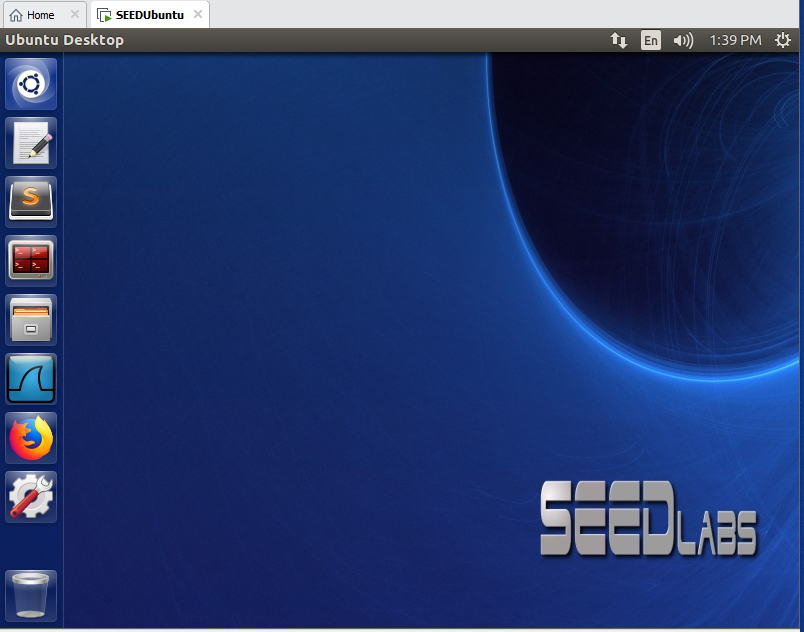
Huỳnh Nghiêm Phú Hưng

1712478

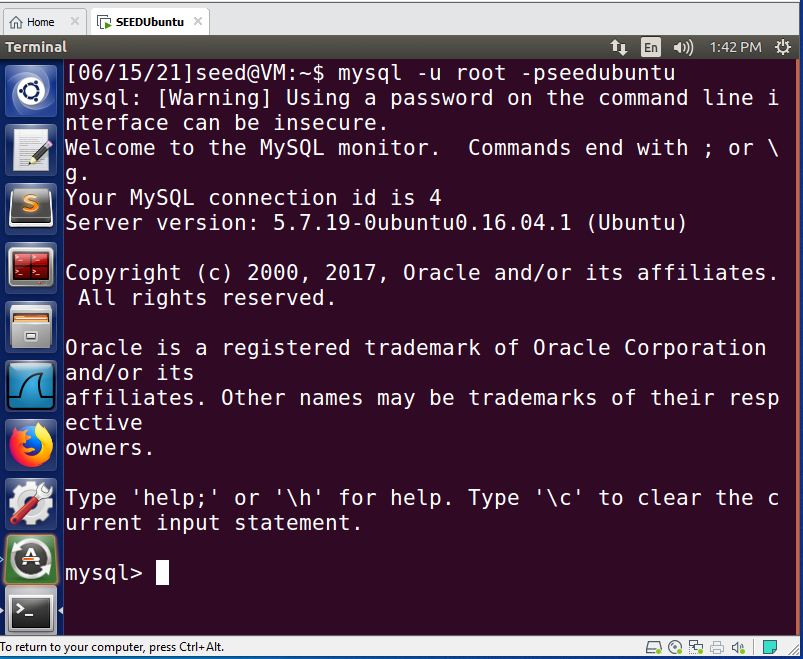
LAB 5: WEB SECURITY

1. SQL Injection

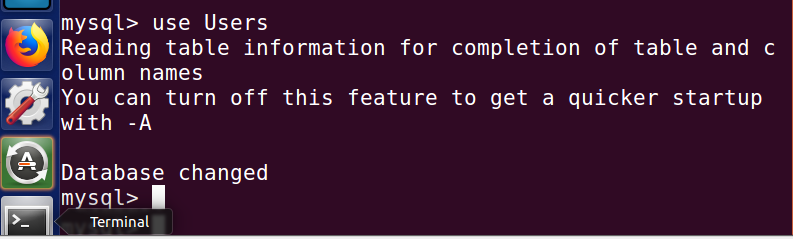
- Cài đặt môi trường cho bài lab, sử dụng SEED Ubuntu 16.04 VM



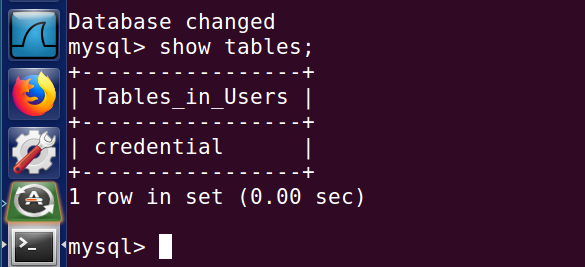
- Để đăng nhập vào database, dùng lệnh: **mysql -u root -pseedubuntu**



- Môi trường đã tạo sẵn Users database, ta chỉ cần load bằng lệnh: **use Users**

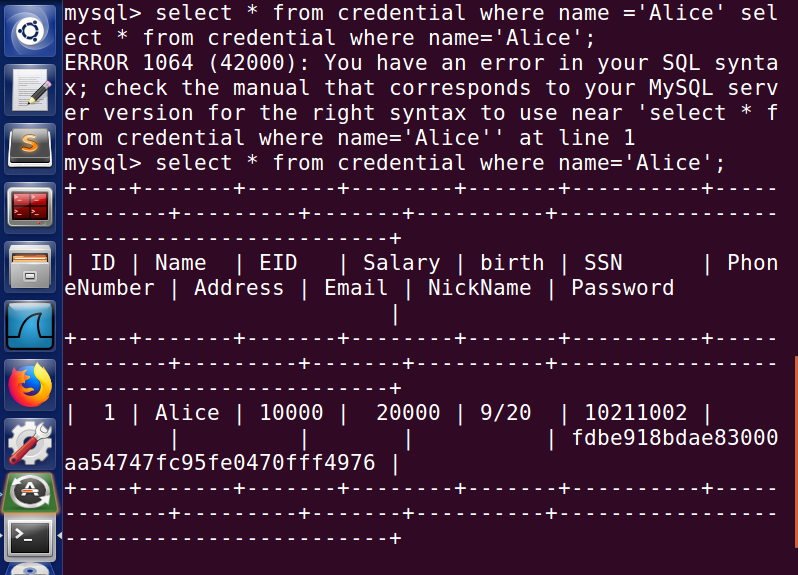


- Để show toàn bộ các bảng của database trên, dùng lệnh: **show tables;**

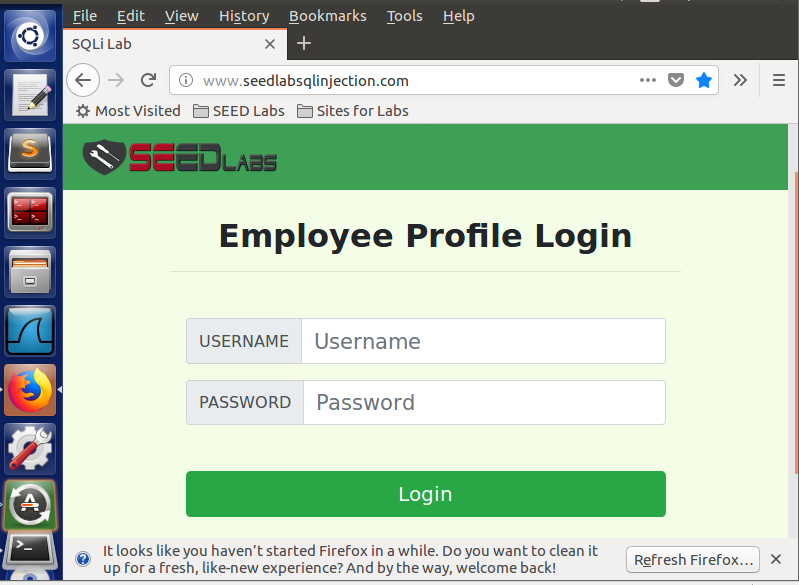


- Để show các thông tin của Alice trong bảng credential.

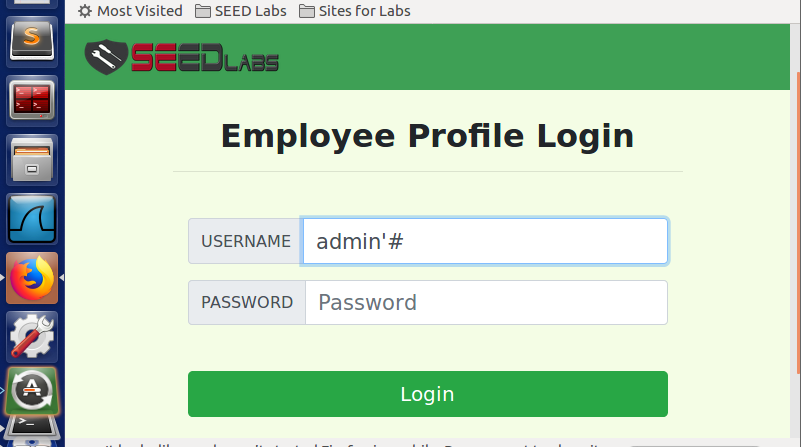
dùng lệnh: **select \* from credential where name = ‘Alice’;**



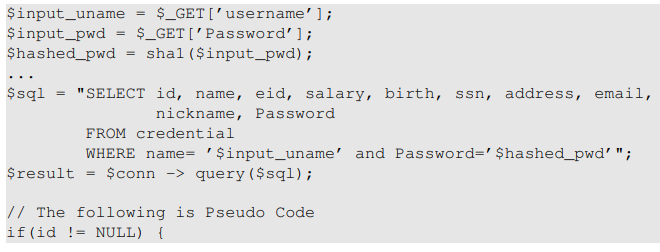
- Ta sẽ thực hiện tấn công SQL Injection trên trang web **seedlabsqlinjection.com**



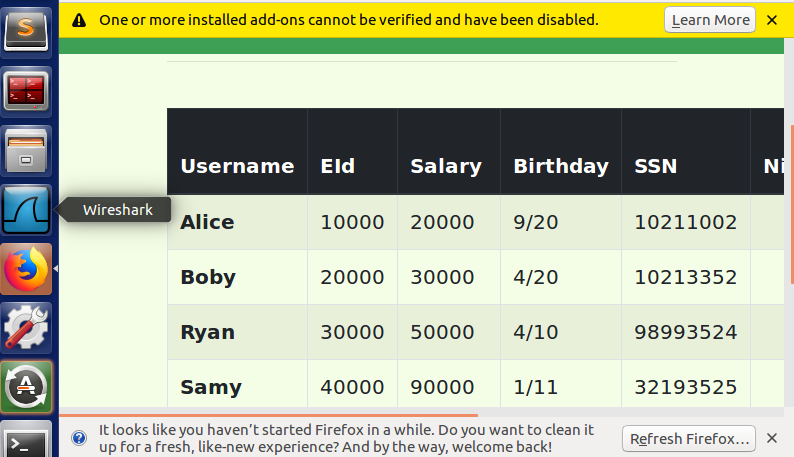
- Có thể đăng nhập tài khoản quản trị (giả sử đã biết tên tài khoản quản trị là admin) mà không cần mật khẩu, bằng cách điền vào ô USERNAME: **admin’#**



- Nguyên nhân là do câu lệnh điều kiện WHERE khi chứng thực user admin, sử dụng dấu nháy để đóng phần USERNAME và dấu # để làm vô hiệu điều kiện phía sau.

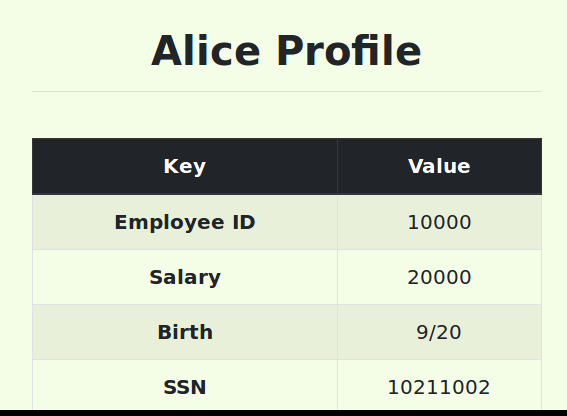


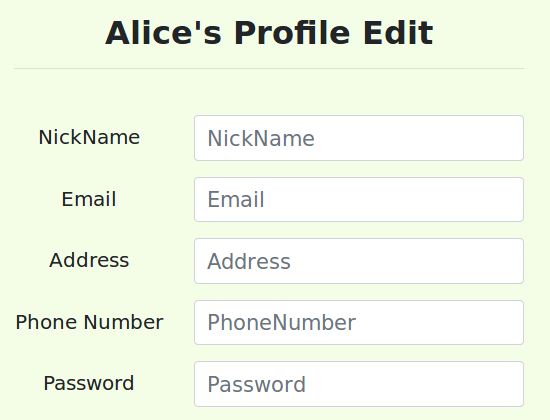
- Tại đây có thể lấy được thông tin các user trong database



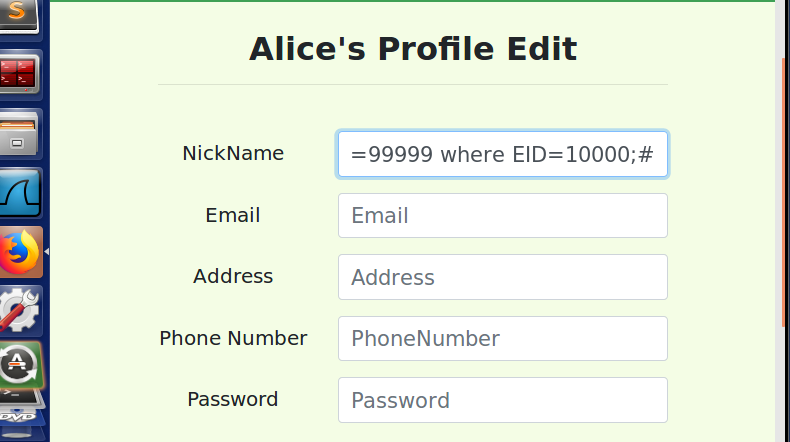
• Task 5.1: Modify your own salary. As shown in the Edit Profile page, employees can only update their nicknames, emails, addresses, phone numbers, and passwords; they are not authorized to change their salaries. Assume that you (Alice) are a disgruntled employee, and your boss Boby did not increase your salary this year. You want to increase your own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. Please demonstrate how you can achieve that. We assume that you do know that salaries are stored in a column called ’salary’.

Mỗi User đều có thể chỉnh sửa các thông tin cơ bản như Nickname, Email, ... Ở đây, sử dụng cách trên để đăng nhập vào tài khoản Alice (nhập Alice’# vào ô USERNAME khi đăng nhập), sau đó qua mục Edit Profile để xem các thông tin được quyền chỉnh sửa.

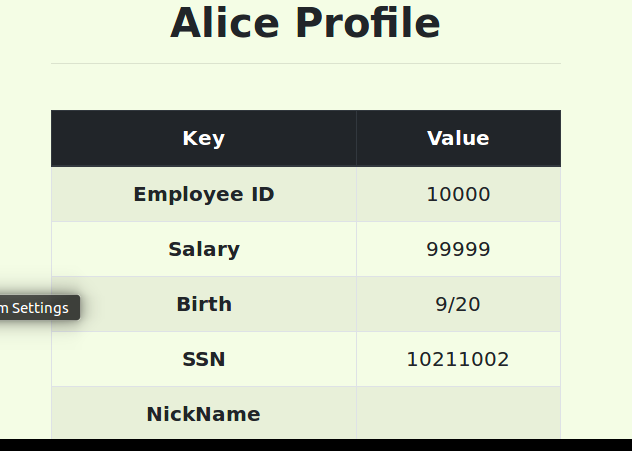




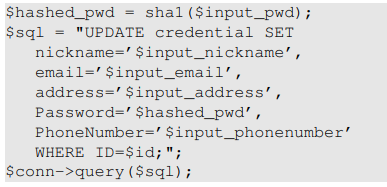
- Có thể thấy rằng các User không có quyền chỉnh sửa các thông tin khác ngoài những thông tin có trong form. Tuy nhiên, có thể chỉnh sửa lương của Alice, nhập vào ô NickName: **’,salary=99999 where EID=10000;#**



- Nhấn Save để lưu lại, ta sẽ thấy thông tin lương ban đầu của Alice là 10000 nay đã trở thành 99999.

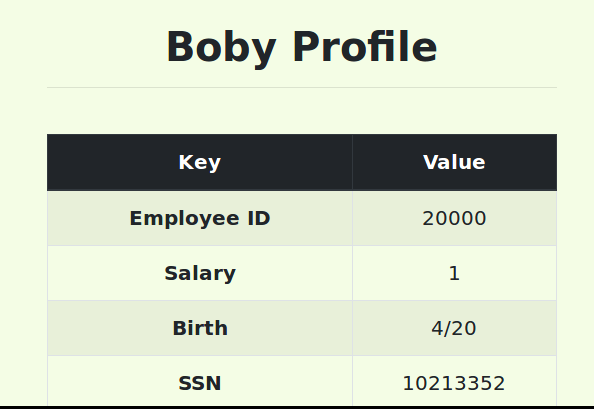


- Nguyên nhân là do đoạn code thực hiện UPDATE thông tin mắc lỗi tương tự như phần đăng nhập, dấu nháy làm đóng lại phần nick name, sau đó tự tùy chỉnh salary và bỏ qua thành phần, điều kiện phía sau dấu #.



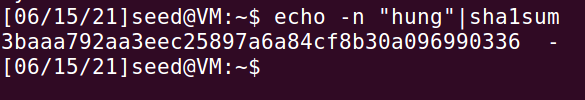
• Task 5.2: Modify other people’ salary. After increasing your own salary, you decide to punish your boss Boby. You want to reduce his salary to 1 dollar. Please demonstrate how you can achieve that.

- Có thể thay đổi lương của người khác ngay trong giao diện chỉnh sửa user Alice bằng cách khai thác lỗ hổng trên, nhập: ’,salary=1 where name=’Boby’;#

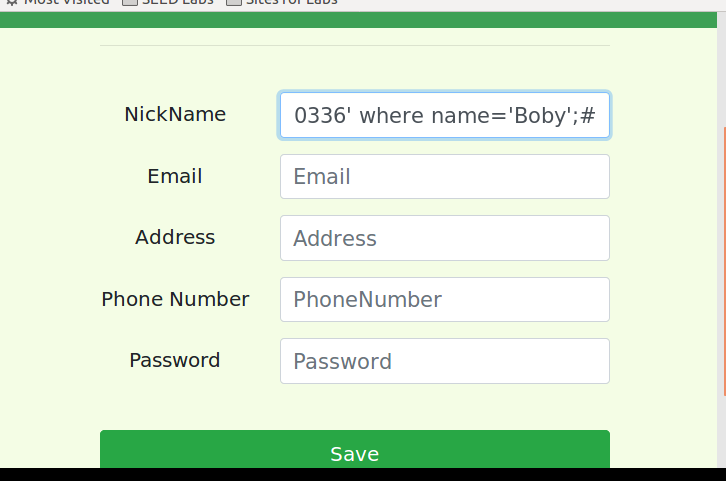


• Task 5.3: Modify other people’ password. After changing Boby’s salary, you are still disgruntled, so you want to change Boby’s password to something that you know, and then you can log into his account and do further damage. Please demonstrate how you can achieve that. You need to demonstrate that you can successfully log into Boby’s account using the new password. One thing worth mentioning here is that the database stores the hash value of passwords instead of the plaintext password string. You can again look at the unsafe edit backend.php code to see how password is being stored. It uses SHA1 hash function to generate the hash value of password.

Ta còn có thể thay đổi password của User khác. Vì password được so sánh trong database là password đã được băm ra bằng sha1, nên phải chuyển password muốn đổi thành dãy được băm bởi sha1. Giả sử muốn đổi password của tài khoản Boby thành ‘**hung**’, đầu tiên cần phải băm password, dùng lệnh: **echo -n “hung” | sha1sum**



- Copy dãy sau khi băm, nhập vào ô NickName trong giao diện edit của tài khoản: ’,password=’3baaa792aa3eec25897a6a84cf8b30a096990336’ where name =’Boby’;#



- Trở về trang đăng nhập, đăng nhập với tài khoàn Boby, mật khẩu: **hung**