**SQL injection attack steps**

1. Open Metasploitable2 and run the command “ifconfig” to see if ip address is assigned or not. After the command is run, we see that it is connected with ethernet, so we need to assign it an IP address.
2. Now open Kali Linux and run the command “ifconfig” here too. It will show the IP address assigned to it. For eg in my case it is 192.\*\*\*.\*\*\*.\*\*, and netmask is 255.\*\*\*.\*\*\*.\*
3. Now go back to Metasploitable2 and assign the IP address by running the following command “sudo ifconfig eth0 <IP address I want to assign> netmask <netmask same as Kali Linux>”

**“sudo ifconfig eth0 192.\*\*\*.\*\*\*.\*\* netmask 255.\*\*\*.\*\*\*.\*”**

1. Enter the password of Metasploitable2.
2. Enter the command “ifconfig” again to check if the IP address is assigned.
3. Go back to Kali Linux, and use the command “ping <IP address of Metasploitable2>” i.e., **“ping 192.\*\*\*.\*\*\*.\*\*”**, to see if Kali Linux is able to ping Metasploitable2.
4. To access Metasploitable2 from Kali Linux we open the browser and enter the IP address of Metasploitable2 in it.
5. The browser opens a page with the banner of Metasploitable2 and a lot of applications.
6. We open “Mutillidae”, go to “OWASP Top 10” -> “A1- Injection” -> “Sqli – Extract Data” -> “User info”. It takes us to login page.
7. In kali Linux go to applications, and under “web application analysis” open “Burpsuite”.
8. Once Burpsuite opens, select “Proxy” and then “Options”, there we will find an IP address with port number (127.\*.\*.\*:\*\*\*\*) which we will use later to send requests.
9. Now go to “intercept” option and make sure “intercept is on”.
10. We open a new tab in the browser, go to settings-> general (scroll down, in “Network Settings”) -> settings -> select options “Manual proxy configuration” + “Also use this proxy for HTTPS”, and write the IP address and port number in “HTTP Proxy” field.
11. Now we go back to “Mutillidae” tab in browser, and enter random username and password. We go back to burpsuite and see if our request is captured. Keep trying random usernames and passwords until a request is captured. Once we get “Upgrade-Insecure-Requests: 1” it means a request is captured. Right click, go to “save item” and save the file as “filename”.txt in Desktop.
12. Go back to browser and reset the settings to default.
13. In applications of Kali Linux under “Database assessment” there is a tool “sqlmap” which is used to exploit and detect vulnerabilities in database and provide options to inject malicious code into them.
14. Now open Kali Linux terminal and type “sqlmap -r <path of txt file saved on Desktop> --dbs”

**“sqlmap -r /root/Desktop/extract.txt –dbs”**

This command will show all the injection points from where data can be extracted.

1. Type “0” and enter. It fetches **“the back-end DBMS is MySQL”**, and multiple databases that are available.
2. Choose a database and write “sqlmap -r /root/Desktop/extract.txt -D <name of chosen database> --table”

**“sqlmap -r /root/Desktop/extract.txt -D owasp10 --table”**

1. It asks for options again, so we go with default option “0” and enter.
2. All the tables fetched are shown.
3. To see further what information is there in the tables type “sqlmap -r /root/Desktop/extract.txt -D owasp10 -T <name of table> --dump”

**“sqlmap -r /root/Desktop/extract.txt -D owasp10 -T accounts --dump”**

1. Again, go with default option “0”.
2. All the information in “account” table will be displayed.