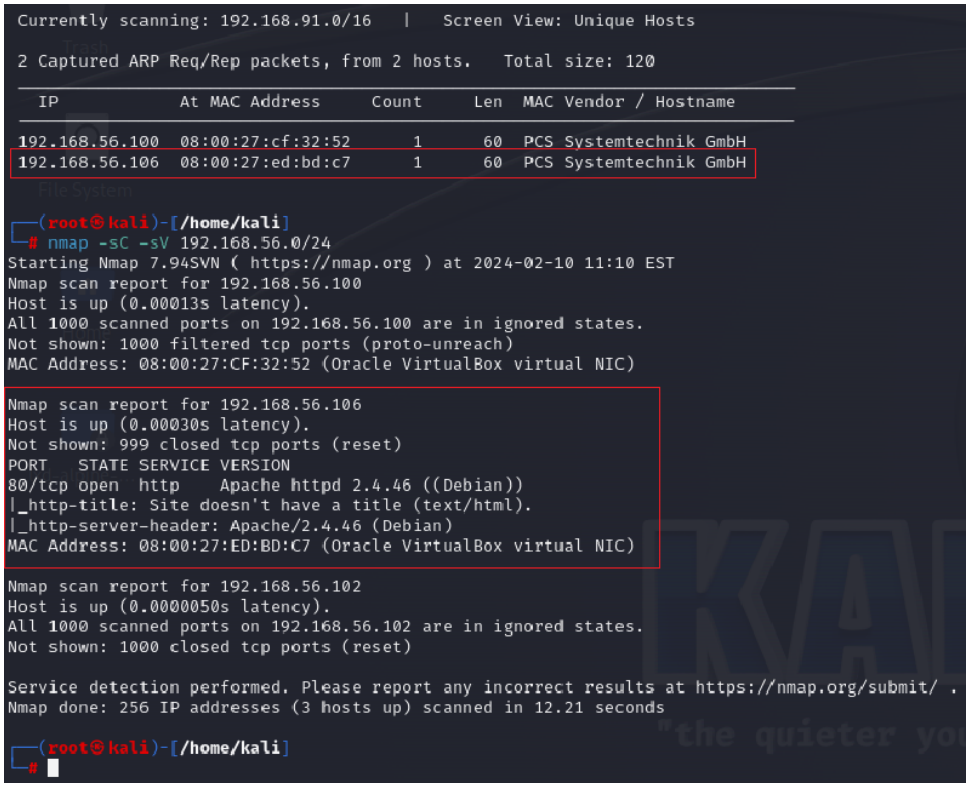
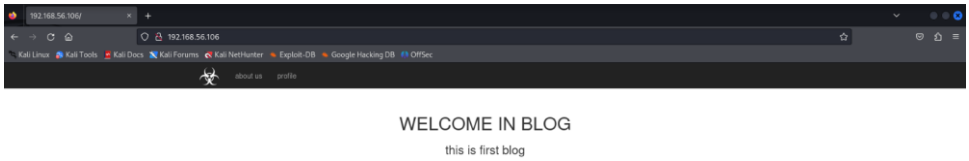
Vamos a hackear unptsa máquina de nivel “Medium” por el valor de un punto. Lo primero que debemos hacer es, además de levantar el Kali y Web Machine (N7), dejar las máquinas en Host Only, a partir de aquí podremos hacer la práctica.

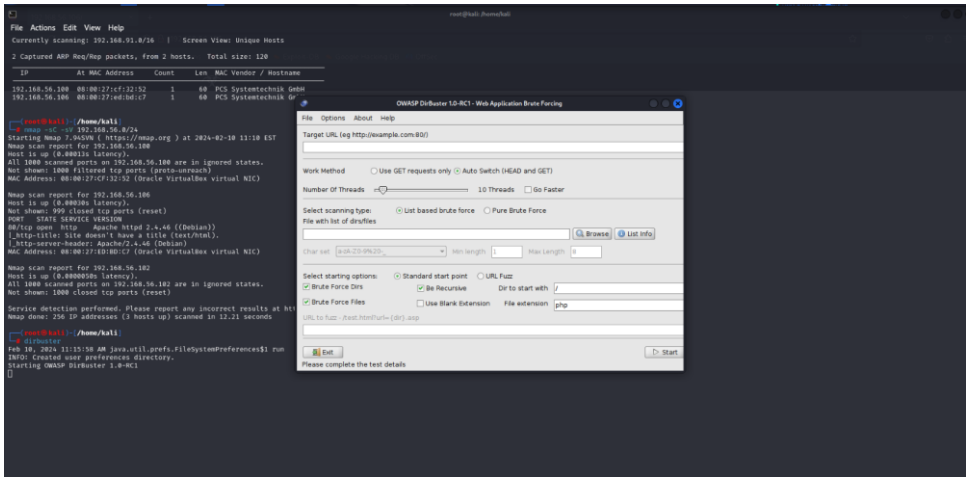
1. Abriremos el Kali y con Nmap descubriremos la IP de Web Machine (N7) utilizando el comando nmap –sN –p- 192.168.56.0/24y podremos ver que Web Machine (N7) tiene la IP 192.168.56.106



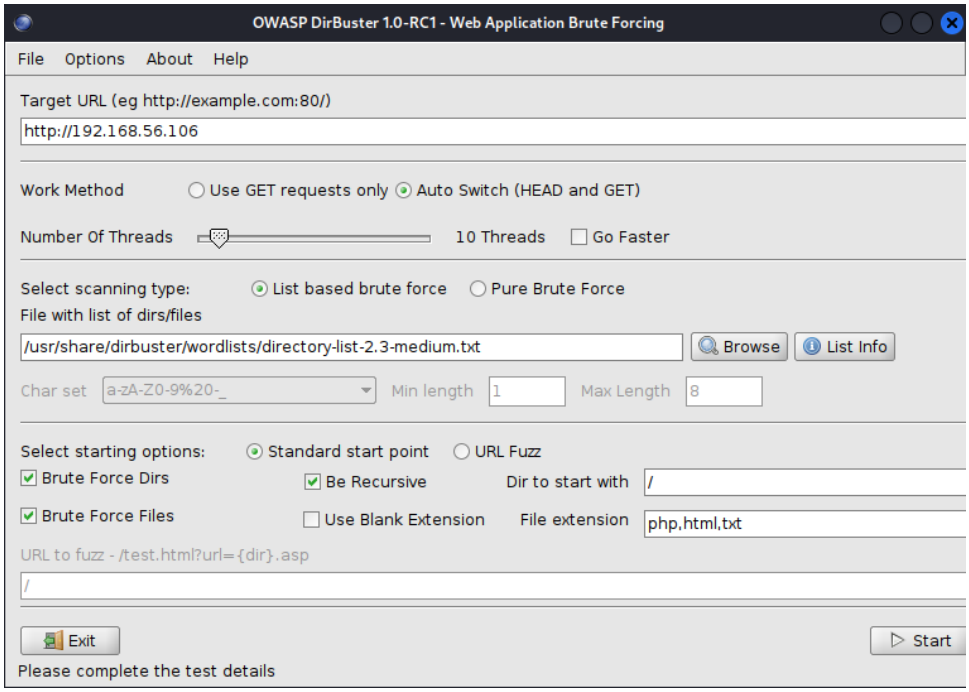
2. Si accedemos a la IP desde el buscador, encontraremos una web



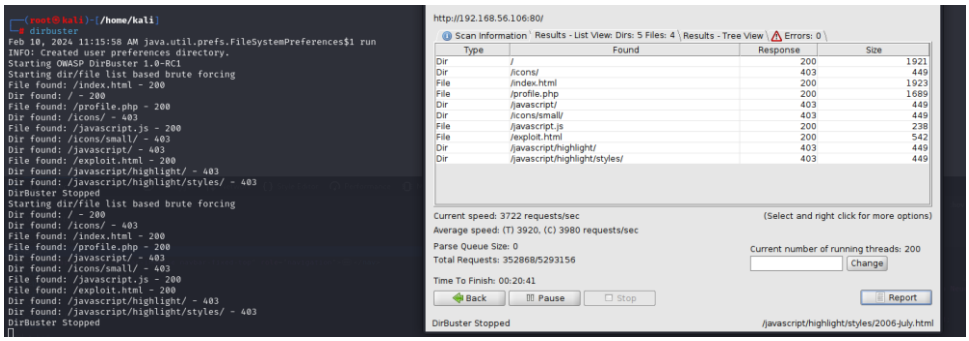
3. Abrimos el dirbuster



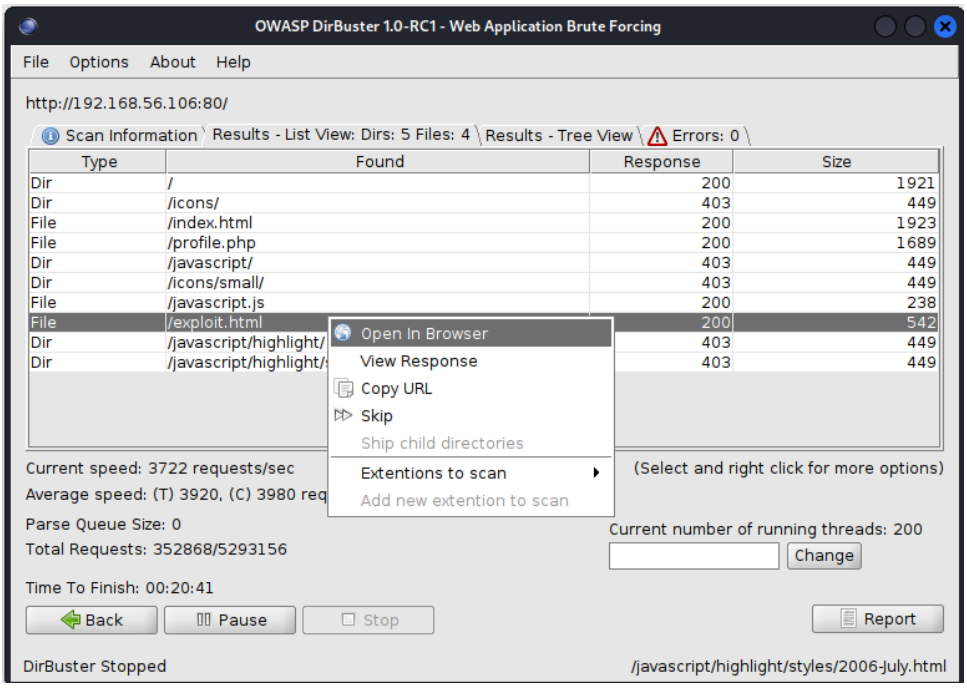
4. Pondremos los siguientes parámetros y le daremos a start



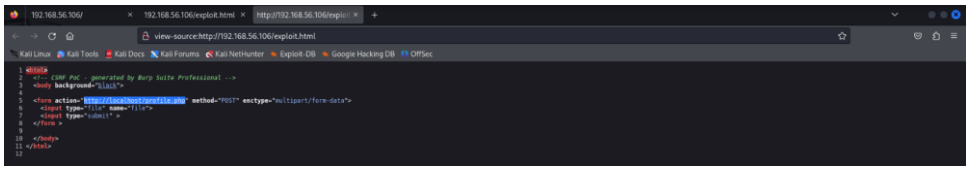
5. Habremos encontrado los siguientes archivos



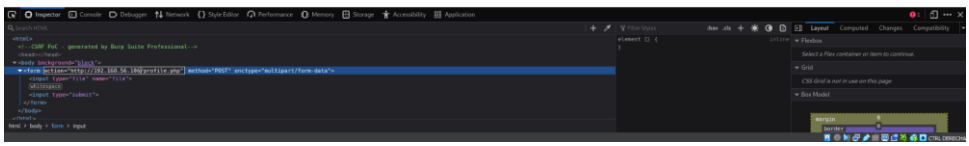
6. Abriremos el archivo exploit.html



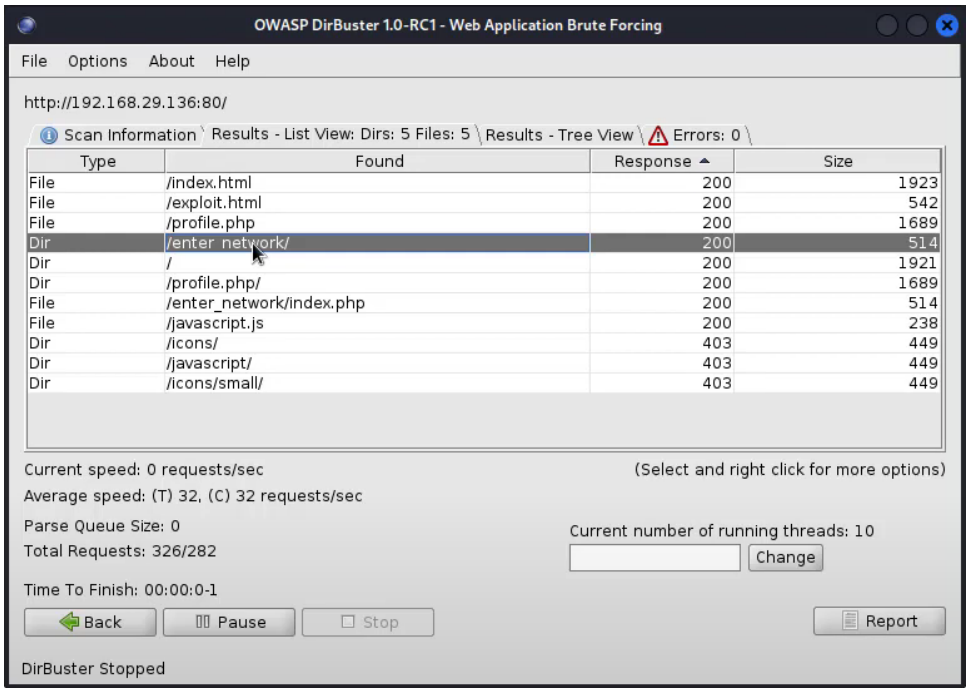
7. Si vemos el código fuente veremos que hace referencia a otro fichero

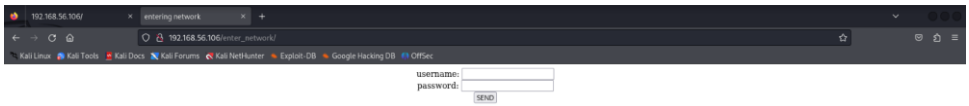


8. Desde el inspector, cambiaremos el localhost por la IP de la máquina y veremos una flag

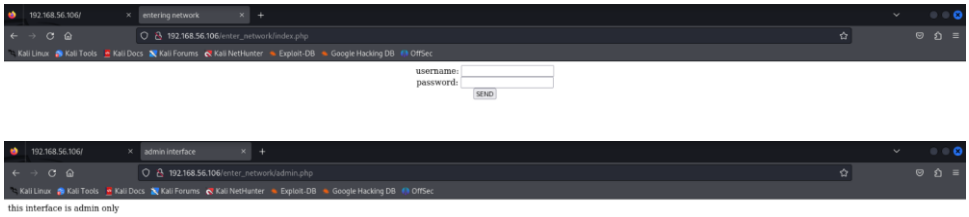


9. Desde el dirbuster podremos ver también enter_network, contiene un formulario

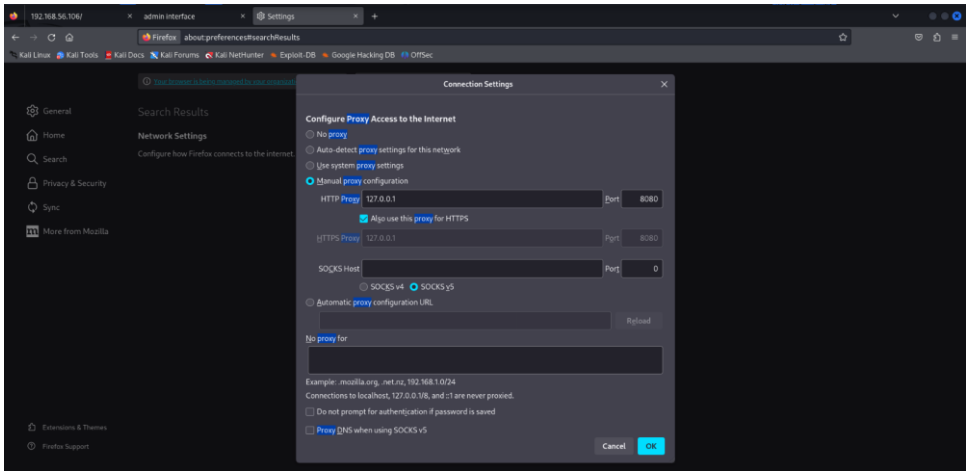




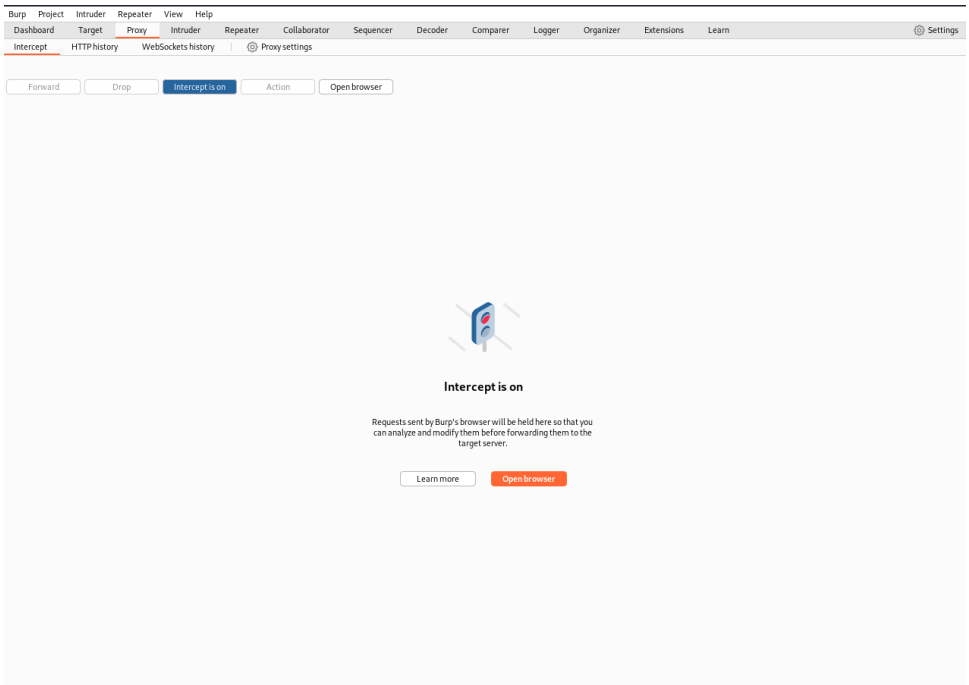
10. Veremos que también hay un par de ficheros, index.php y admin.php, sin embargo, el segundo está bloqueado



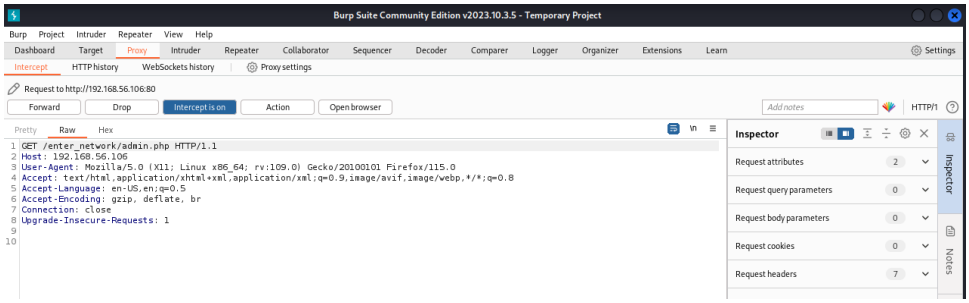
11. Para acceder al fichero de admin.php usaremos el burpsuite. Primero debemos acceder al proxy de firefox y dejarlo en local



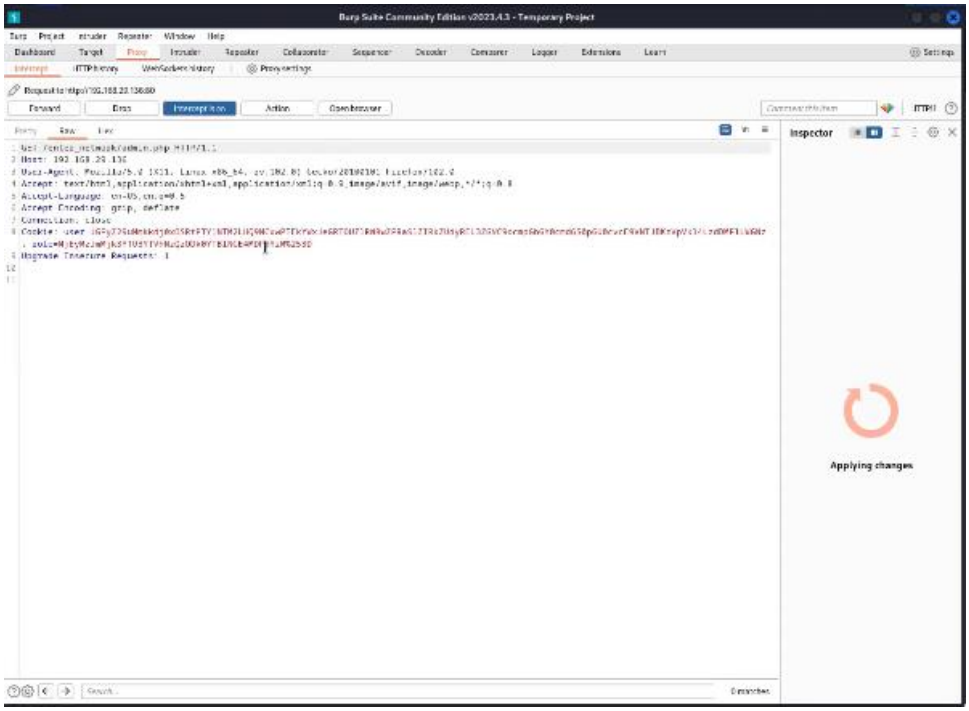
12. Ponemos el intercept en On



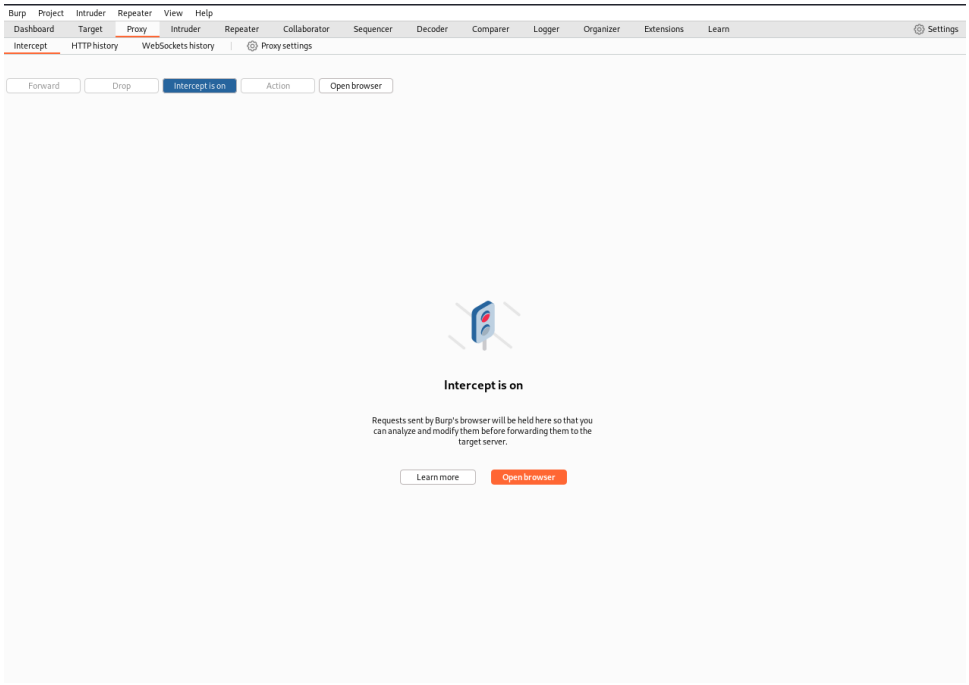
13. Recargamos la página de admin para que la pille el burpsuite



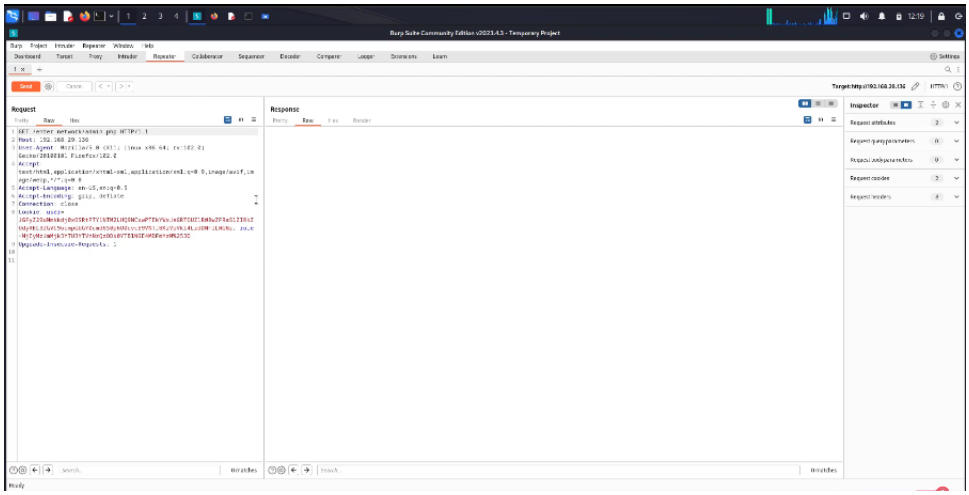
14. La mandamos al Repeater



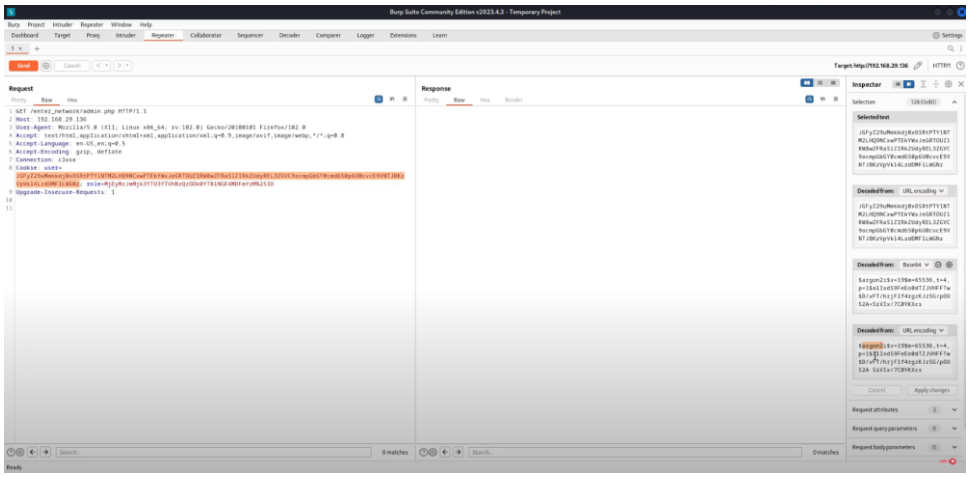
15. Apagamos el Intercept



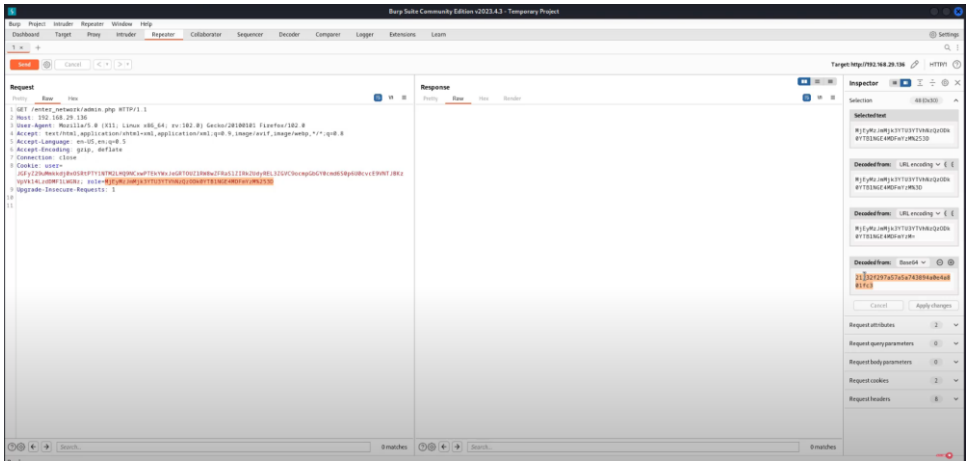
16. Abrimos el repeater



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



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



19. Usamos el desencriptador

Plain Text Input

21232f297a57a5a743894a0e4a801fc3

Salt	Parallelism Factor	Memory Cost	Iterations	Hash Length
rpVFelZU5lWEXH19	1	16	2	16

Argon2i | 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