CIS 214 Assignment SQL Injection

This assignment assumes you have already set up SQLol as described in SQLInjectionDemo.pdf.

Recall that the first significant step in the attack by Anonymous on HBGary Federal was to use SQL Injection to dump administrator usernames and passwords from the DBMS. That's exactly what you will do in this assignment.

First however, you will have to add an administrator. This is done by interacting directly with the DBMS (not through the web server) as as administrator of the DBMS.

At a root command prompt in Kali (with the mysql service started) type:

**# mysql**

This will change your prompt to

**mysql >**

This is the command line interface to the DBMS. As an administrator, you can add a new user to the database using the command:

**mysql > CREATE USER 'aaron'@'localhost' IDENTIFIED BY 'dumbpassword';**

The result of this is that aaron will be able to login locally to the database using the password “dumbpassword”.

Exit the database

**mysql > exit**

For the rest of this assignment, you will interact with the database through the web browser as an attacker would. Your task is to use SQL injection to retrieve aaron's hashed password.

Like all other metadata, aaron's hashed password is stored in one of the tables in the information\_schema database.

Use commands like the ones in the demo to poke around in those tables to find out where it is stored and retrieve it when you find it. The table names are fairly descriptive so it's not hard to find them!

What to Turn in

When you are done, answer the following questions:

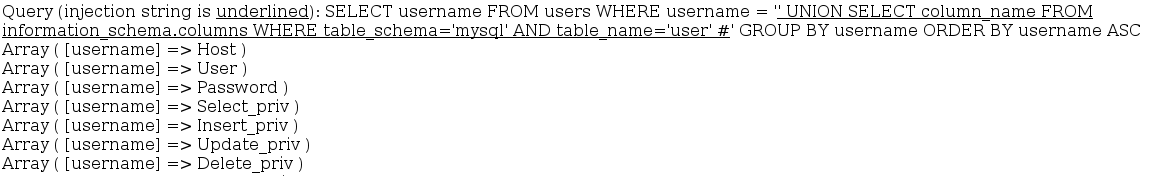
1. What is the name of the table where the password hashes are found?

Answer here

The table with the hashed passwords is called “Password”, and is within the table “user” within the schema “mysql”.

2. What are the names of all columns in the table where the password hashes are found?

Answer here



Host, User, and Password are the columns that we care about.

3. What is aaron's hashed password?

Answer here

\*B96E9E701CCF8A5B7E99FDE5D78D9CB110E13A49 )

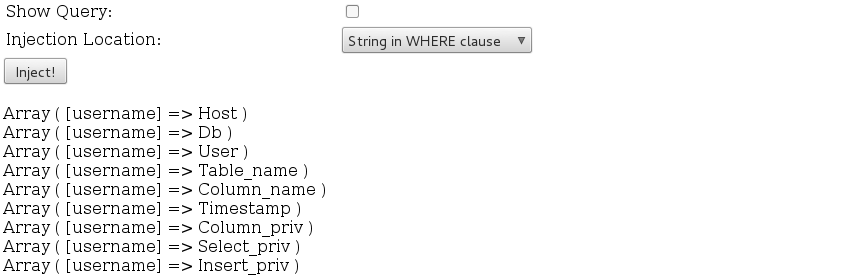
4. What command, typed into the form on the web page, retrieves the names of the columns in question 2?

Answer here

' UNION SELECT column\_name FROM information\_schema.columns WHERE table\_schema='mysql' AND table\_name='user' #

Show a screenshot of the result of that command (i.e., the portion of the web page starting at “results:”):

screenshot here



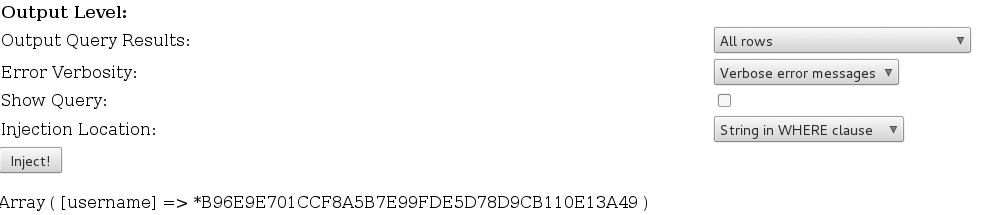
5. What command, typed into the form on the web page, retrieves aaron's hashed password?

Answer here

' UNION SELECT password FROM mysql.user WHERE user='aaron' #

Show a screenshot of the result of that command (i.e., the portion of the web page starting at “results:”):

screenshot here



**Just for fun:**

I put Aaron’s hashed password into crackstation and was able to decrypt it very easily:

