**Steps for SQL Injection**

* First, we need to open both Kali Linux and Metasploitable2 and make sure the network connection is bridged.
* Then we would log in to Metasploitable2 by using admin and password" "msfadmin."
* After that, we will make sure that IP address is assign by using command ifconfig
* If it is not assign we will assign it to Metasploitable2 with same subnet by using command sudo ifconfig eth0 IPaddress netmask (netmask)
* We can check in Kali Linux using command ping IPaddress\_of\_Metasploitable2 to see if it is working
* Then we will go to Firefox and type IP address for Metasploitable2 in the search bar and will land you on the page.
* We will then click on Mutillidae and the click on OVAStop10 and then click on SQL injection and then user info. This will take you to log in page
* We will then open BURPSUITE on Kali Linux and then go to PROXY and navigate to options and choose the IP address available so we can use it a proxy and the make intercept ON.
* Then we will open Firefox and click on the settings and manually set the proxy to IP in the BURPSUITE
* Then we will go back to Muttillidae and enter random username and password. Once the request is captured and you can confirm that by checking on BURPSUITE.
* After that, right click and save the data extracted.
* Then go back to settings in Firefox and set it back to default.
* After that open SQLMAP. Go to terminal and write command sqlmap
* Write command sqlmap -r location\_on\_the\_file\_that\_has\_data\_extracted --dbs
* It will fetch multiple injection points in the database. We can then choose any of the points for SQLinjection.
* It will then fetch different databases and you can choose any that you want to exlpoit.
* Write command sqlmap -r location\_on\_the\_file\_that\_has\_data\_extracted --D databasename --tables
* It will give injection options again you can choose any of the options and it will fetch the tables in the database
* Use command sqlmap -r location\_on\_the\_file\_that\_has\_data\_extracted --D databasename -T tablename --dump
* It will give options and you can choose any and then it will fetch all the data in the table.