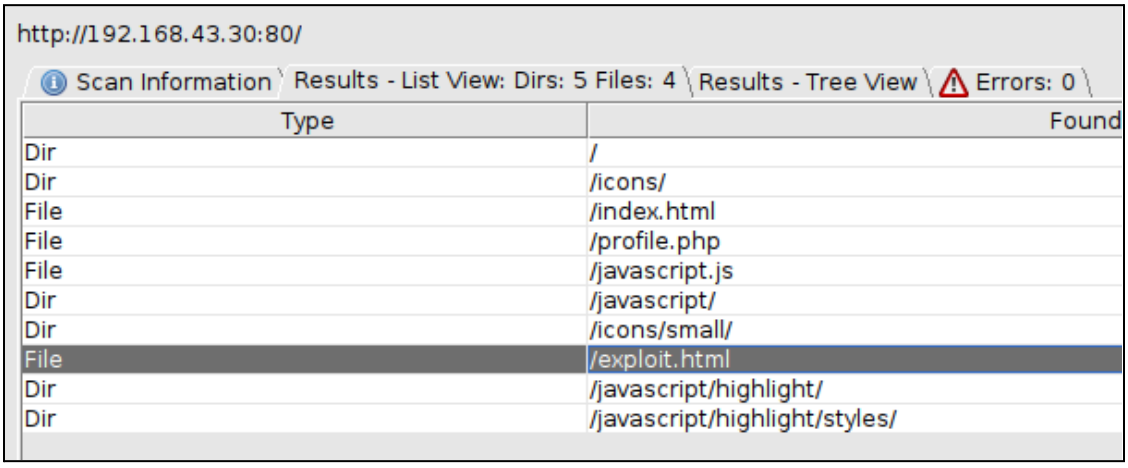
Obtener la versión de los servicios que se ejecutan en todos los puertos abiertos.



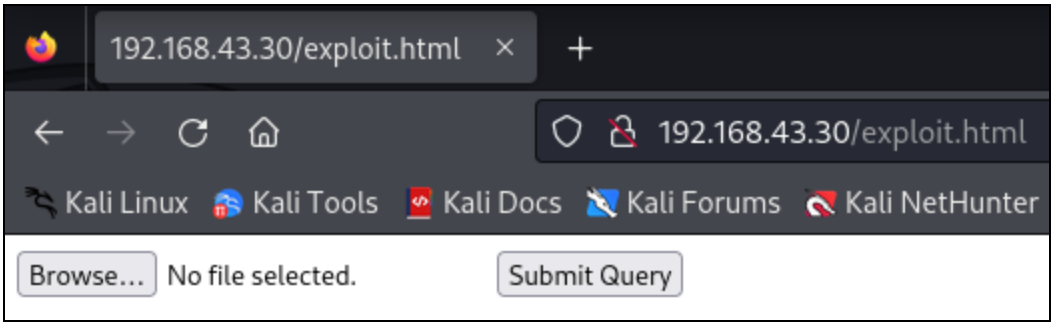
Acceder a la web de la máquina vulnerable escribiendo su ip en el firefox de Kali Linux.



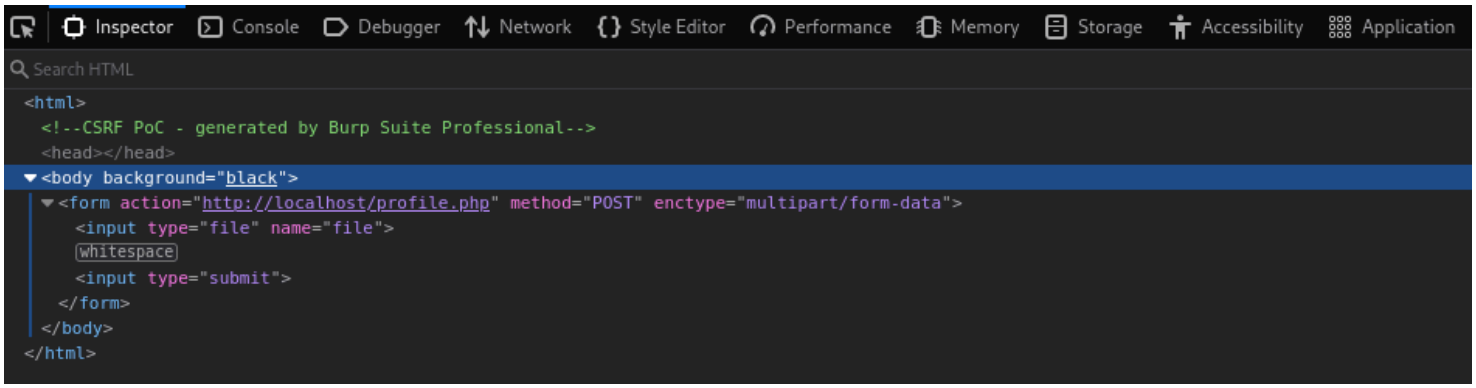
Ejecutar dirbuster en Kali Linux y obtener todos los ficheros con las extensiones que vemos en la imagen y los directorios mediante un diccionario que contiene una lista sobre los ficheros y directorios más usados en cualquier máquina.



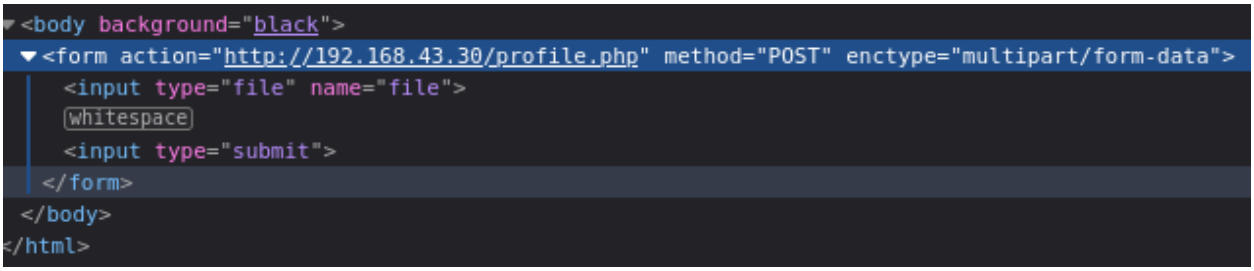
Cuando obtenemos una lista sobre todos los ficheros y directorios dentro de la máquina. Nos fijamos en el fichero “exploit.html”.



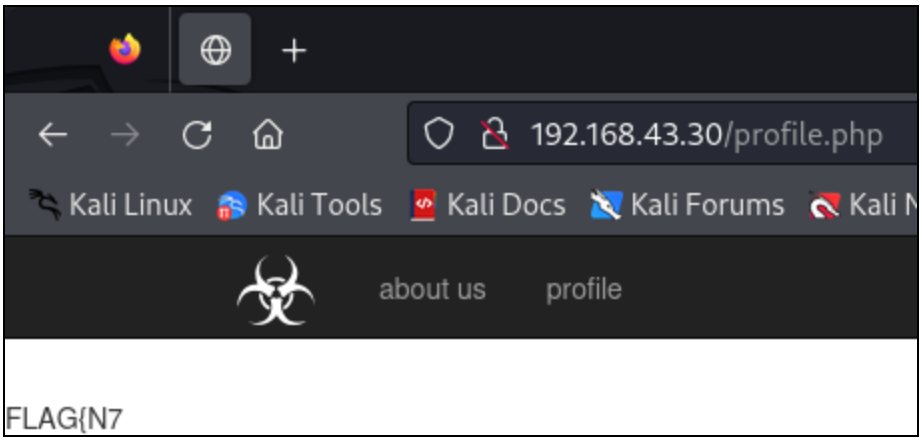
Accedemos al fichero “exploit.html” mediante el navegador.



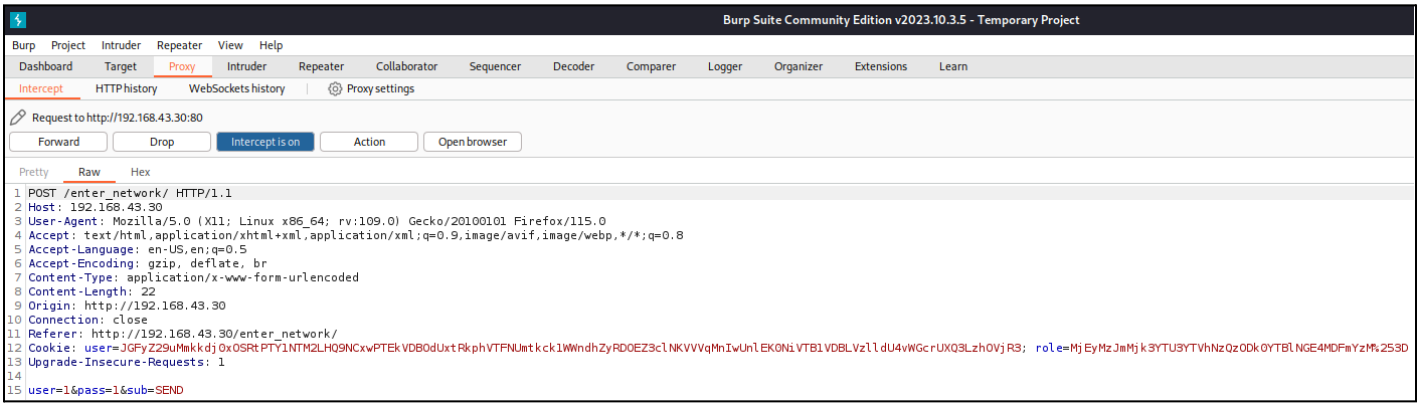
Y observamos el código html.



Sale un error y cambiamos localhost por la ip de la máquina vulnerable.
Hacer click en el botón “Submit Query” que están en el archivo ‘exploit.html’



Obtener la flag a partir del fichero “profile.php”



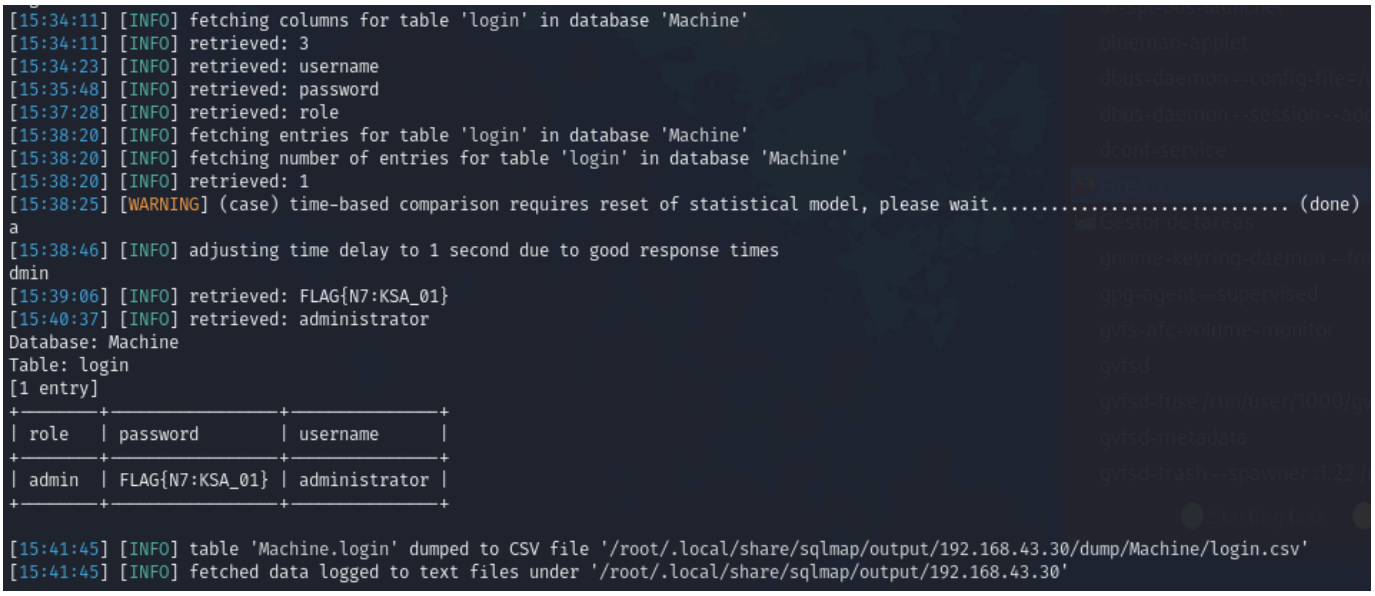
Usar el Burp Suite para analizar y registrar el tráfico de navegación en una página web. Y obtenemos los datos de respuesta del servidor, para poder realizar ataques en la página de la máquina vulnerable.

Ahora podemos realizar ‘SQL Injection’ a la página y obtenemos todas las bases de datos disponibles.

Obtenemos todas las bases de datos.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sqlmap -r /home/kali/Desktop/data.txt -D Machine --dump
```

Ahora tenemos que buscar todas las tablas que hay dentro de la base de datos Machine.



Y obtenemos el usuario administrador y la contraseña que contiene la flag.
FLAG{N7:KSA_01}