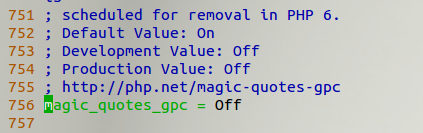
Daniel Oliveros

Garrett Bogart

Spring 2018 – Independent Study

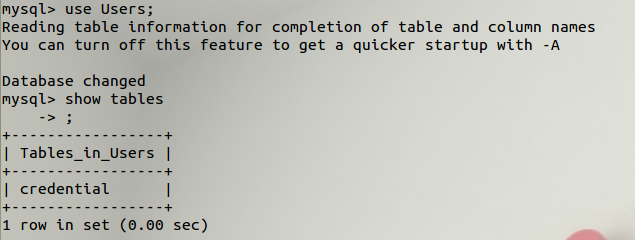
SQL Injection Vulnerability Lab

First, we turned off the countermeasures found in apache to defend against a SQL injection

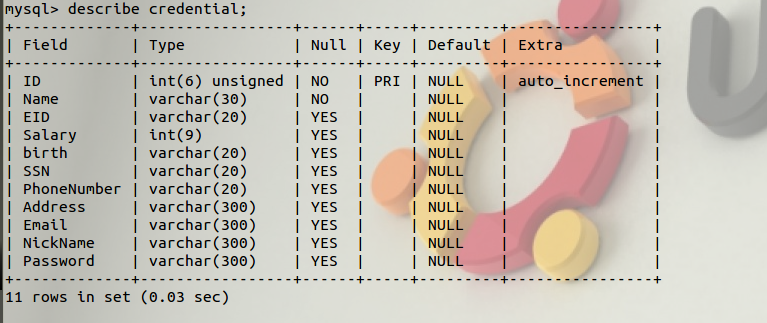


**Task 1:**

We need to find information about the database that we will be using. Looking at the Users we can see that it has a credential table.



To look at what kind of data credential has we can use the command: describe credential.

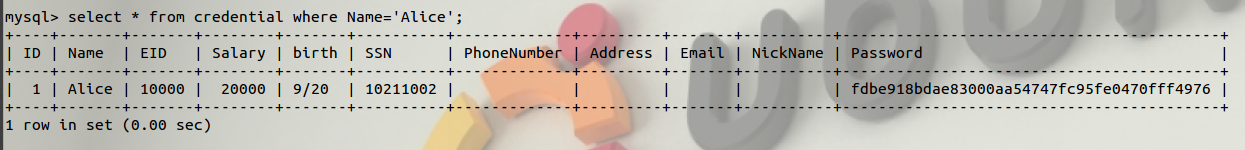


To select a specific user from the credential table we have to use a query.

select \*

from credential

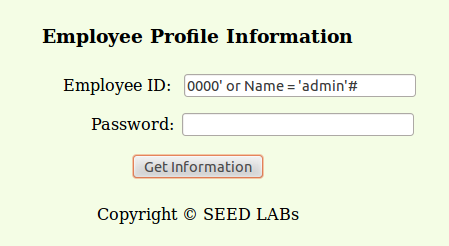
where Name=’Alice’;

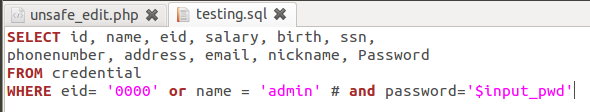


**Task 2:**

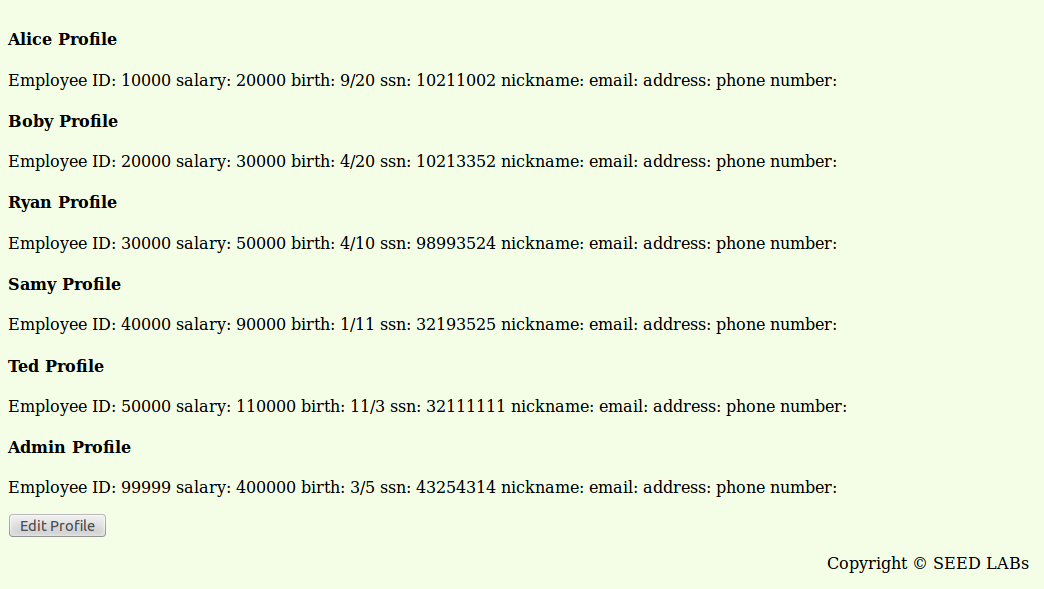
**2.1.**

Looking at the SQL statement, we found that inputting the following to the Employee ID field executes the command we want to. We tested this approach by pasting the code onto a text editor and seeing what happened.

****

****

This statement will display all the information we want to get through the admin profile.



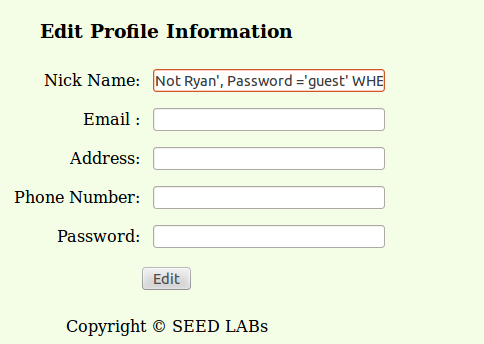
**2.2.**

Using curl we have to rewrite the request to contain our new query. We used an encoding website <http://demo.nickname.net/demo/testpak/encode.pl> to help convert our query into the proper format. We attached our converted query to EID in the url so that when the request is sent our query is inserted into the normal query.



**2.3.** query() only executes a single SQL statement. We can’t append a second one to our original one and expect it to work. Info on that here: <http://php.net/manual/en/function.mysql-query.php>





Not Ryan', Password ='guest' WHERE Name = 'Ryan'#



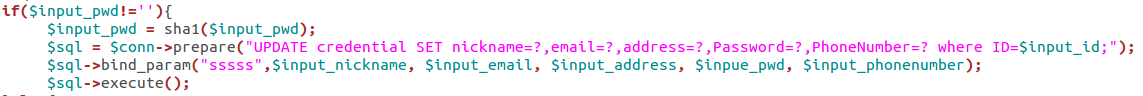
After hashing guest: Not Ryan', Password using the sha1 approach =**35675e68f4b5af7b995d9205ad0fc43842f16450** WHERE Name = 'Ryan'#



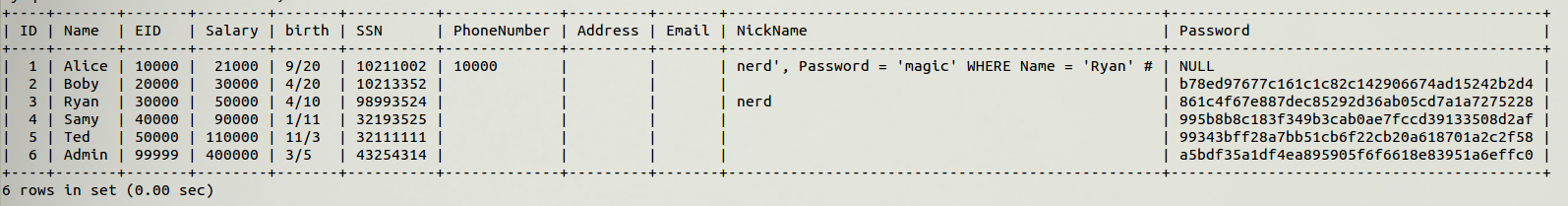
We can now log in as guest on Ryan’s profile

**Task 4:**

After changing the code for it to work using prepared SQL statements, we restarted the server and ran the previous command on the edit page.

****

The result went as we expected. The SQL code that was injected was passed in as a parameter instead of as runnable code.

****

**Resources**

* <http://www.sha1-online.com/>
* <http://demo.nickname.net/demo/testpak/encode.pl>

**Ideas for Improvement:**

* It would be very wise to go over SQL commands, especially with how to profile the database to learn what’s going on in it. Also would be good to go over comments and basic SQL syntax.