Colin Quinn

Wireless Security

Lab 2

Due: 7th Friday, 8/27/2021

SQL Injection Seed Labs

With SQL, we can search for certain information within the database, searching for all of Alice’s information is done with the command shown below. Chart, bubble chart

Description automatically generated with medium confidence

When performing the SQL injection on the website, running this command in the username field will result in accessing the entire table available on the site. Graphical user interface, text, application

Description automatically generatedand the result looks like this:

Text

Description automatically generated

Running the same attack through cURL gives a result that looks like this:

Text

Description automatically generated

Attempting to run multiple SQL commands does not seem to work properly according to this screenshot below. Graphical user interface, text, application, email

Description automatically generated

For task 3, in order to change the salary of a user, you must enter a command such as this: `,salary=’new salary’ where EID=’employee ID’; #. Doing so results in a page that looks like this where we change Alice’s salary to 999999.

Table

Description automatically generated

When changing someone’s password, it is common for it to be stored as a hash value. So we must convert our new password using the same hash algorithm as the database, in this case it is SHA1, so we can do so by entering this command to hash the word “password”.

A picture containing text, screenshot, indoor

Description automatically generated

In order to load this new password, we enter a string like this: ',Password='5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8' where name='Boby'; #

And we can check it by logging in as admin or attempting to sign in to Boby’s account. Graphical user interface

Description automatically generated with low confidenceAs a result, we can log in with Boby’s EID and the new password that we have set for him.

In order to secure the database from SQL injection, prepared statements can be used to separate user input from compiled statements. The following changes were made to /var/www/SQLInjection/unsafe\_home.php in order to secure this site from SQL Injection attacks.

Text

Description automatically generated