Vulnerability Assessment and Penetration Techniques

**Practical – 9**

**Aim: Create any wordlist using crunch and use the same wordlist to perform a dictionary attack using Hydra on DVWA and Mutillidae**.

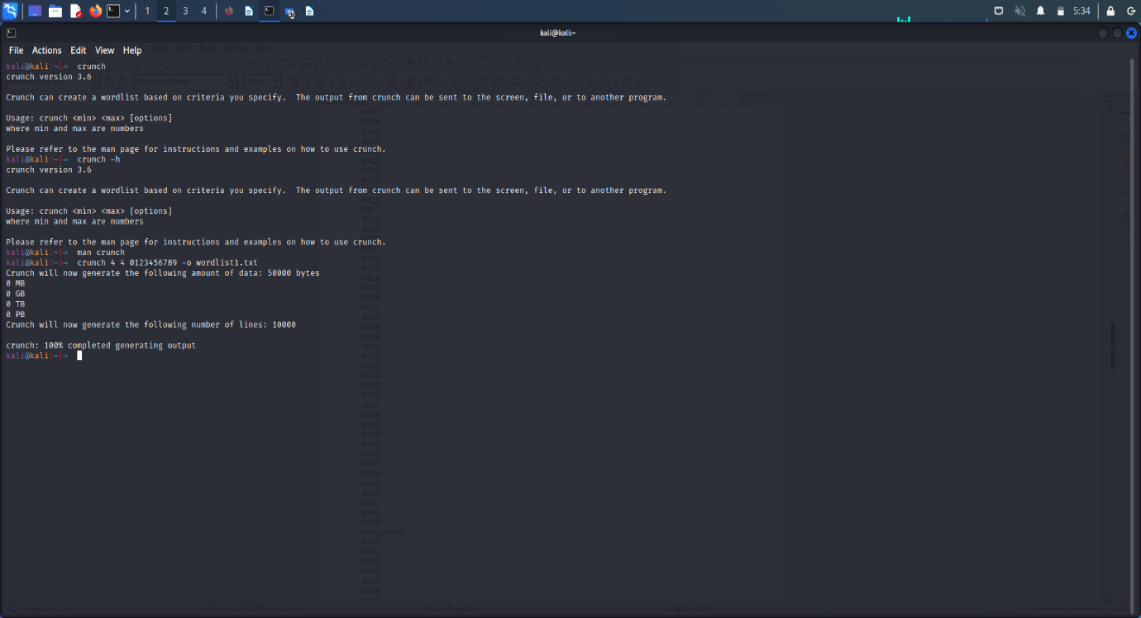
**Requirement:** Metasploitable 2,Kali Linux, BurpSuite

**Procedure:**

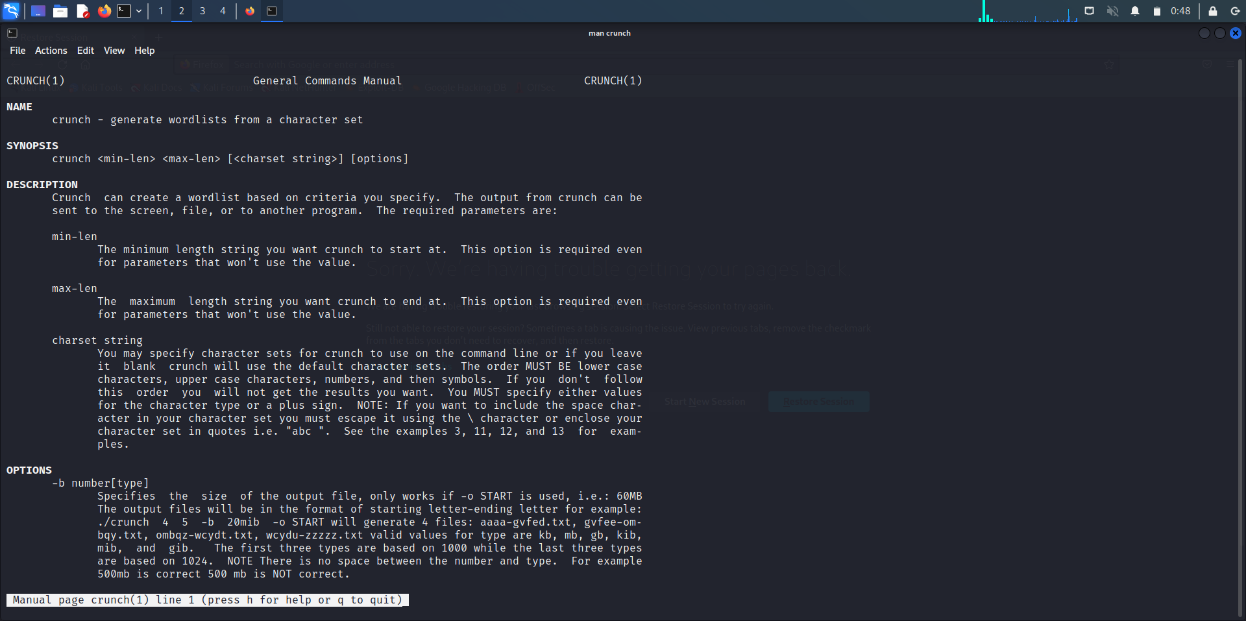
1. Open Kali Linux.
2. Open Metasploitable. Find its IP address.

**TO CREATE A WORDLIST WITH CRUNCH:**

1. Type crunch to check whether crunch is installed in our host.



1. To get various options we open the manual page: man crunch



1. To create a wordlist using crunch we use the following syntax:

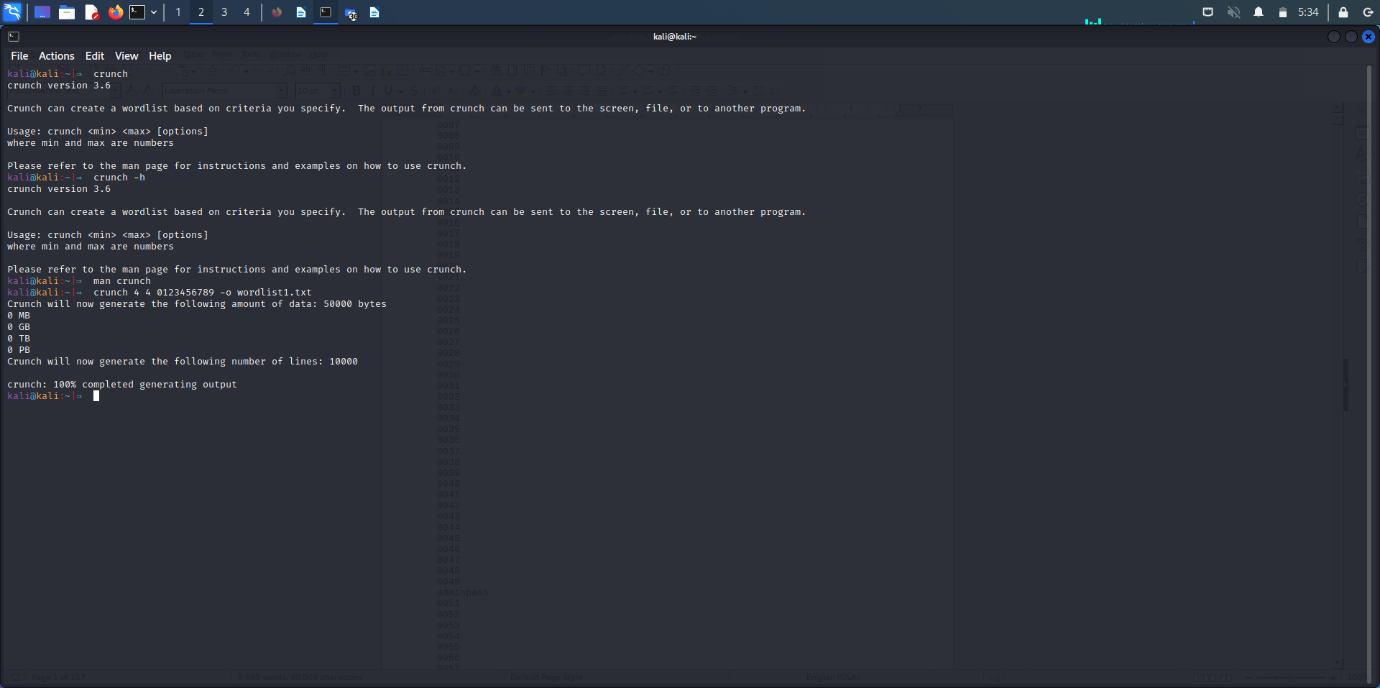
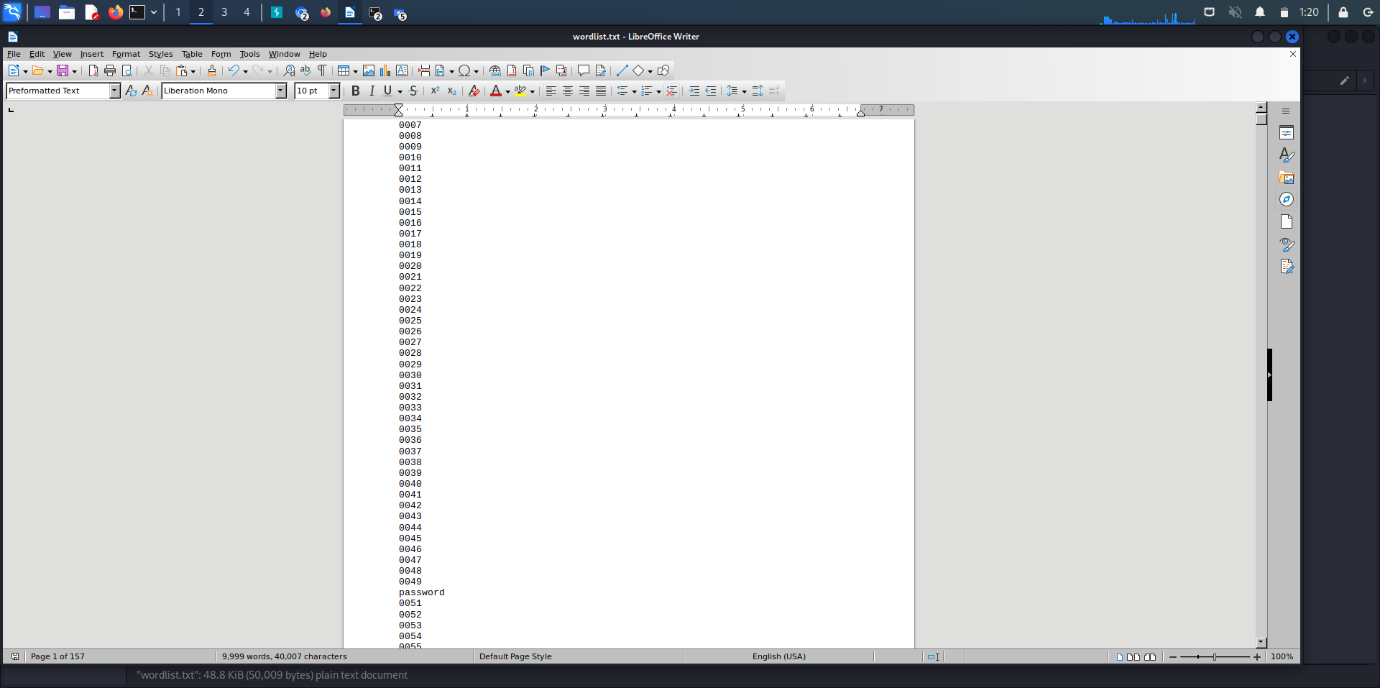
Crunch <min\_len> <max\_len> [<charset string>] [options]

1. To create a wordlist with minimum length – 5 and maximum length 8, we enter the following command:

-o: the file in which the output will be written.

a-z: represents the character set.

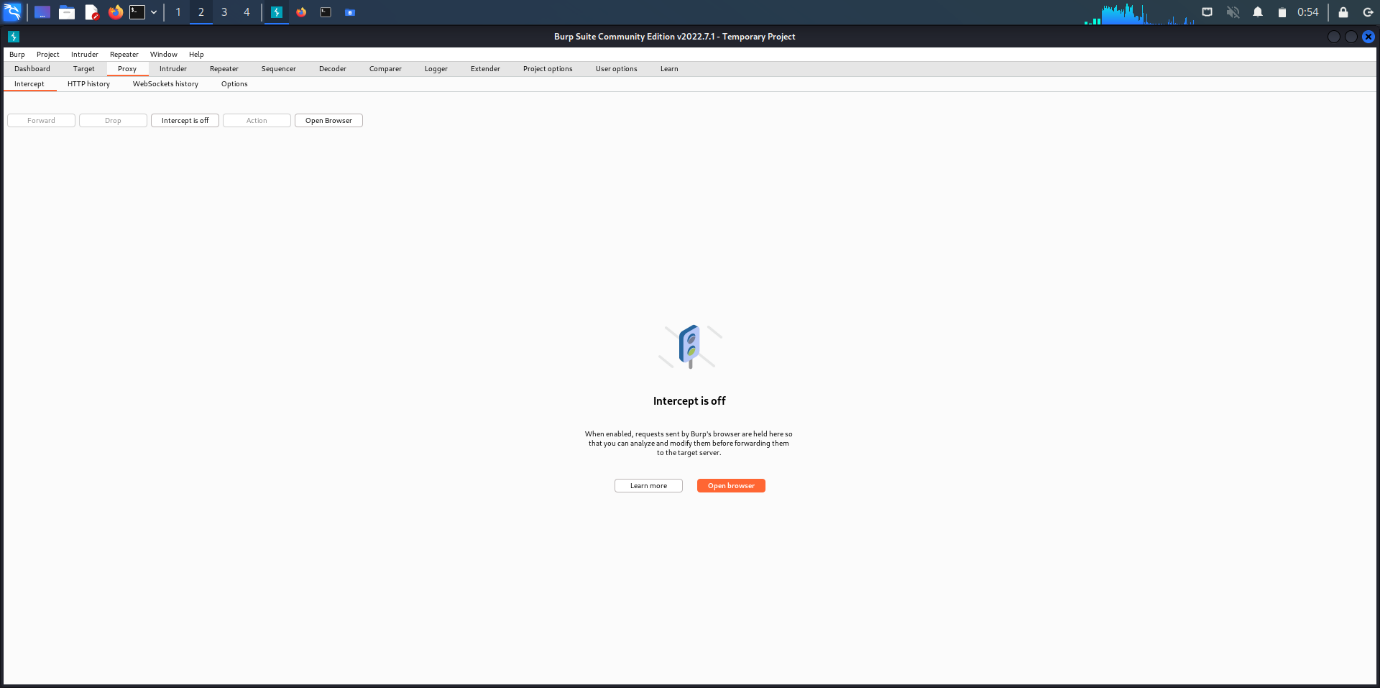
Use crunch command- crunch 4 4 0123456789 -o wordlist1.txt

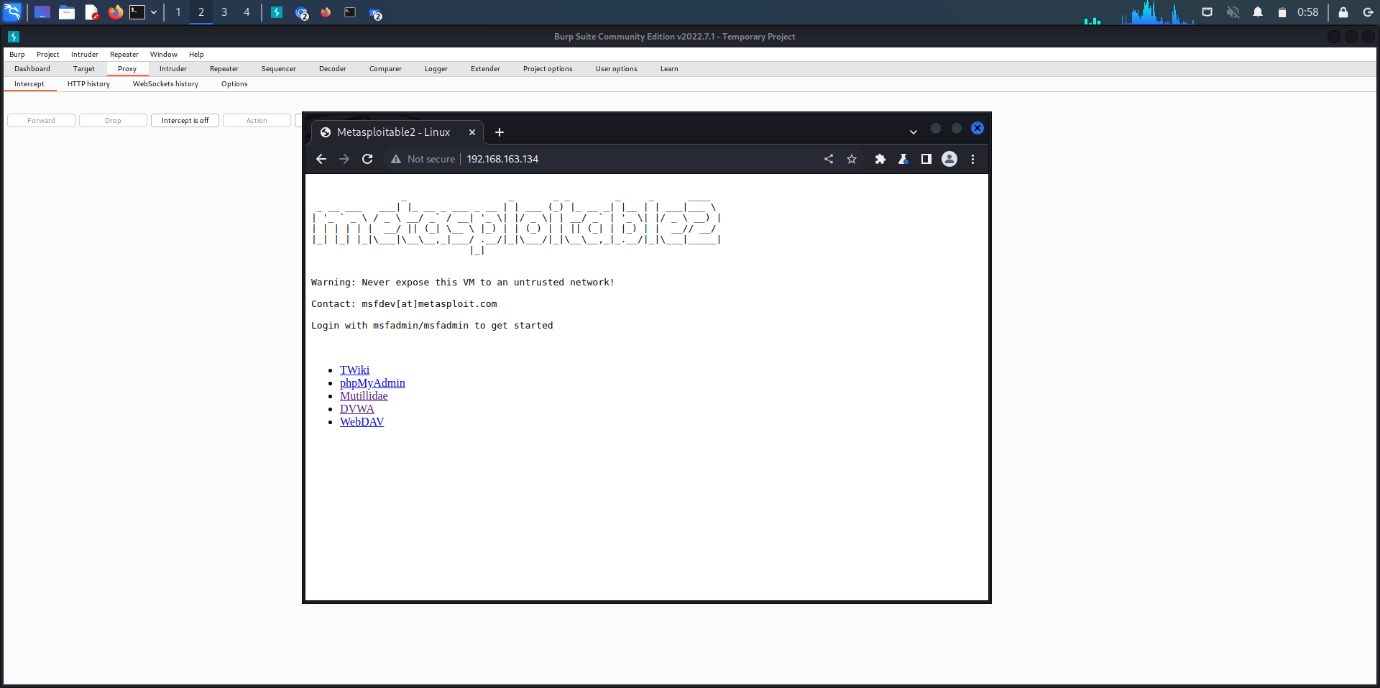
The wordlist is generated, we can confirm this by using ls command in the command prompt.

**TO PERFORM DICTIONARY ATTACK ON DVWA USING HYDRA:**

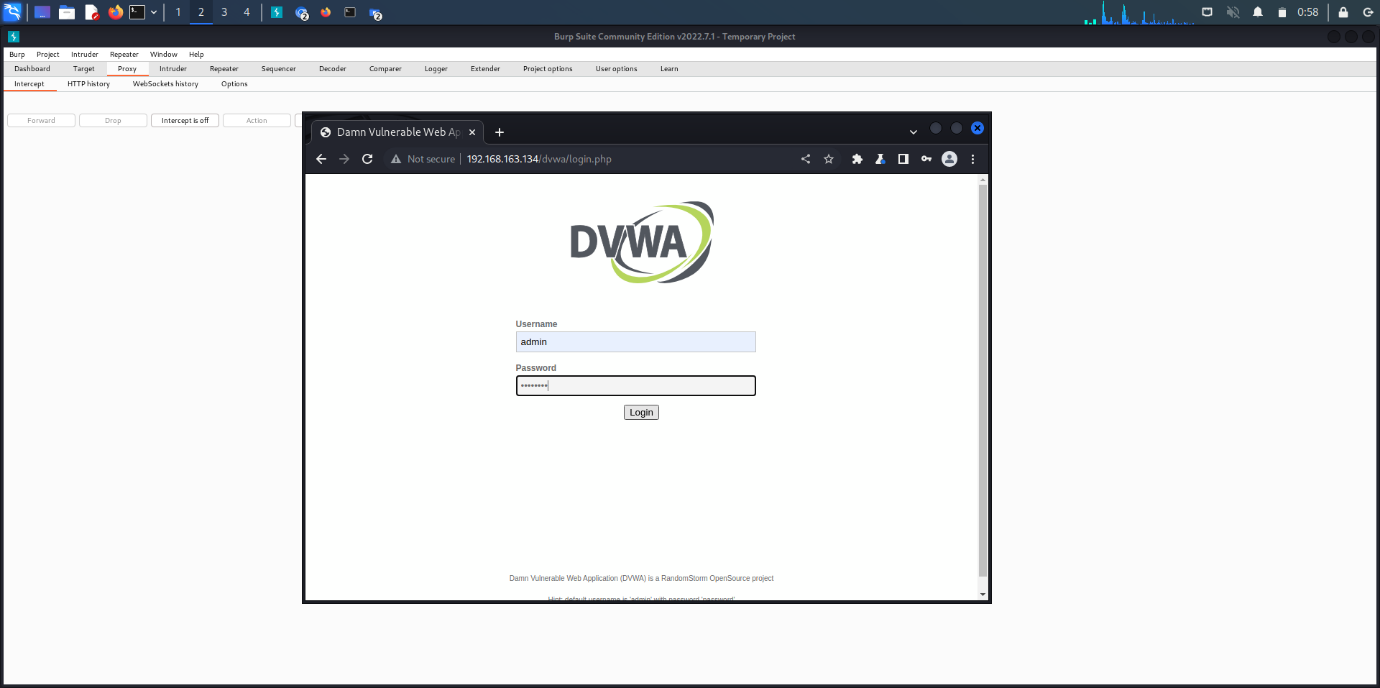
1. Open Burp Suite, enter into the proxy tab.



1. Open Burp Suite Browser, enter IP address of Metasploitable into it.

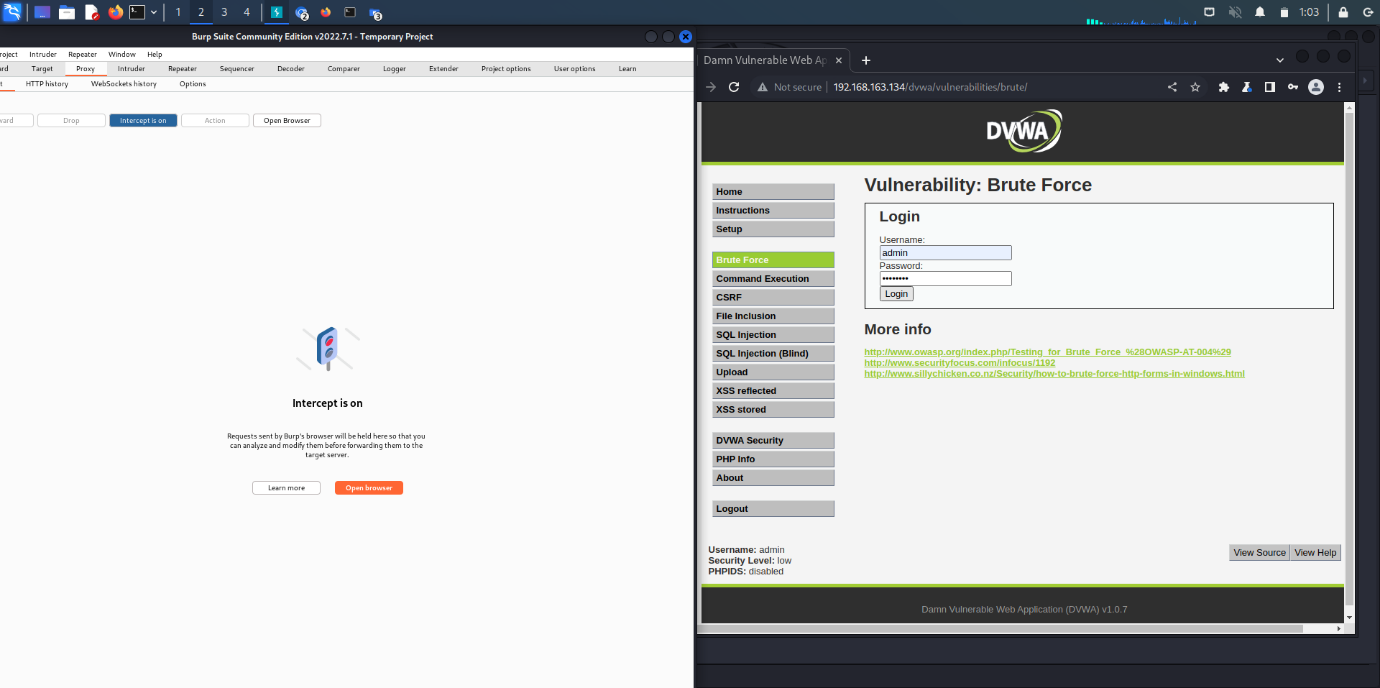


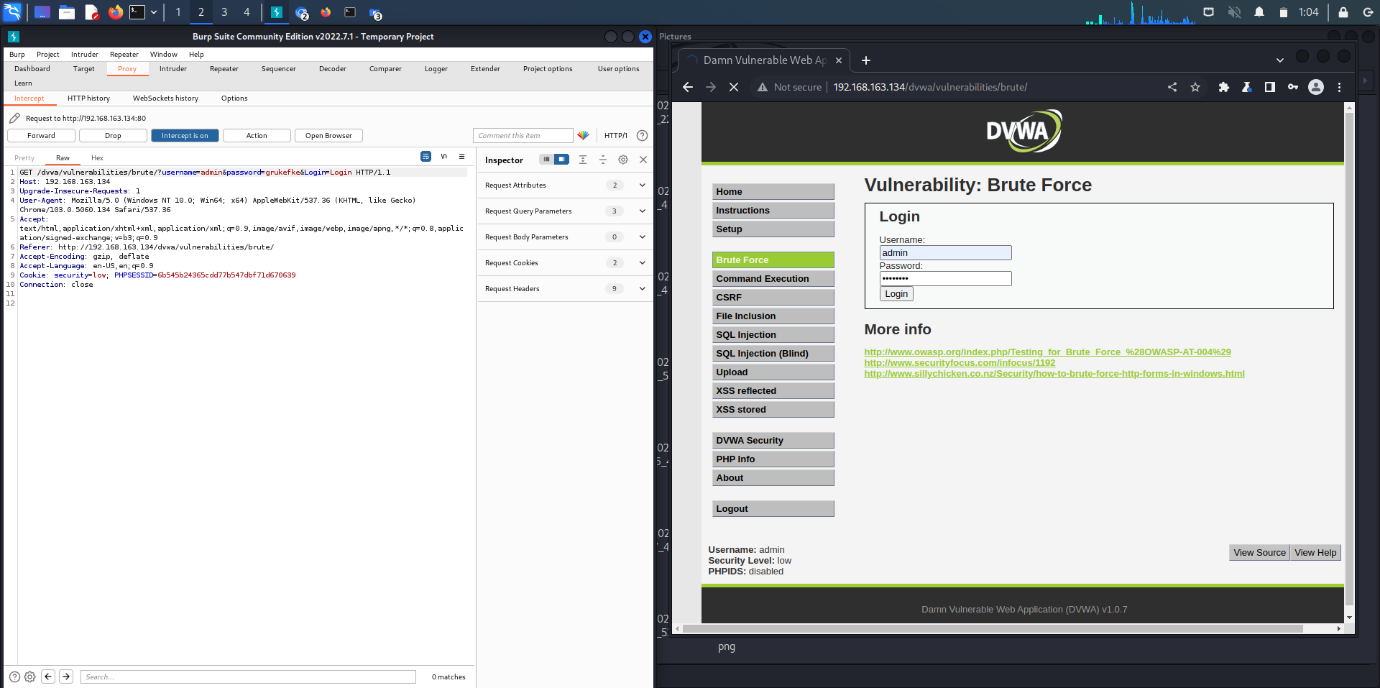
1. Login to DVWA, set the security level to – low.



1. Enter into the Brute Force tab. Enter any name in username and enter any random password.
2. Before hitting Login button, turn the BurpSuite intercept ON. BurpSuite will act as

proxy and catch our request.

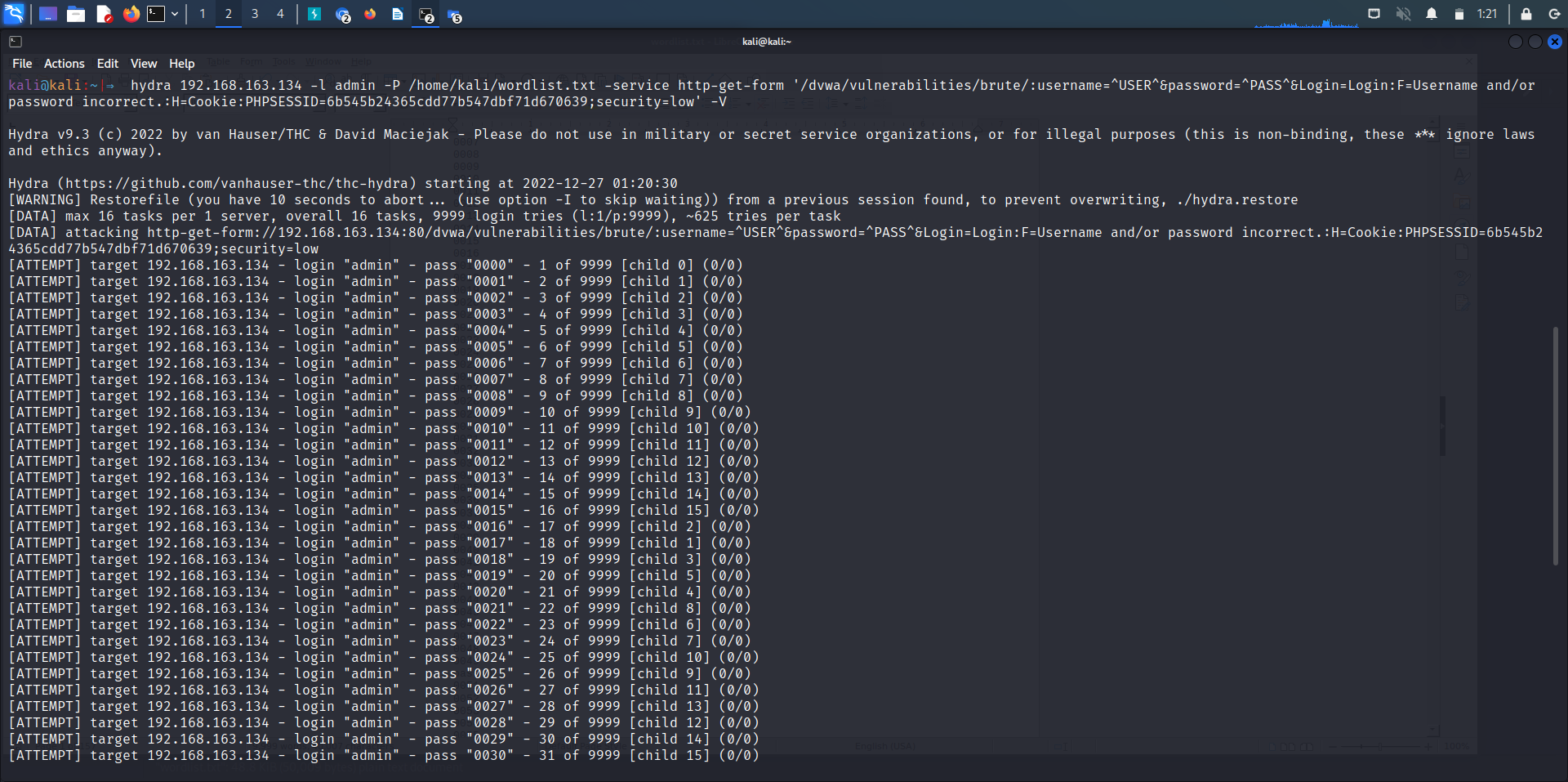


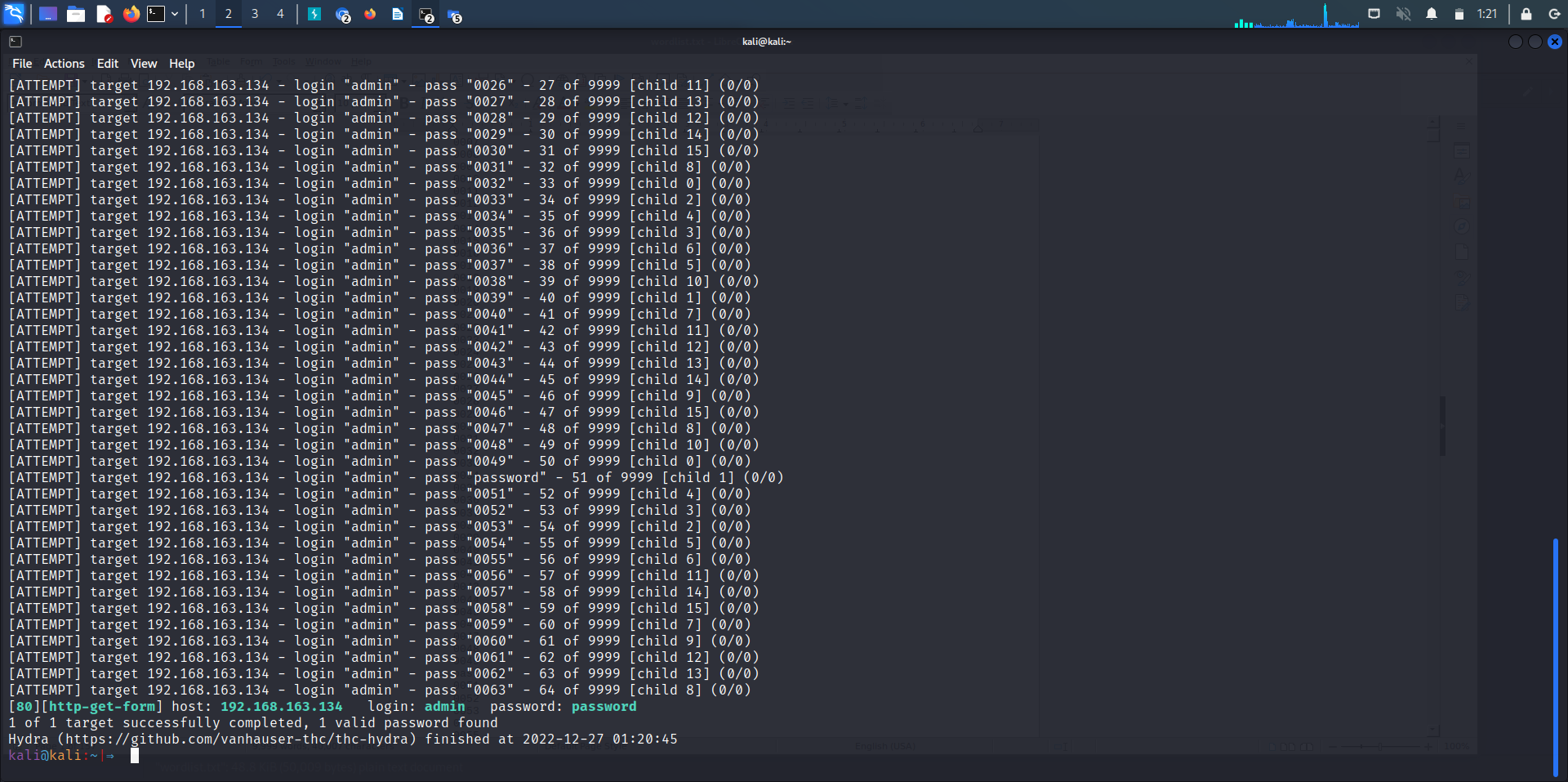


1. Open the command prompt in Kali Linux.
2. To perform dictionary attack using hydra, following command is entered:

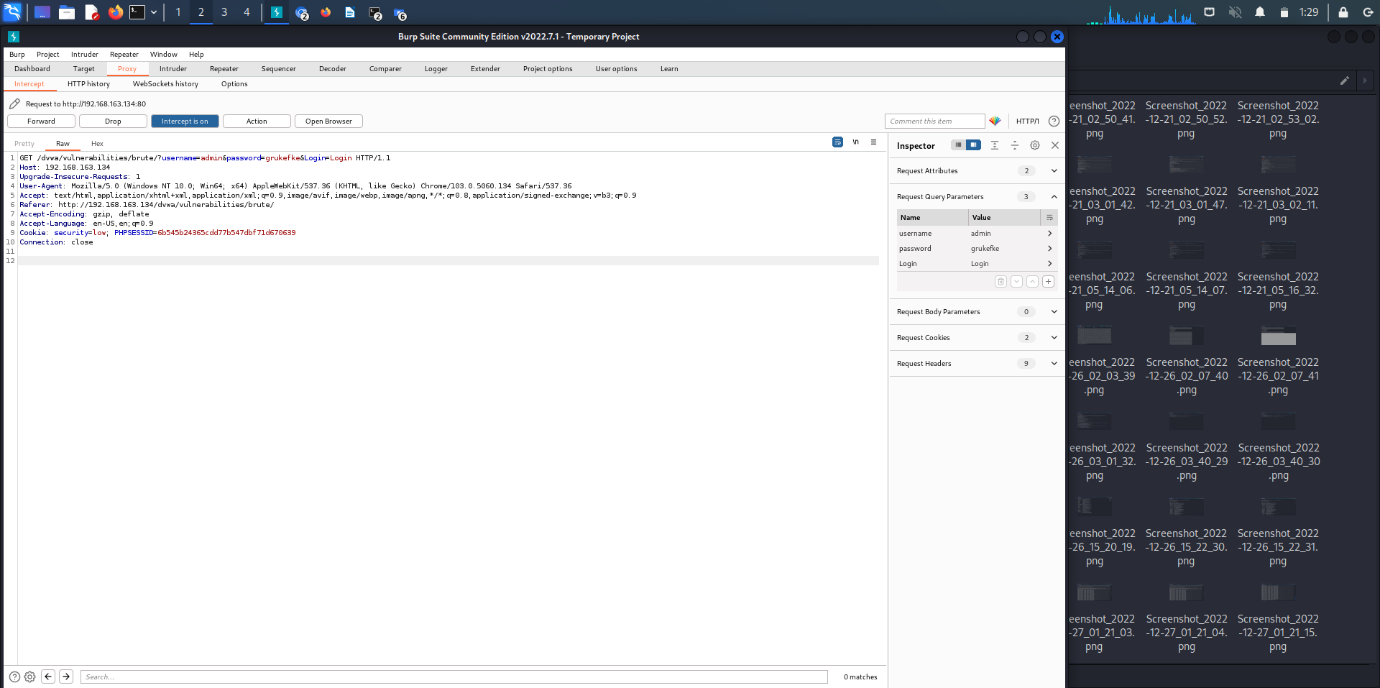
Hydra 192.168.163.134 -l admin -P /home/kali/wordlist.txt -service http-get-form ‘/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect.:H=Cookie:

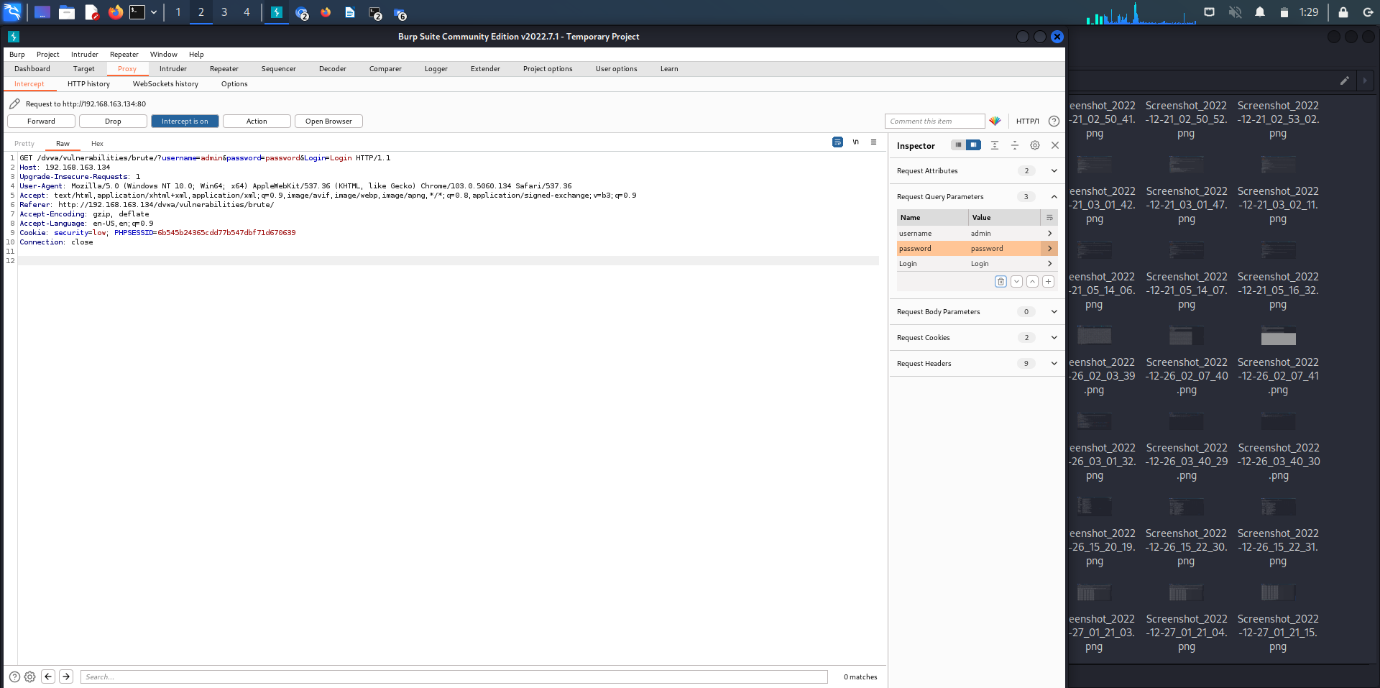
PHPSESSID= 6b545b24365cdd77b547dbf71d670639;security=low’ -V

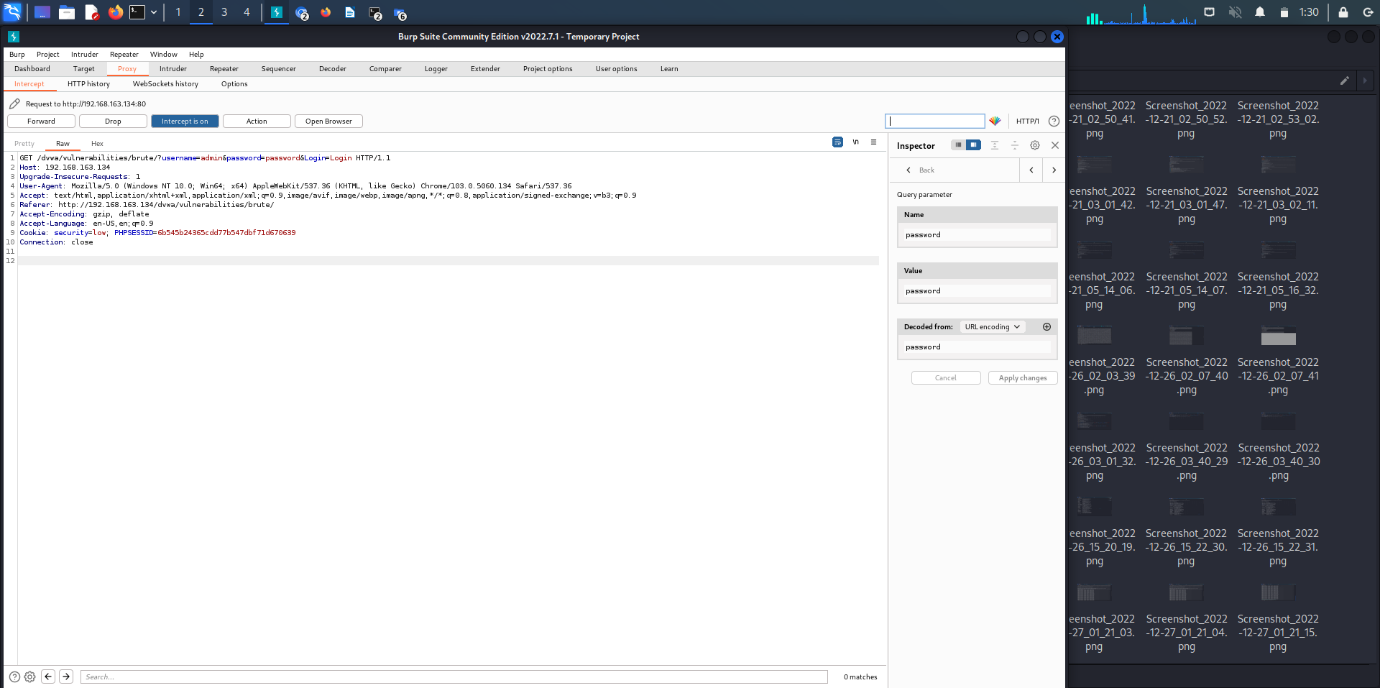




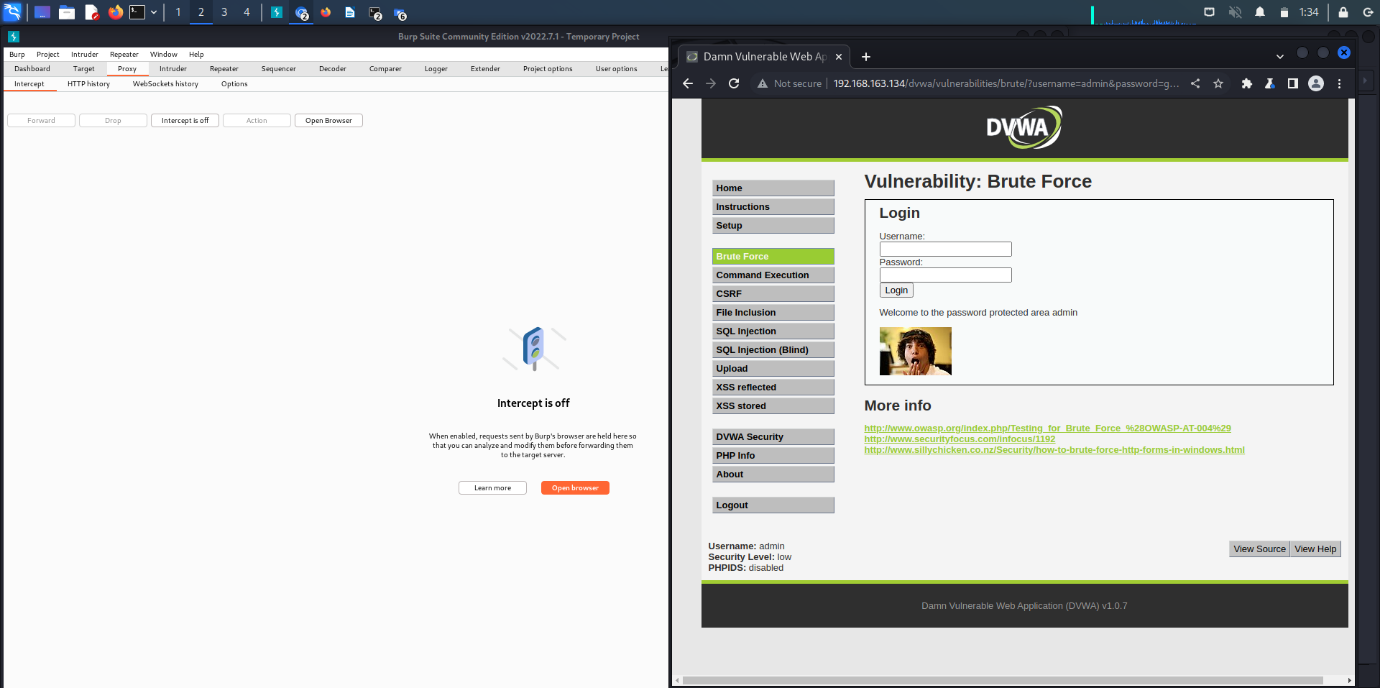
1. Hydra was successful in performing the dictionary attack on the dvwa login page and the password was found to be – password.
2. In Request Query Parameter, we will enter into the password field.





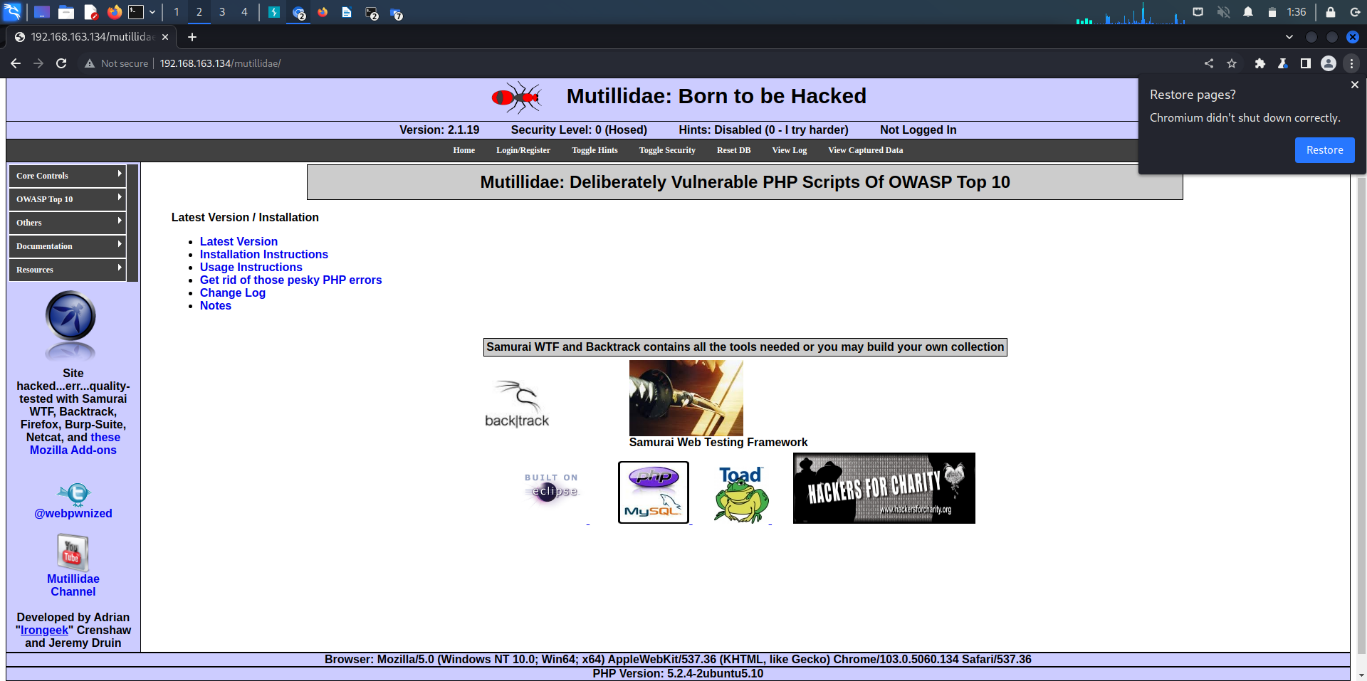


1. Next, we will hit FORWARD and forward our login request. As soon as we hit forward, we will be directed to the

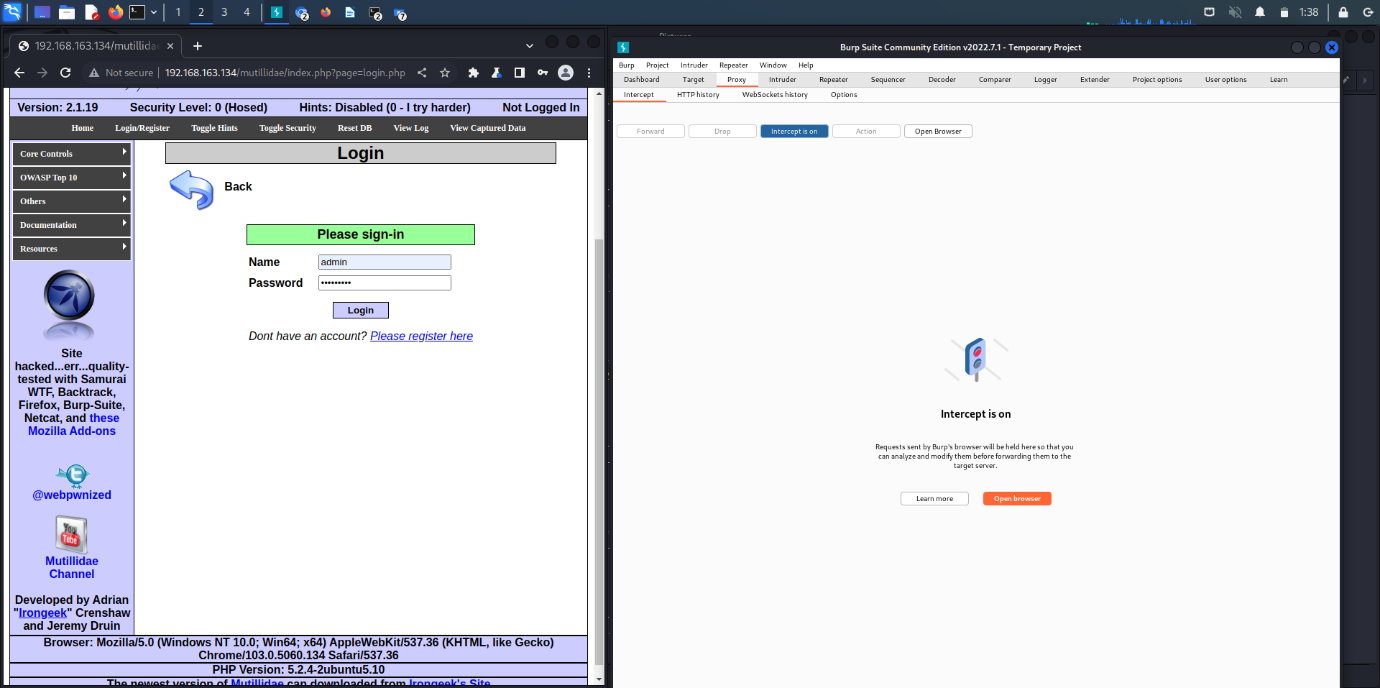


**TO PERFORM DICTIONARY ATTACK ON MUTILLIDAE USING HYDRA**

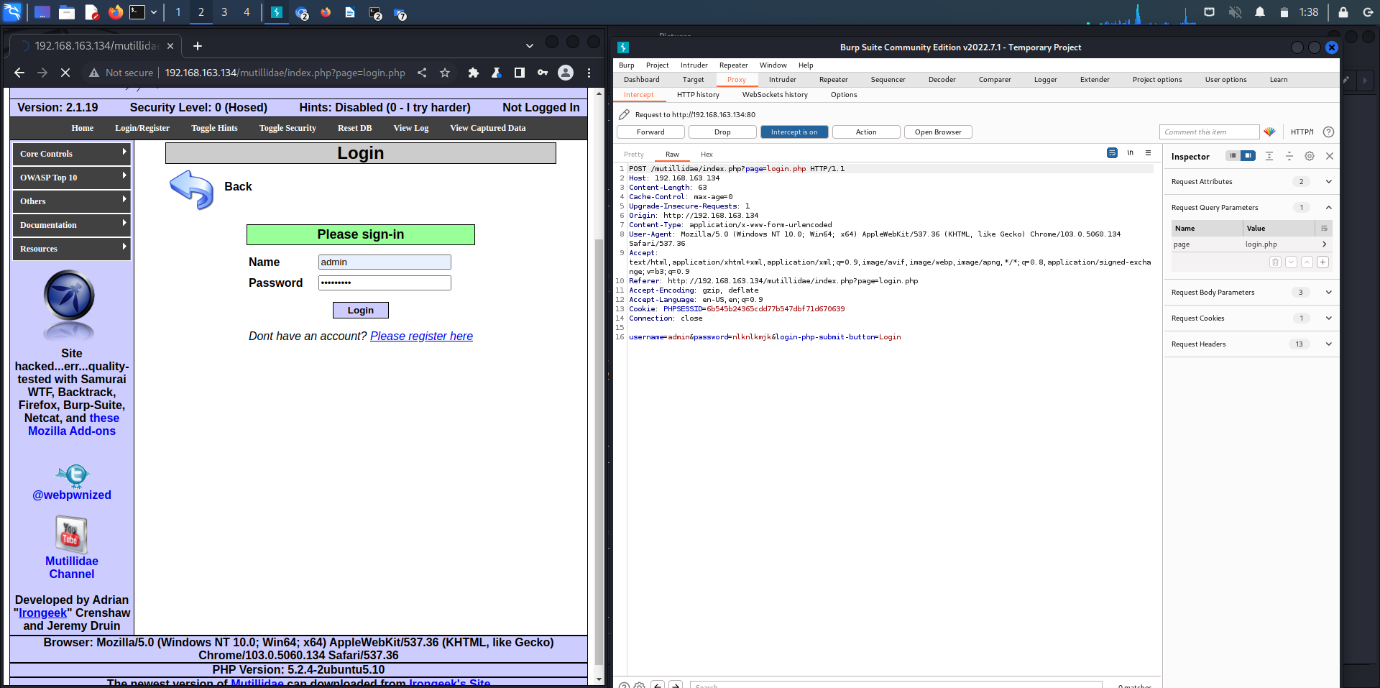
1. Open BurpSuite. Type the IP address of Metasploitable and then open Mutillidae.



1. In the Login/Register tab, enter any name and password, and turn the intercept ON.

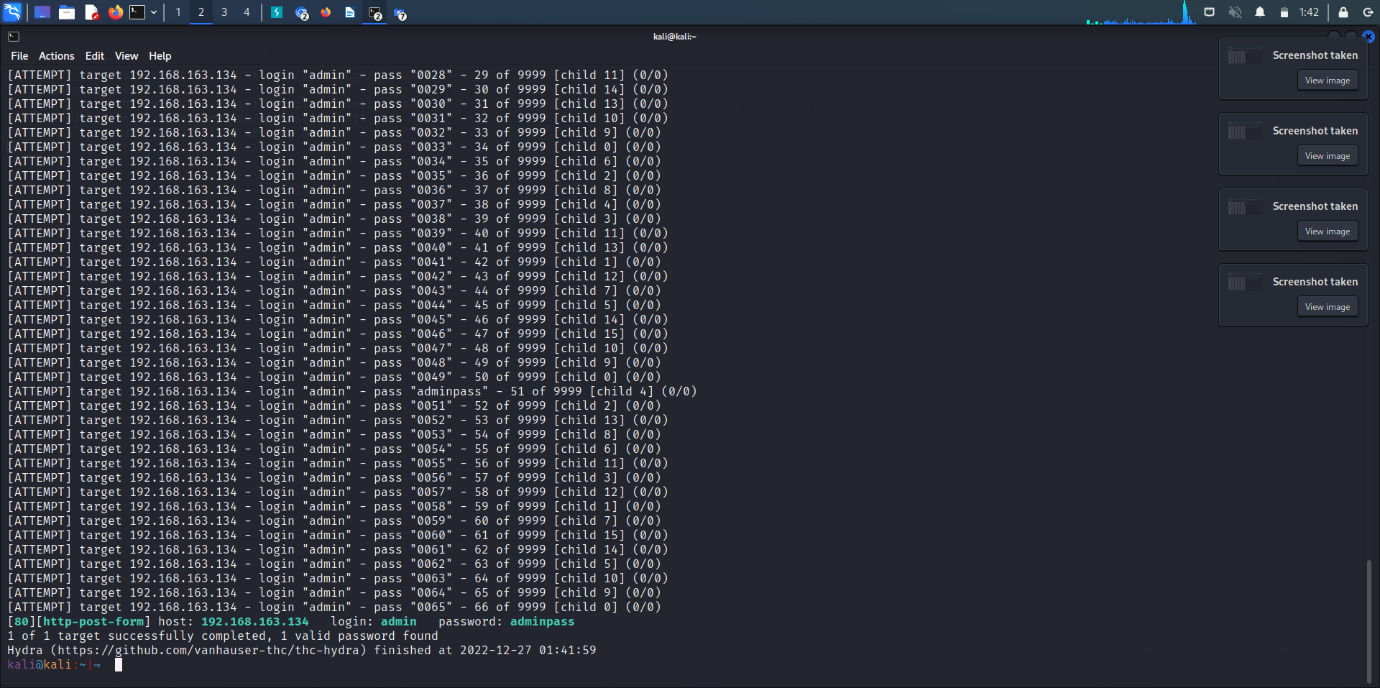
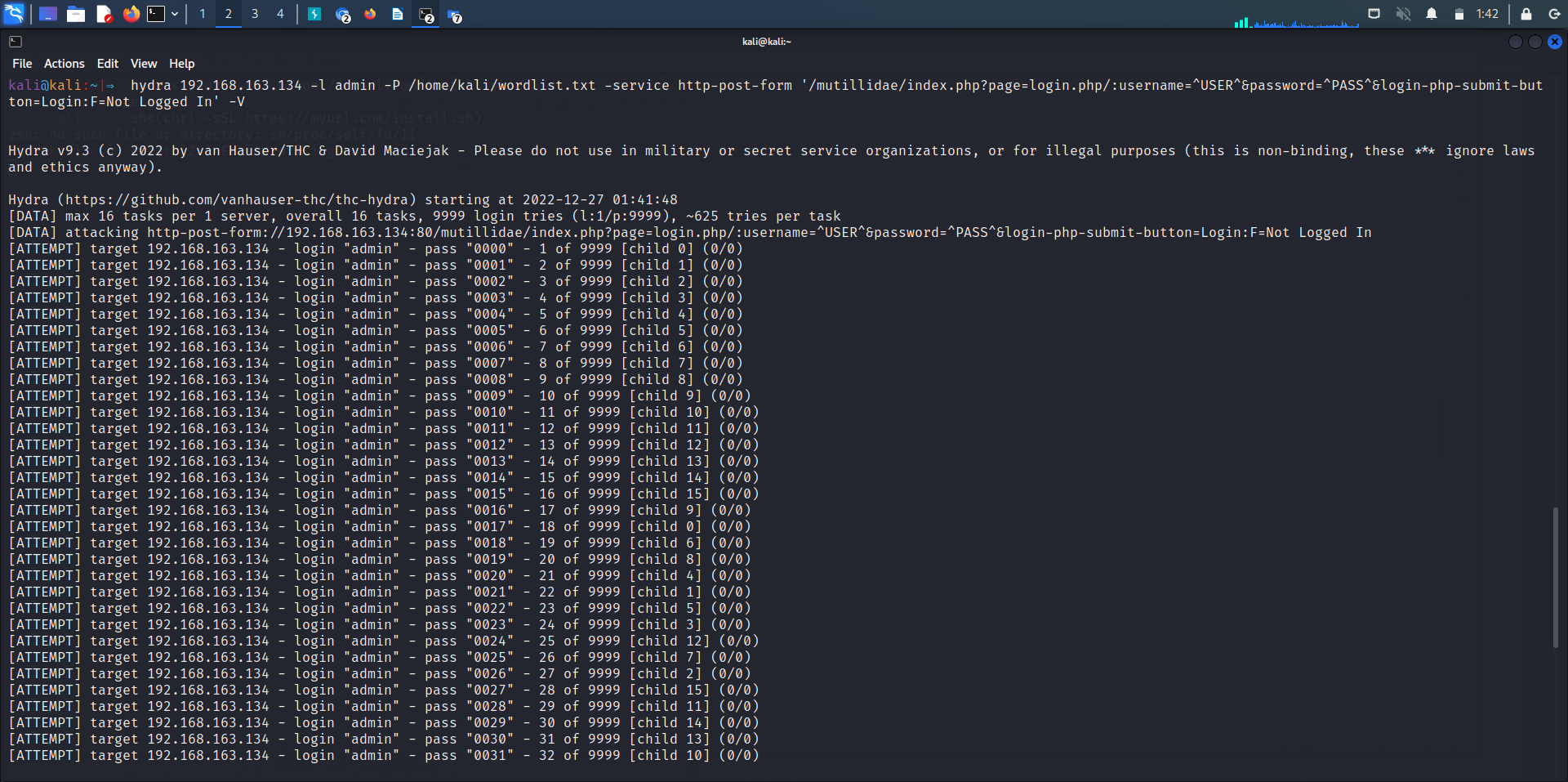


1. The intercept captures our request. We get details like http-get-post, the url, etc which will be used in hydra.



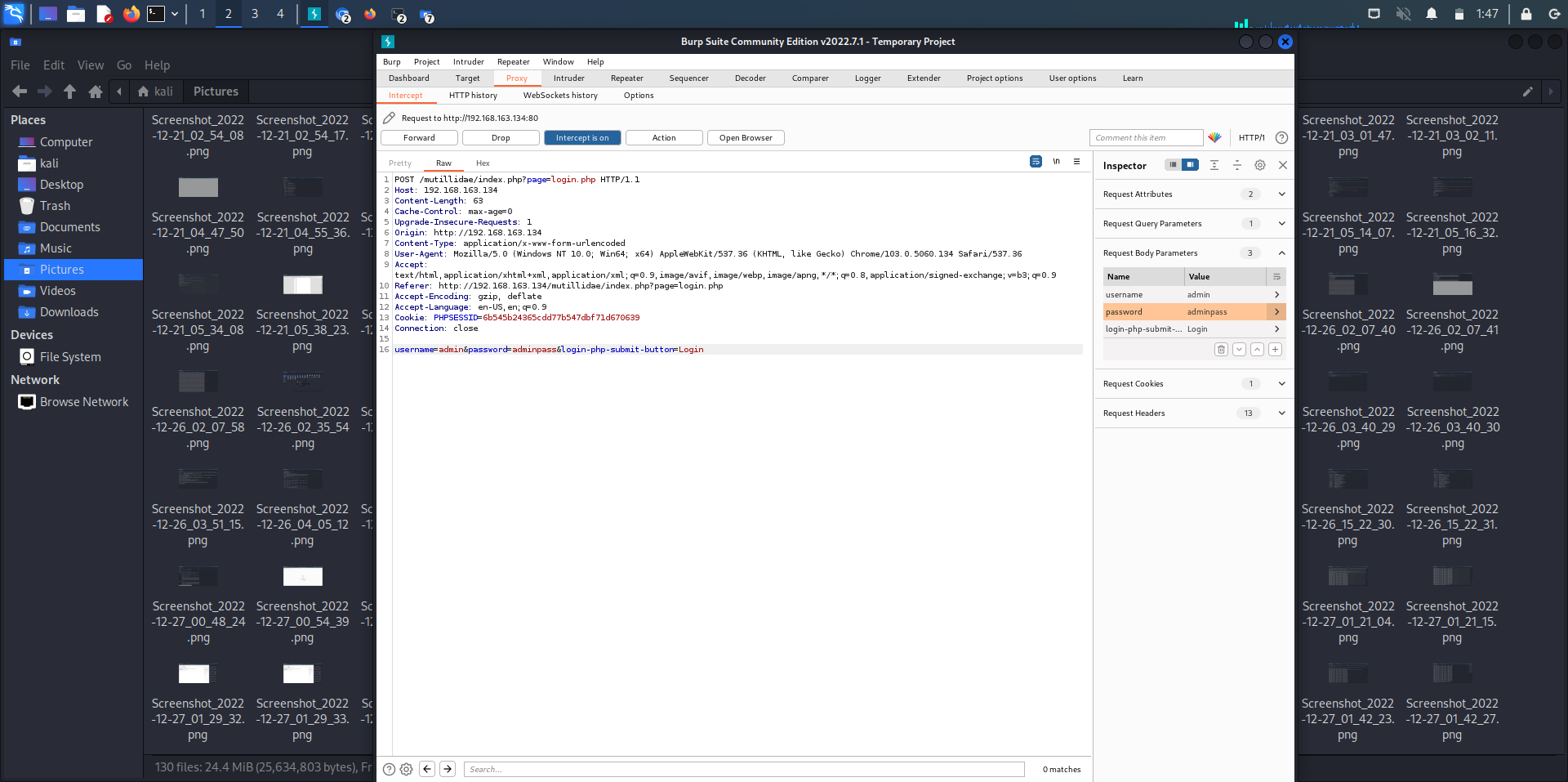
1. In the command prompt, we type the following command and hydra carries out a brute force attack using the wordlist that we created earlier.

hydra 192.168.163.134 -l admin -P /home/kali/wordlist.txt -service http-post-form ‘/mutillidae/index.php?page=login.php/:username=^USER^&password=^PASS^&login-php-submit-button=Login:F=Not Logged In’ -V

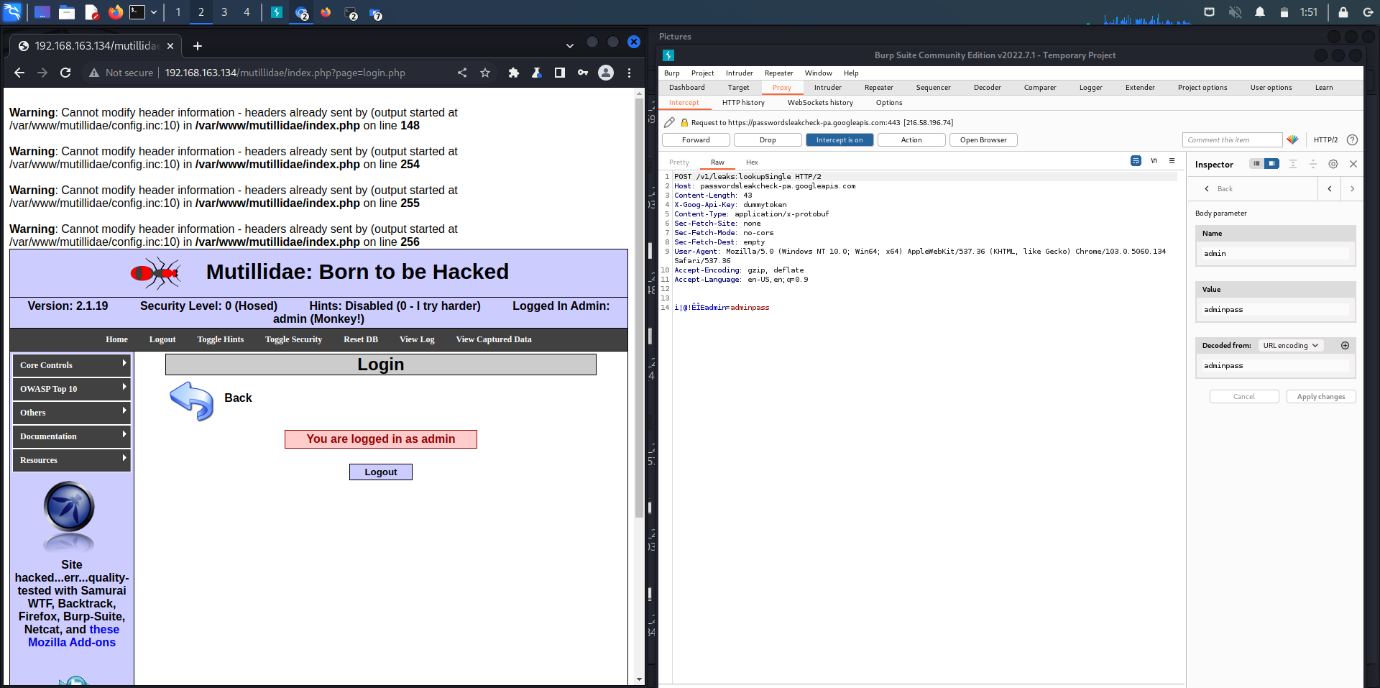


1. We get the password as – adminpass and use this to bypass the login page of Mutillidae.

6.We change the value of password in body parameter and replace it with – adminpass



7.As soon as we forward the request, the user gets logged into Mutillidae.



**RESULT:** Wordlist (wordlists.txt) was created using crunch and the same was used to successfully conduct a dictionary attack on DVWA and Mutillidae using Hydra.