**Môn học:** An toàn thông tin

**Họ tên:** Võ Văn Đức

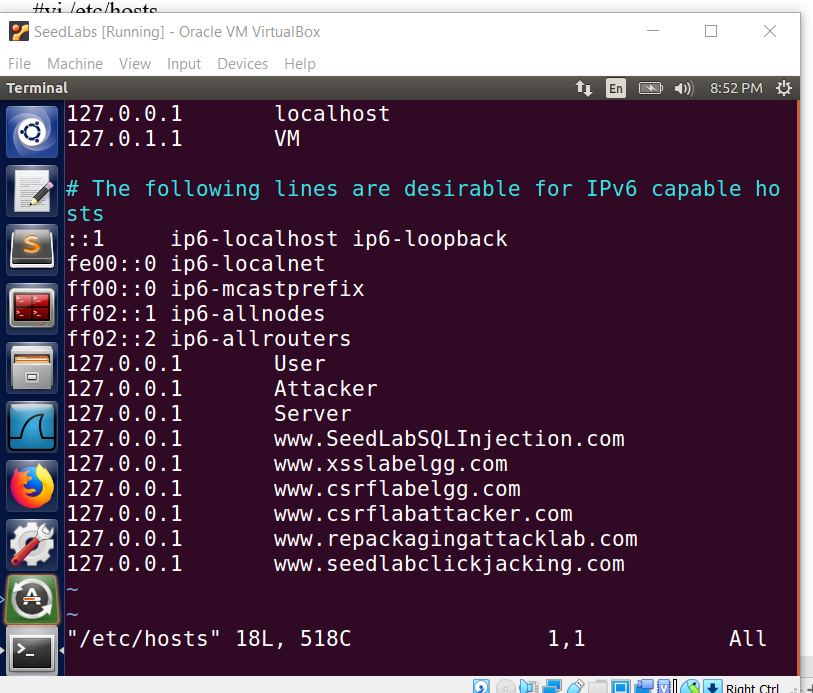
**MSSV:** 20110635 lớp sáng thứ 3

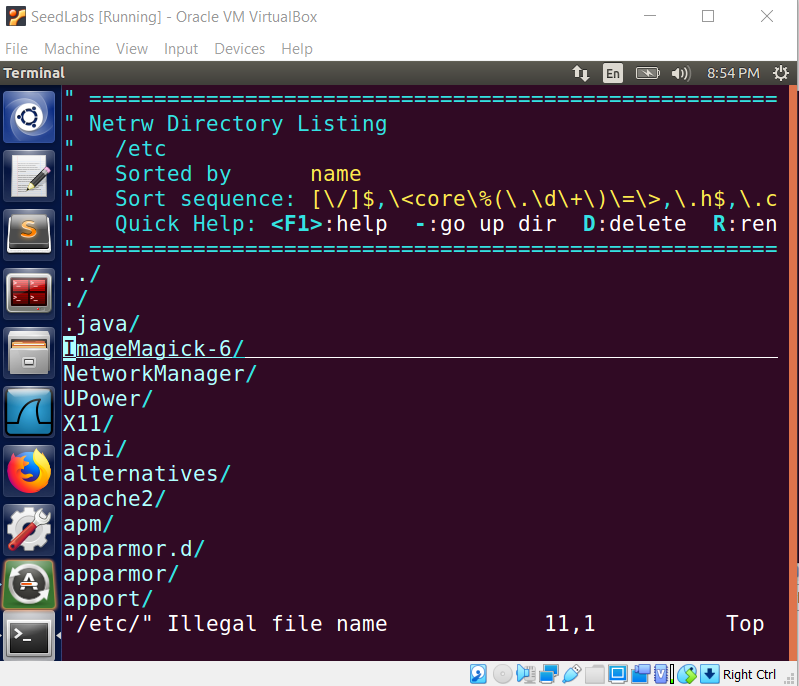
**Lab 5. SQL Injection**

1. **Lab environment**

URL: <http://www.SEEDLabSQLInjection.com>

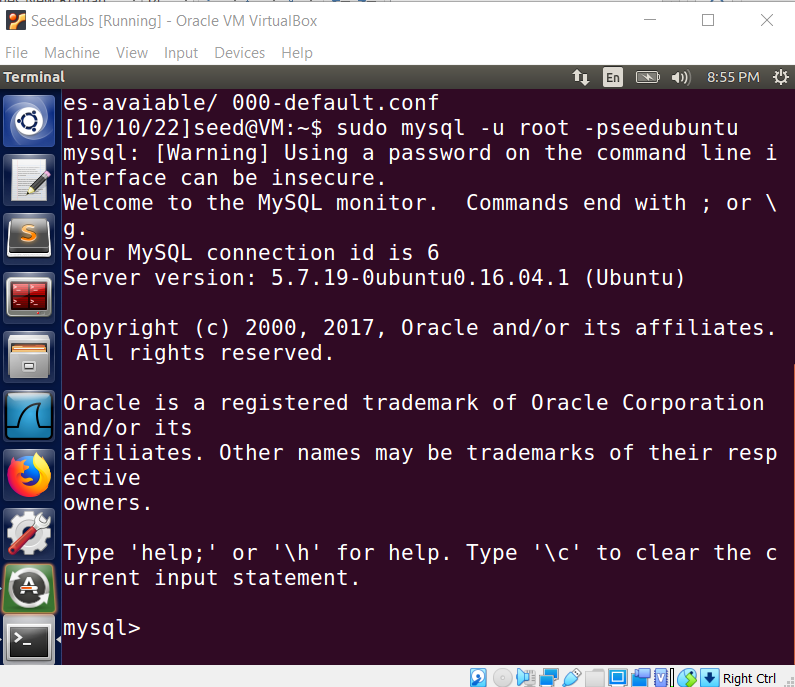
Folder: /var/www/SQLInjection



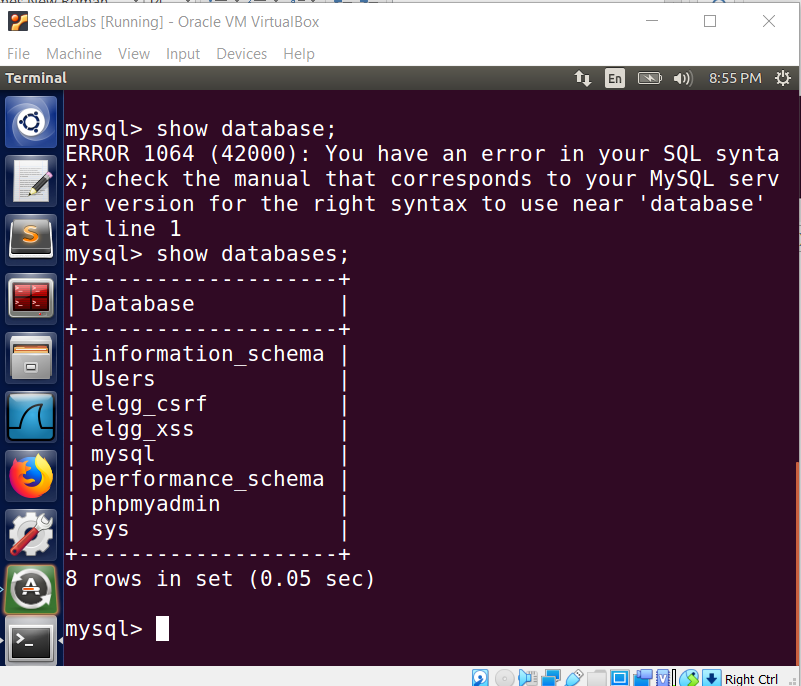


1. **Làm quen với các câu lệnh mysql**

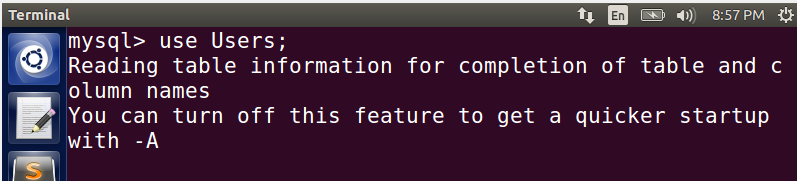
Sử dụng lệnh: mysql -u root -pseedubuntu để sử dụng mysql



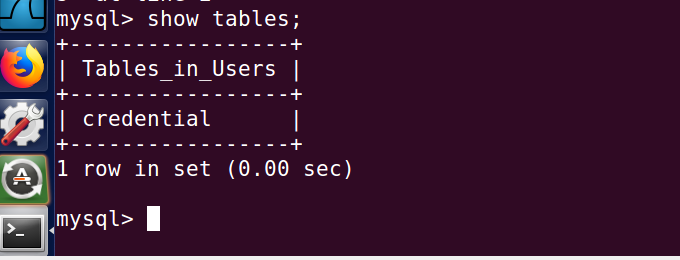
Show databases; // để xem các database trong hệ thống



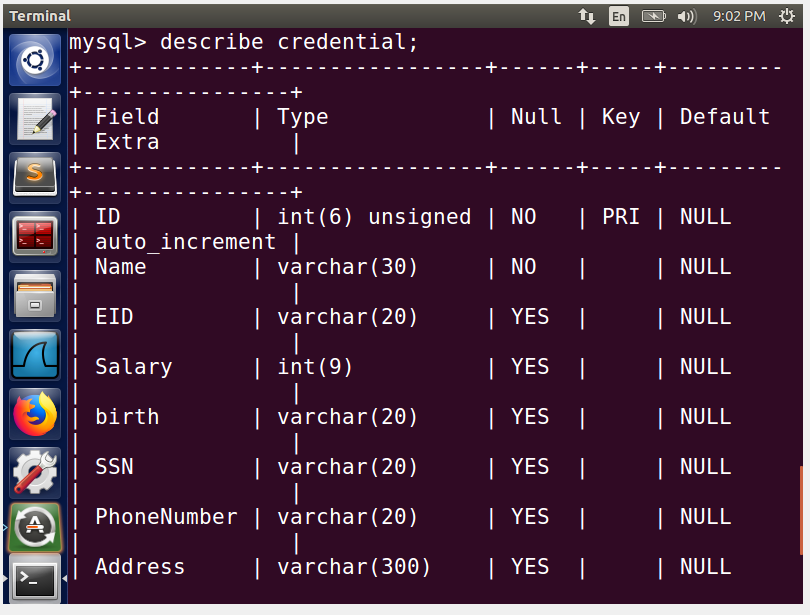
Use <database\_name> ; // sử dụng database đó



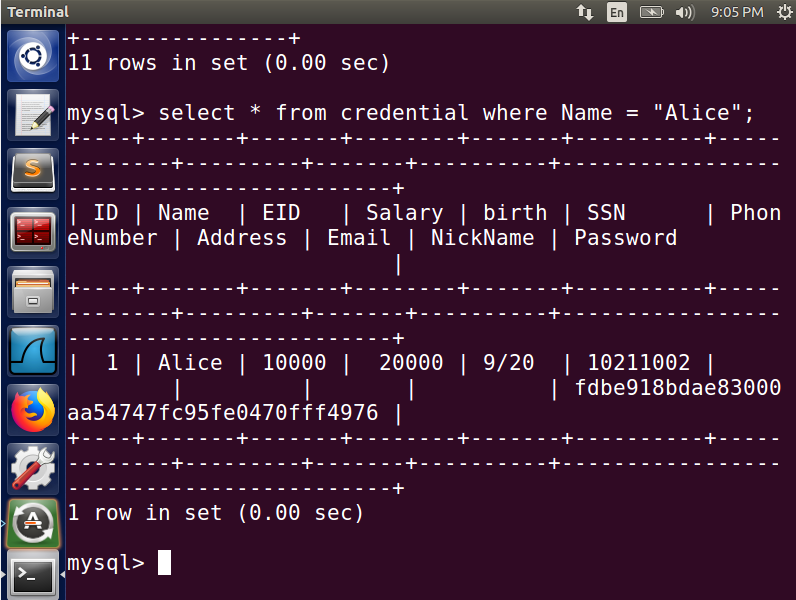
Trong bài này, ta sẽ sử dụng database Users

Dùng lệnh show tables; // xem các bảng trong database ta đang use

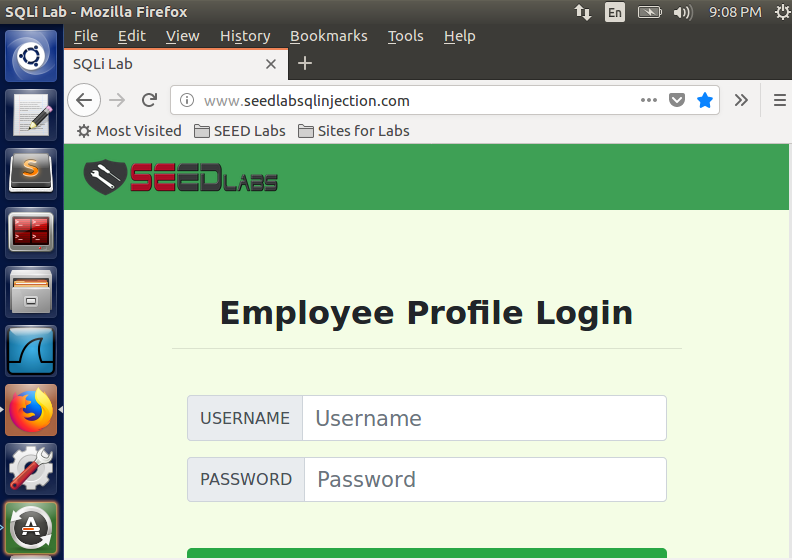
Lệnh describe <table\_name> ; // xem thông tin của bảng



Lệnh select để xem dữ liệu toàn bộ dữ liệu của Alice

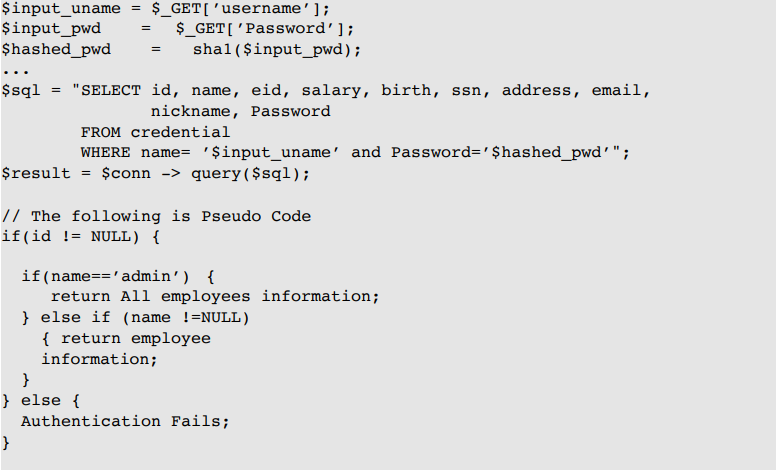


1. **Sử dụng SQL Injection để truy cập vào hệ thống**



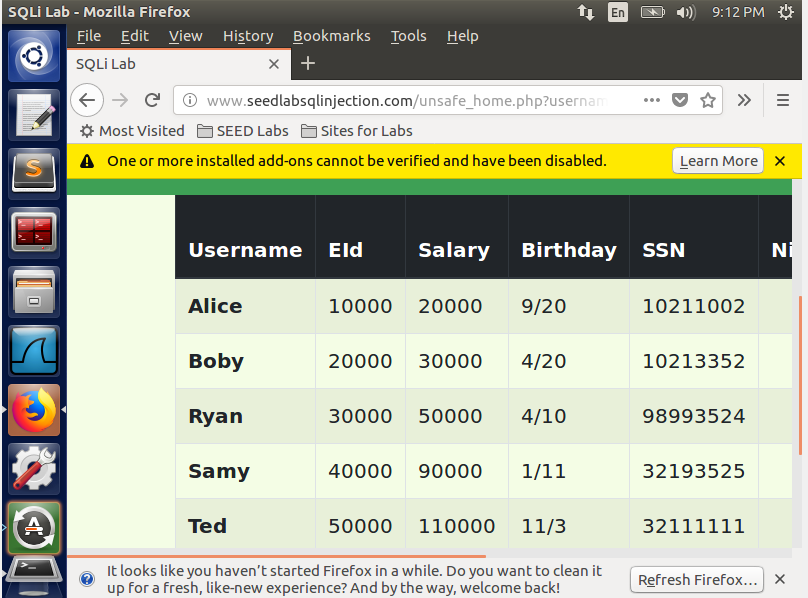
Cách Sql injection có thể hoạt động:

Dự đoán câu lệnh mysql kiểm tra login của hệ thống

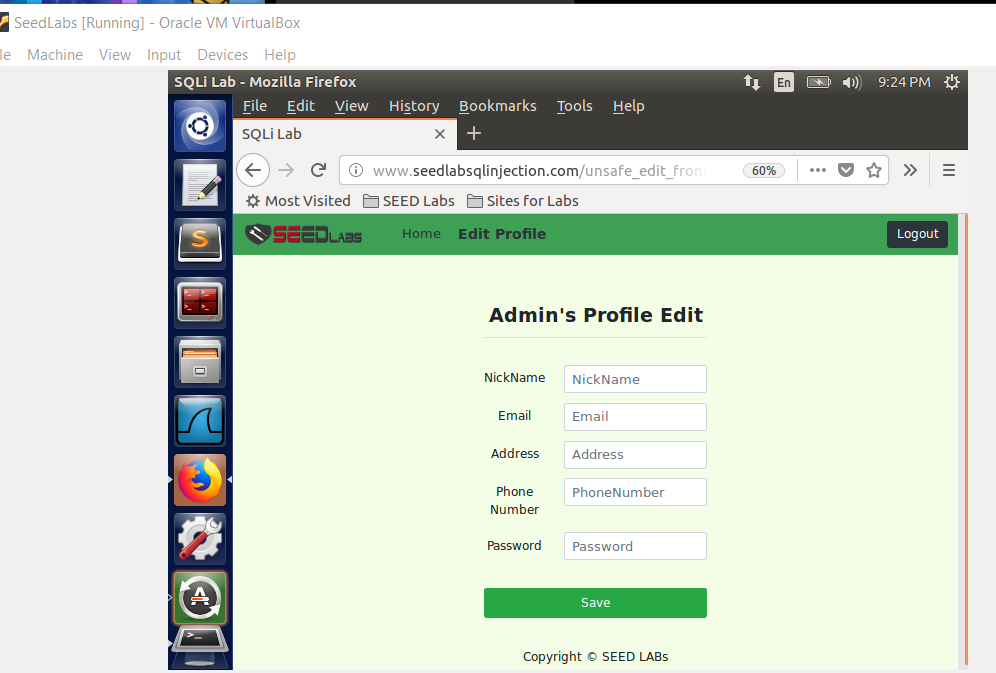


Câu lệnh SQL trên chọn những thông tin cá nhân như id, name, salary, ssn,… từ credential table. Câu lệnh SQL sử dụng 2 biến input uname và hasged\_pwd. Input\_uname giữ một chuỗi được định nghĩa bởi người dùng trong trường username của phần login trên page, trong khi hashed\_pwd giữ SHA-1 được định nghĩa bởi người dùng. Chúng ta giả sử biết tên của administrator’s account name là admin nhưng chúng ta không biết password. Để tấn công, đăng nhập với username là admin’# để xem toàn bộ thông tin của nhân viên.

1. SQL Injection attack from webpage



1. **Sử dụng câu lệnh update injection để sửa đổi thông tin hệ thống**



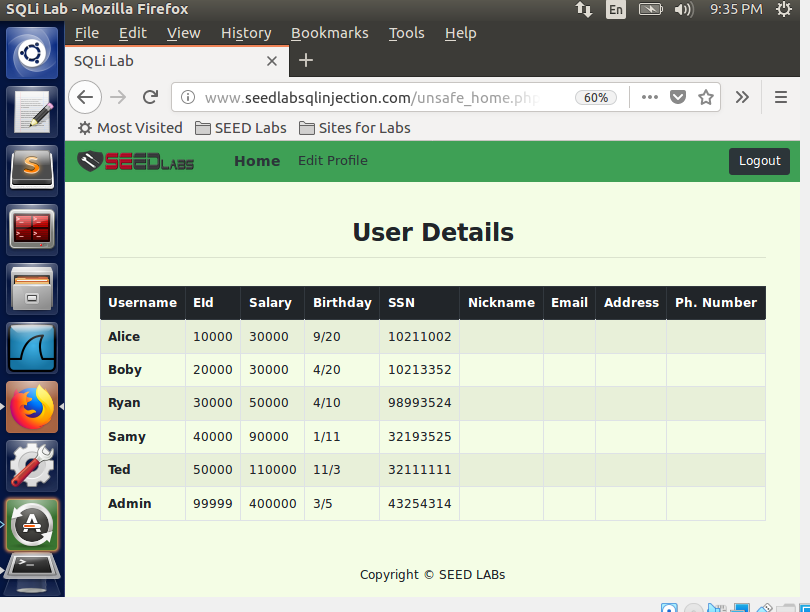
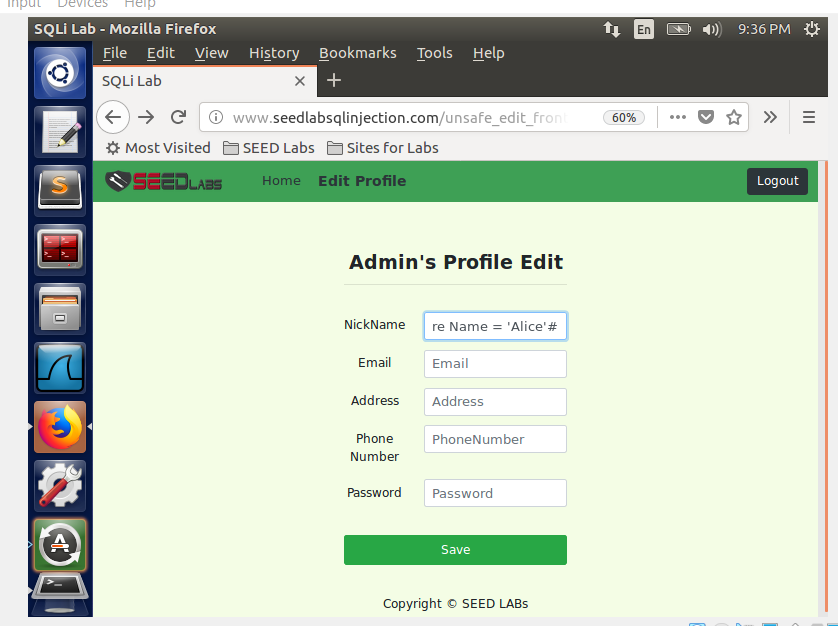
Câu lệnh update của hệ thống

Text, letter

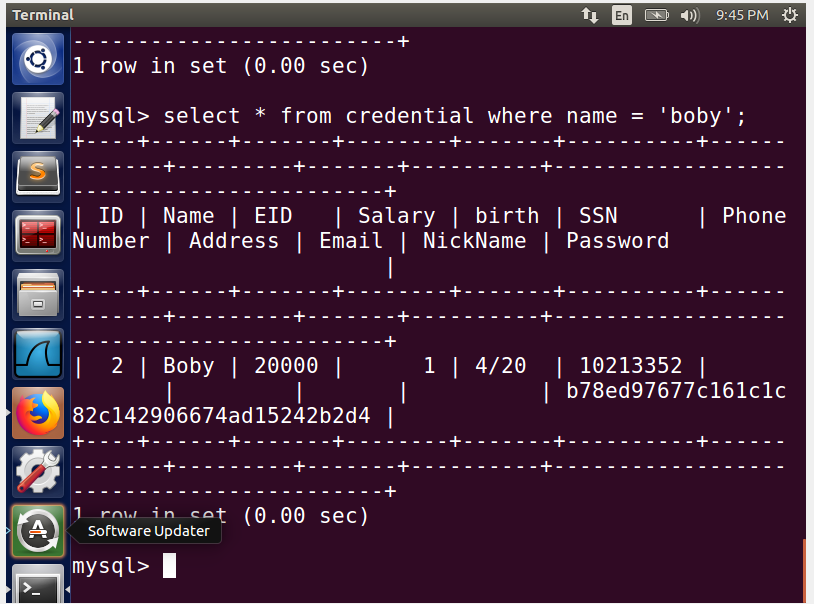
Description automatically generated

**Ta sẽ thử update lương của Alice từ 20000 lên 30000**

Cú pháp: ‘, salary = 30000 where Name = ‘Alice’ #

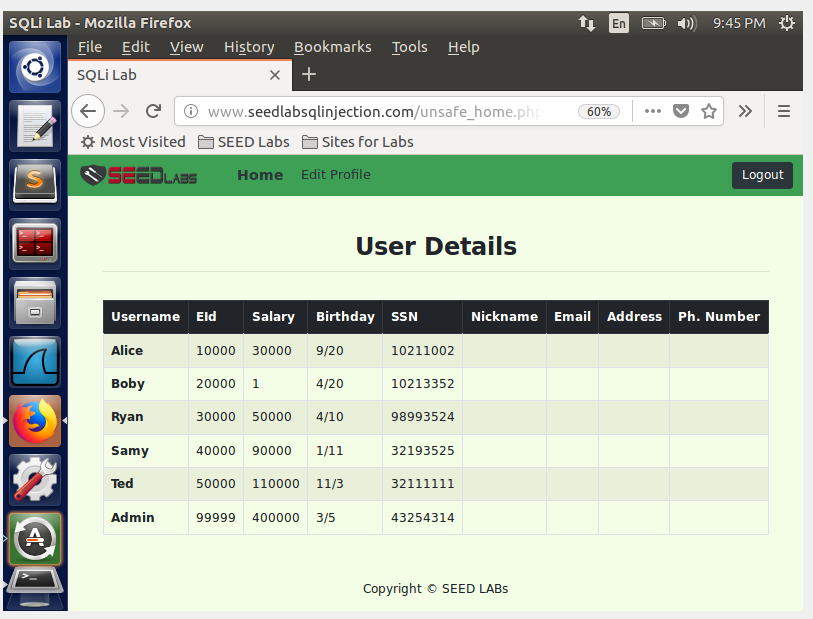


Trừ lương của sếp còn 1 dollar



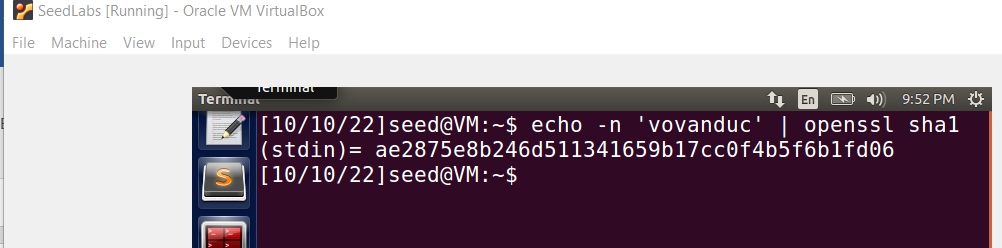
* Sếp có ID = 2

Cú pháp: ‘, salary = 1 where ID = 2 #

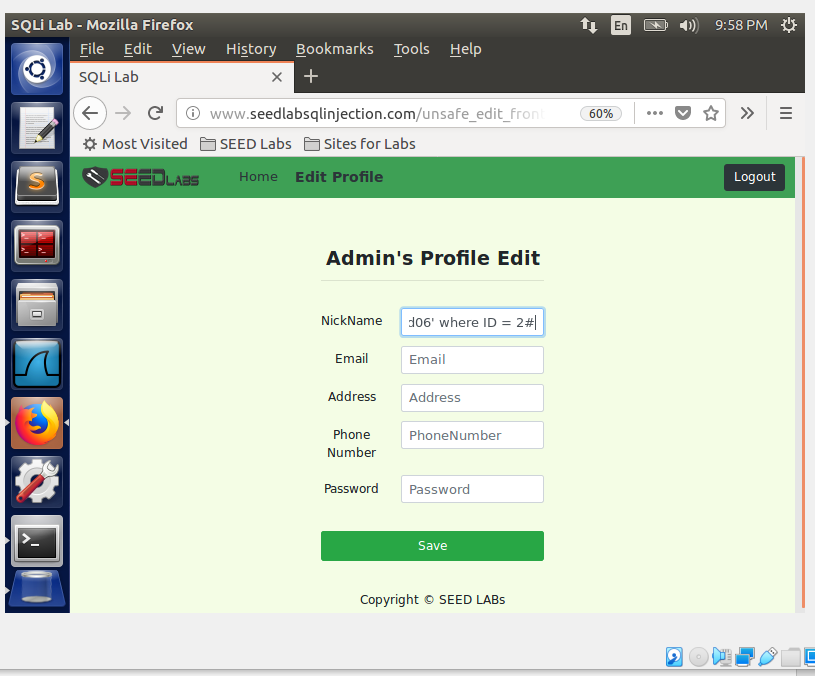


**Giờ ta sẽ thử thay đổi password của user alice**

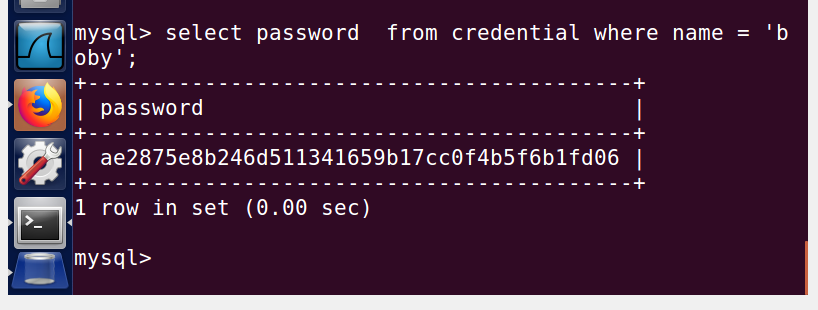
Mật khẩu đã bị mã hoá theo SHA1 nên chúng ta giải mã.

Với pass là vovanduc ta sẽ dùng công cụ để mã hóa sha1:

Ta sẽ copy đoạn mã hóa và thực hiện



Ta kiểm tra kết quả trong database



Ta thấy pass đã được cập nhật. Ta sẽ thử đăng nhập trên hệ thống.

