

Vamos a hackear un ppts máquina de nivel "Medium" por el valor de un punto. Lo primero que debemos hacer es, además de levantar el Kali y Web Machine (N7), dejar las máquinas en Host Only, a partir de aquí podremos hacer la práctica.

1. Abriremos el Kali y con Nmap descubriremos la IP de Web Machine (N7) utilizando el comando `nmap -sN -p- 192.168.56.0/24` y podremos ver que Web Machine (N7) tiene la IP 192.168.56.106

```
Currently scanning: 192.168.91.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120


| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------------|-------------------|-------|-----|------------------------|
| 192.168.56.100 | 08:00:27:cf:32:52 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.56.106 | 08:00:27:ed:bd:c7 | 1     | 60  | PCS Systemtechnik GmbH |


# nmap -sC -sV 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 11:10 EST
Nmap scan report for 192.168.56.100
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:CF:32:52 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.106
Host is up (0.00030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.46 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.46 (Debian)
MAC Address: 08:00:27:ED:BD:C7 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.000050s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

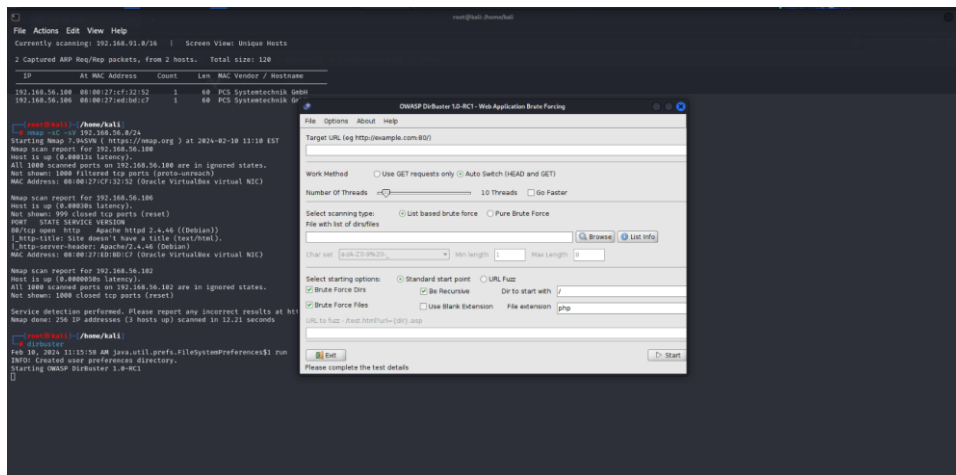
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 12.21 seconds

(root@kali)-[/home/kali]
#
```

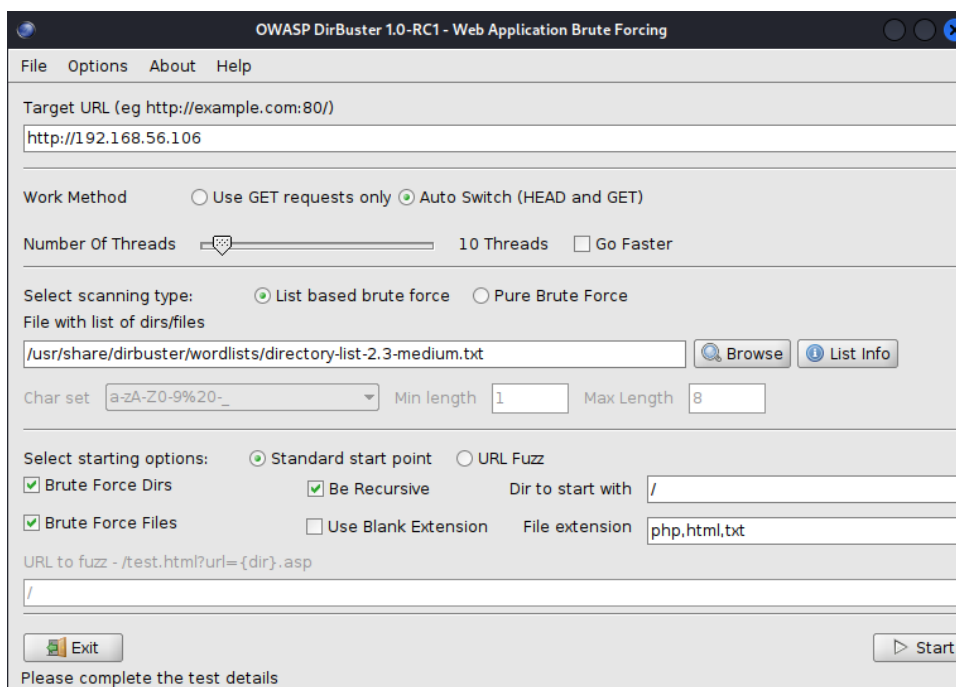
2. Si accedemos a la IP desde el buscador, encontraremos una web



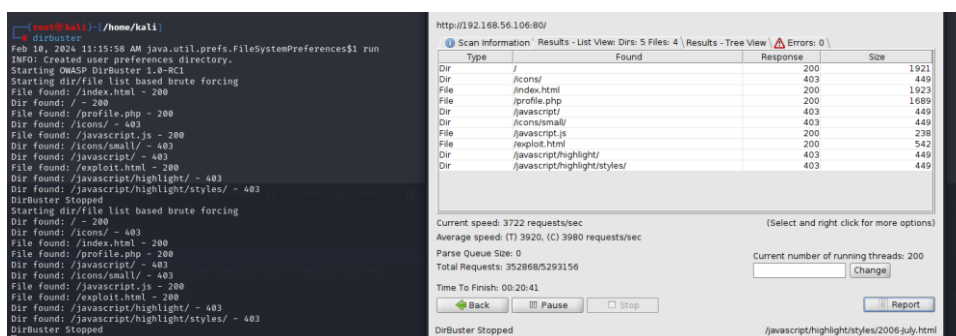
3. Abrimos el dirbuster



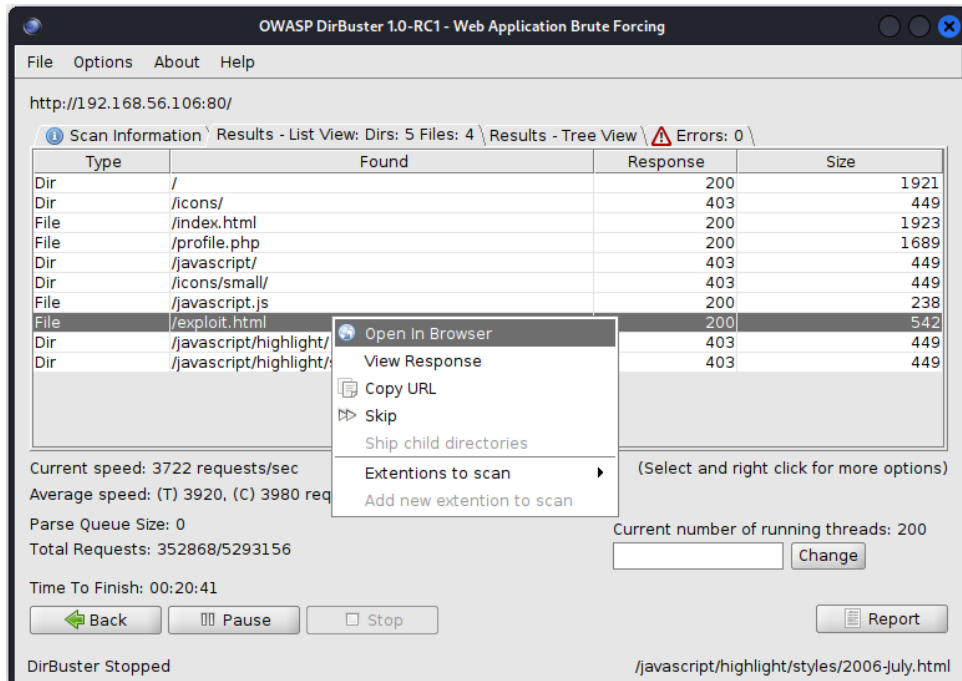
4. Pondremos los siguientes parámetros y le daremos a start



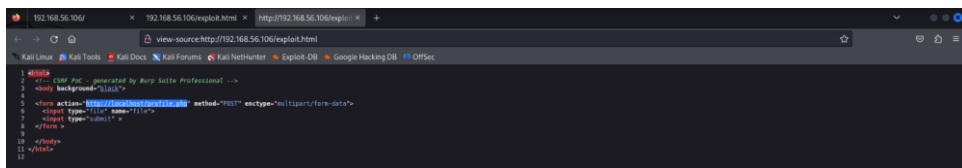
5. Habremos encontrado los siguientes archivos



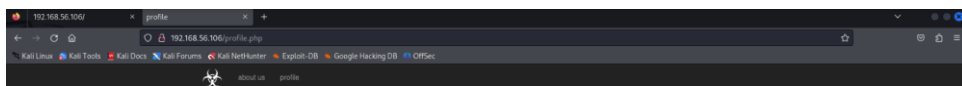
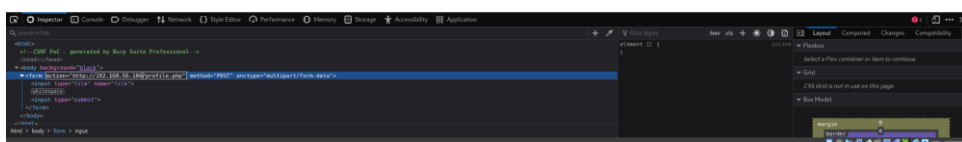
6. Abriremos el archivo exploit.html



7. Si vemos el código fuente veremos que hace referencia a otro fichero

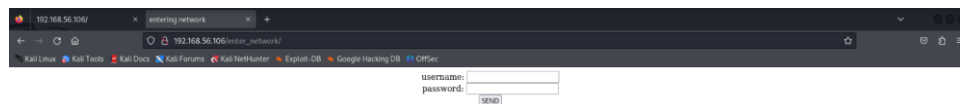
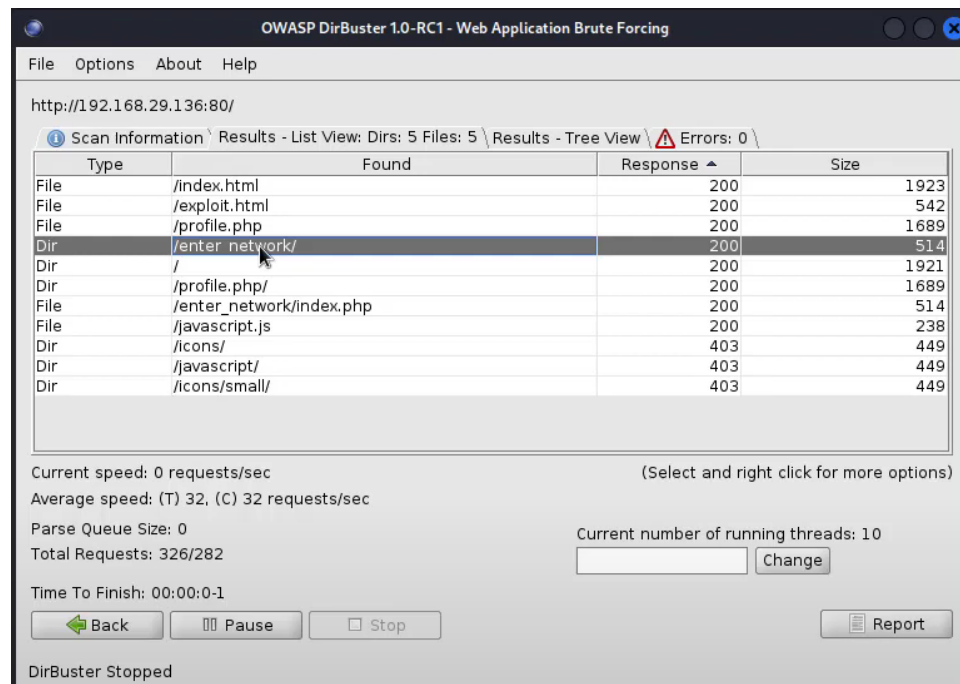


8. Desde el inspector, cambiaremos el localhost por la IP de la máquina y veremos una flag

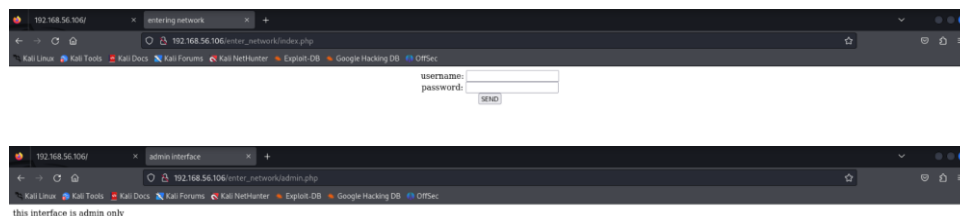


FLAG: 07

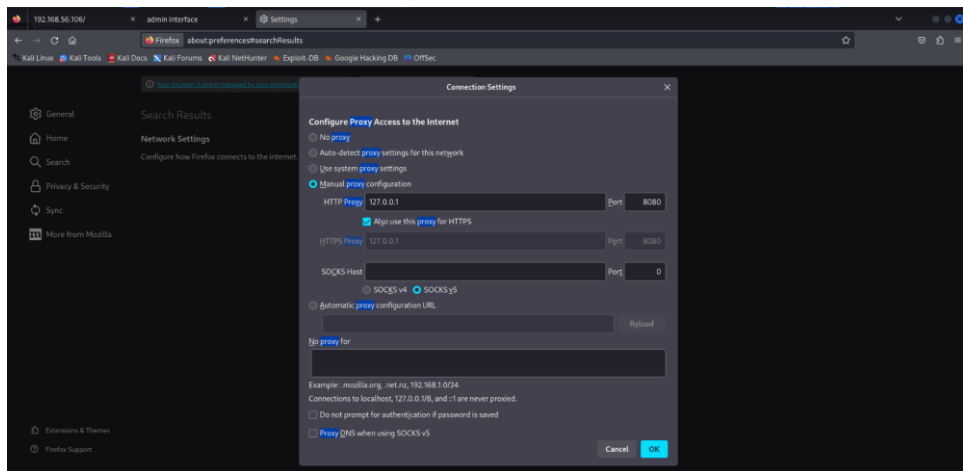
9. Desde el dirbuster podremos ver también enter_network, contiene un formulario



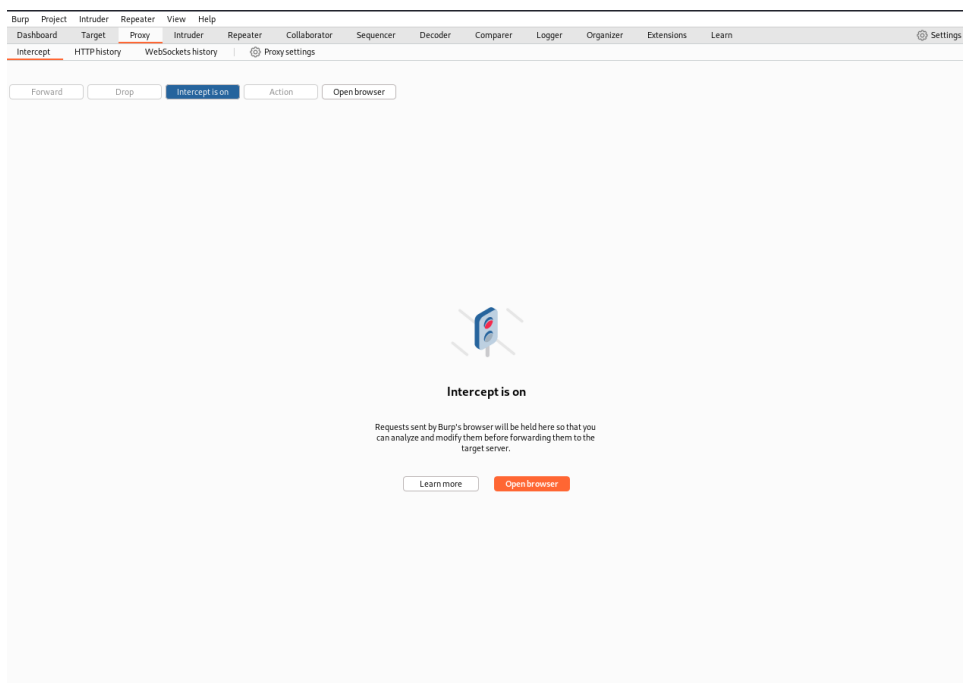
10. Veremos que también hay un par de ficheros, index.php y admin.php, sin embargo, el segundo está bloqueado



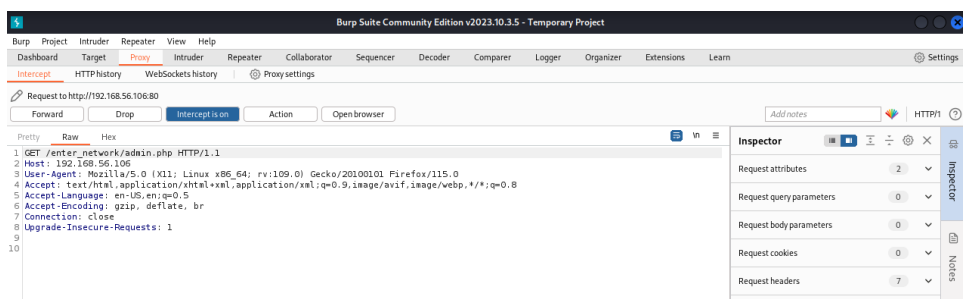
11. Para acceder al fichero de admin.php usaremos el burpsuite. Primero debemos acceder al proxy de firefox y dejarlo en local



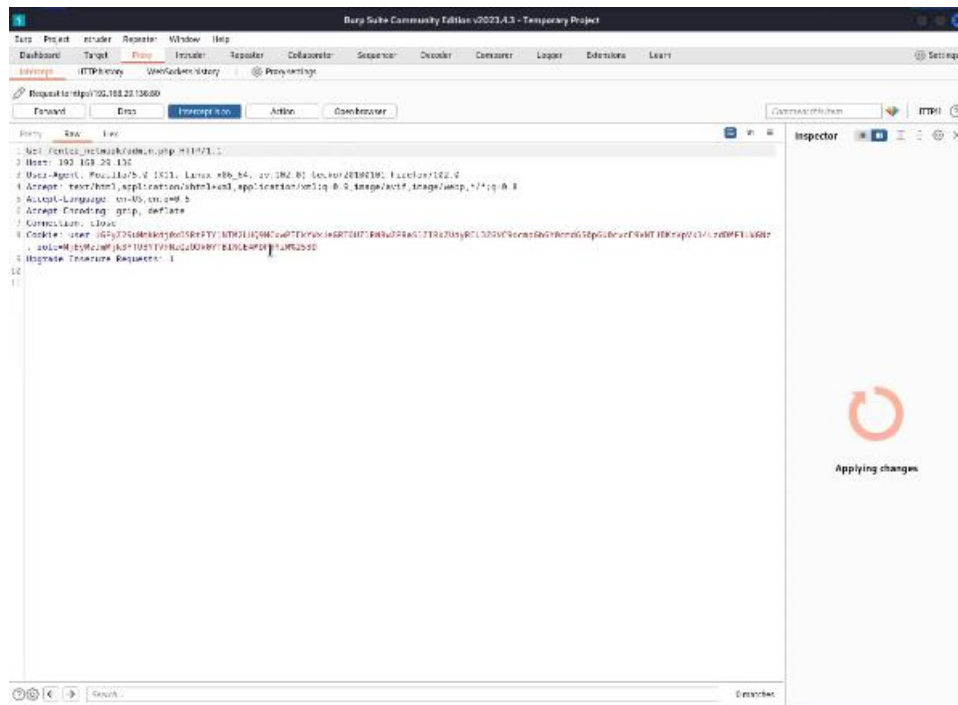
12. Ponemos el intercept en On



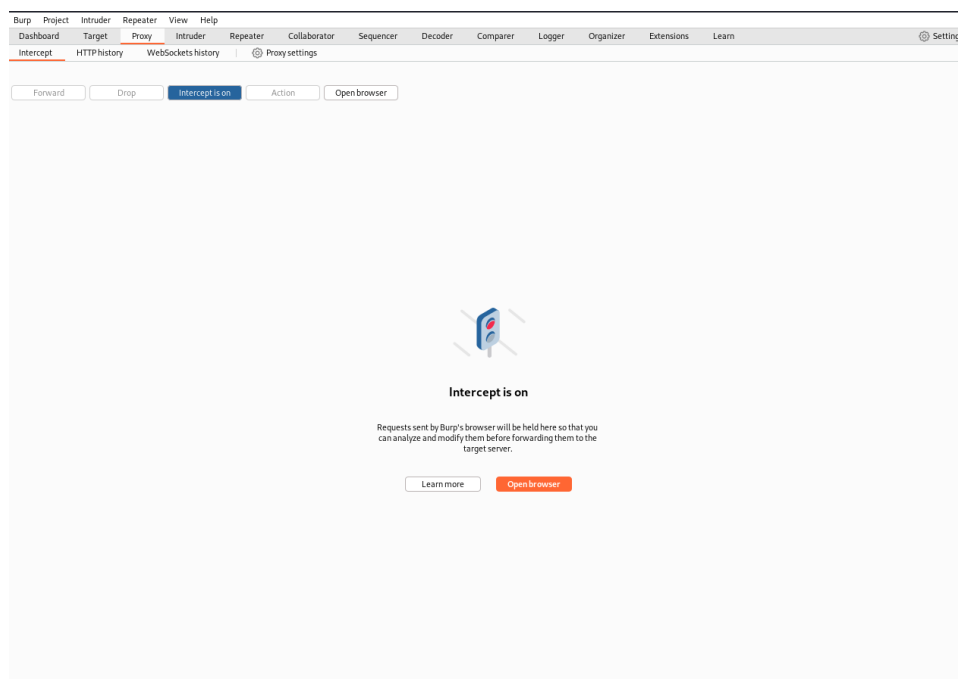
13. Recargamos la página de admin para que la pille el burpsuite



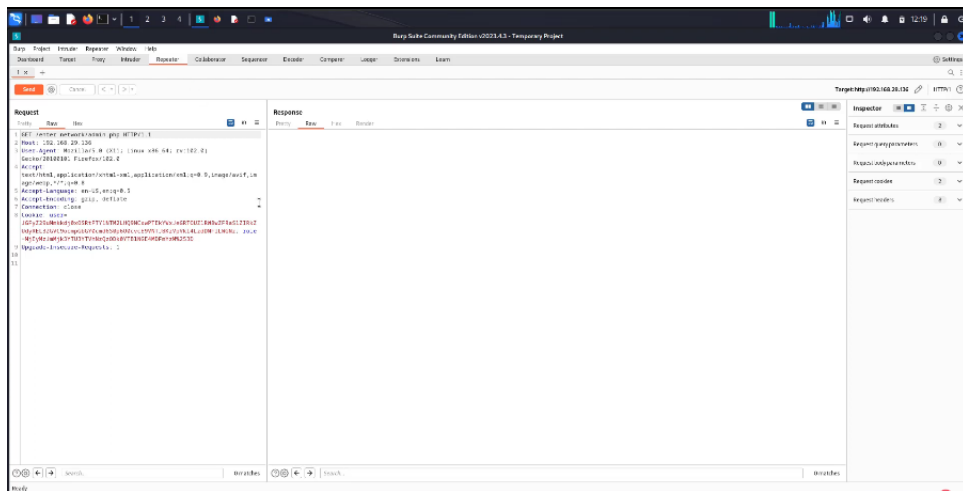
14. La mandamos al Repeater



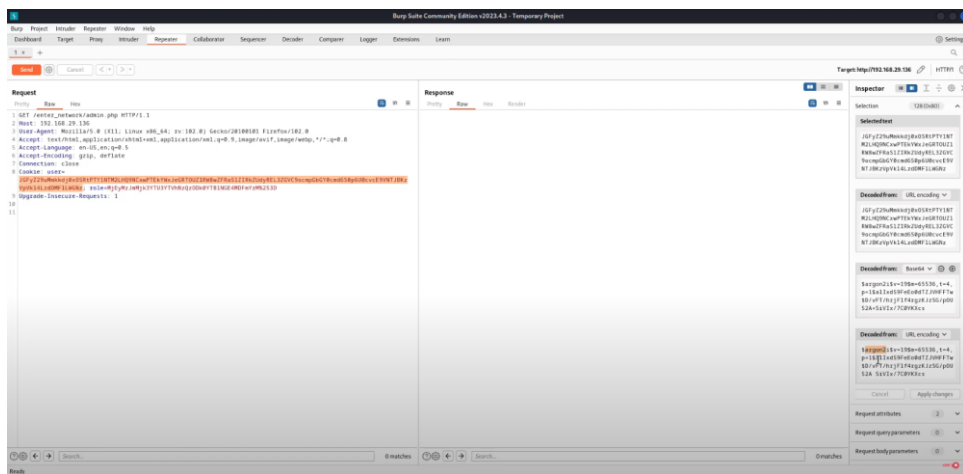
15. Apagamos el Intercept



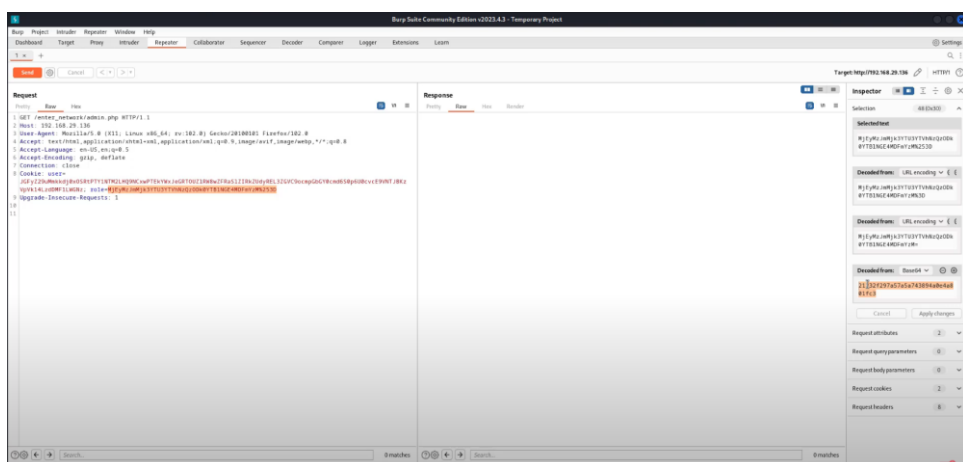
16. Abrimos el repeater



17. Si profundizamos en las cookies, veremos que están cifradas con argon2



18. Vamos a abrir en descifrador y a coger el mensaje descifrado de base 64



19. Usamos el descifrador

Plain Text Input

21232f297a57a5a743894a0e4a801fc3

Salt

rpVFeIZU5IWEXH19

Parallelism Factor

1

Memory Cost

16

Iterations

2

Hash Length

16

Argon2l

Argon2d

Argon2id

How to Choose the Right Parameters for Argon2 »

Output in HEX Form

COPY

e1c7d75b0b53508c94618aa296c9954f

Output in Encoded Form

COPY

\$argon2i\$v=19\$m=16,t=2,p=1\$cnBWRmVsWlU1bFdFWegxOQ\$4cfXWwtTUIyUYyqilsmVTW

GENERATE HASH

RESET FORM

20.Como hemos visto en el apartado anterior, no nos aparece nada coherente. Vamos a cambiar el role por admin y conseguiremos la segunda flag KSA_01

