**Steps and Commands to perform the attack**

1. In order to perform the attack, setup the “Kali Linux” and “Metasploitable” in the virtual environment (VMware or Virtual Box).

2. Once setup, go into the network settings of both “Kali Linux” and “Metasploitable”, select the network connection type “Bridged”.

3. Make sure the option “Bridged” is selected or else, you will have difficulty performing the attack.

4. Boot up both systems.

5. Login details for “Kali Linux” is “kali” for both username and password.

6. Login details for “Metasploitable” is “msfadmin” for both username and password.

7. Type “ifconfig” on kali linux’s terminal and on metasploitable’s terminal.

8. Check that if each system is on same subnet and if it is then skip to step No 14, otherwise

9. Note down the netmask and subnet IP on Kali Linux.

10. If the IP on Kali Linux is like “192.168.1.1” then assign the IP on Metasploitable from onwards from “1.1”, like “192.168.1.2”.

11. On Metasploitable, type the command “sudo ifconfig eth0 192.168.1.2 netmask 255.0.0.0”.

12. In the above command “192.168.1.2” is the IP you will assign and “255.0.0.0” is the netmask IP.

13. Check if the IP is assigned by typing the command “ifconfig”.

14. Go on Kali Linux and ping the IP on the Metasploitable by the command “ping 192.168.x.x” to see if the IP is working or not.

15. Open Firefox, type in the IP address of Metasploitable, once open, select the option “Mutillidae”.

16. At the left side, hover the mouse on the option “OWASP Top 10”, select “A1- Injection” and then select “SQLi – Extract Data” and finally select “User Info”.

17. Now go an application called “Burpsuit” from Kali Linux.

18. Select “Temporary Project” and click “next”.

19. Select “Use Burp defaults” and click “start Burp”.

20. Select the option “Proxy” and then select “Options”.

21. See the IP address and port number in the table below “Proxy Listeners”.

22. It will look something like this “127.0.0.1:8080”, and note it.

23. Now select “Intercept” from the toolbar and make sure the intercept is on.

24. Now open firebox and open settings.

25. Scroll down in settings and there will be an option “Settings...” under Network Proxy.

26. Select “Manual proxy configuration” and type the IP you just noted in the field “HTTP Proxy” and its port number next to it. Make sure the option “Use this proxy server for all protocols” is selected. And click “OK”.

27. Now go back to Metasploitable IP page and type in random “Name” and “Password”. And Click “View Account Details”

28. Now open “Burpsite” and see if it is intercepted when you see the line “Upgrade-Insecure-Request: 1”.

29. If it is not intercepted then turn intercept off and one and re-repeat the step, No 27-29, otherwise.

30. Right click and select “save item”.

31. Save it at desktop with name like “extract.txt” or anything you like.

32. Close Burpsite.

33. Make sure, to set back the default settings of proxy in Firefox.

34. Close Firebox.

35. Open terminal and,

36. Type the command “sqlmap -r /root/Desktop/extract.txt --dbs”.

37. After it shows you the injection options, type “0” and enter.

38. Now, the attack is performed, you will be presented with information such as DBMS type, operating system, web application technology and DBMS version.

39. Also, a list of databases will be presented to you.

40. Now, you can access the databases and their table.

41. Happy Hacking!