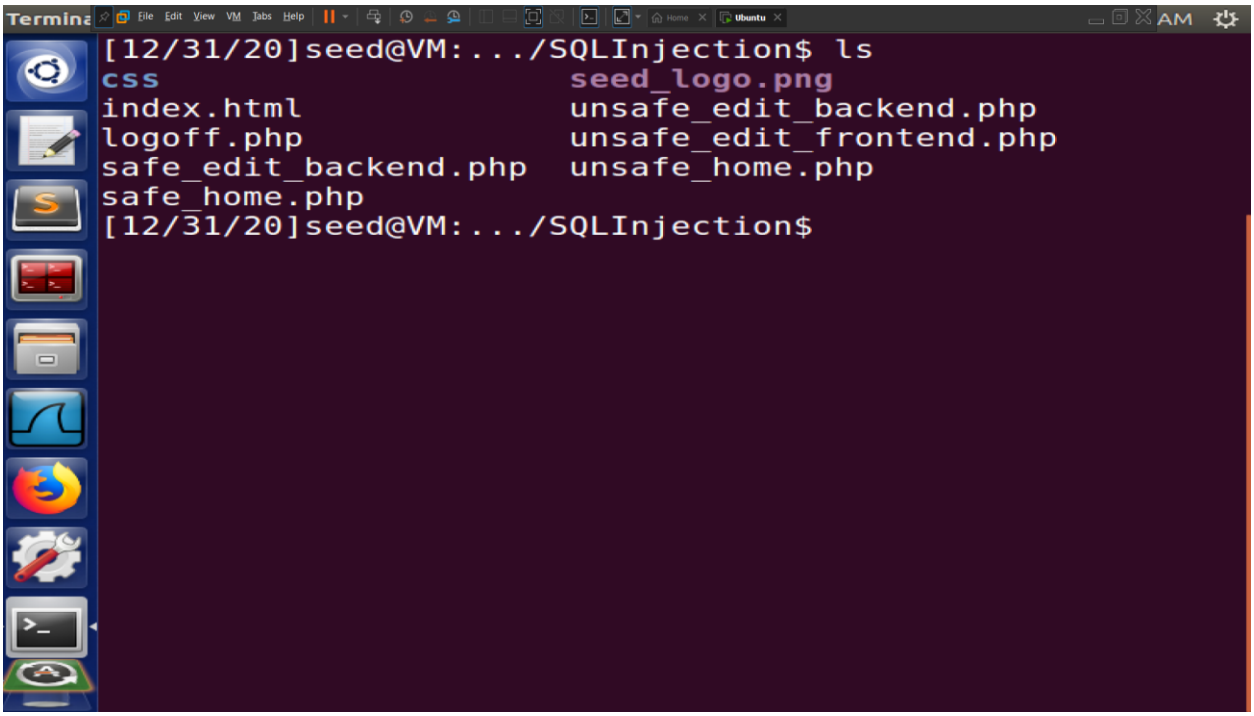
Tên: Nguyễn Minh Hiền

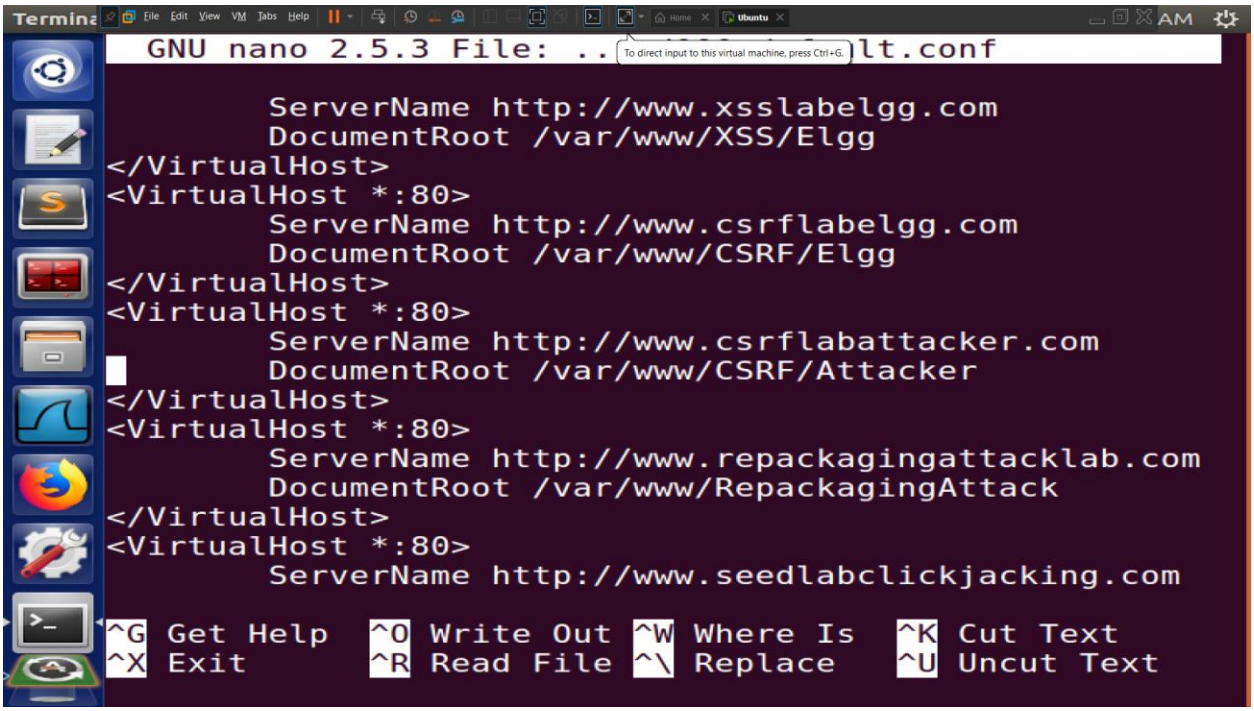
MSSV: 1712425

BÁO CÁO BÀI LAB SỐ 05

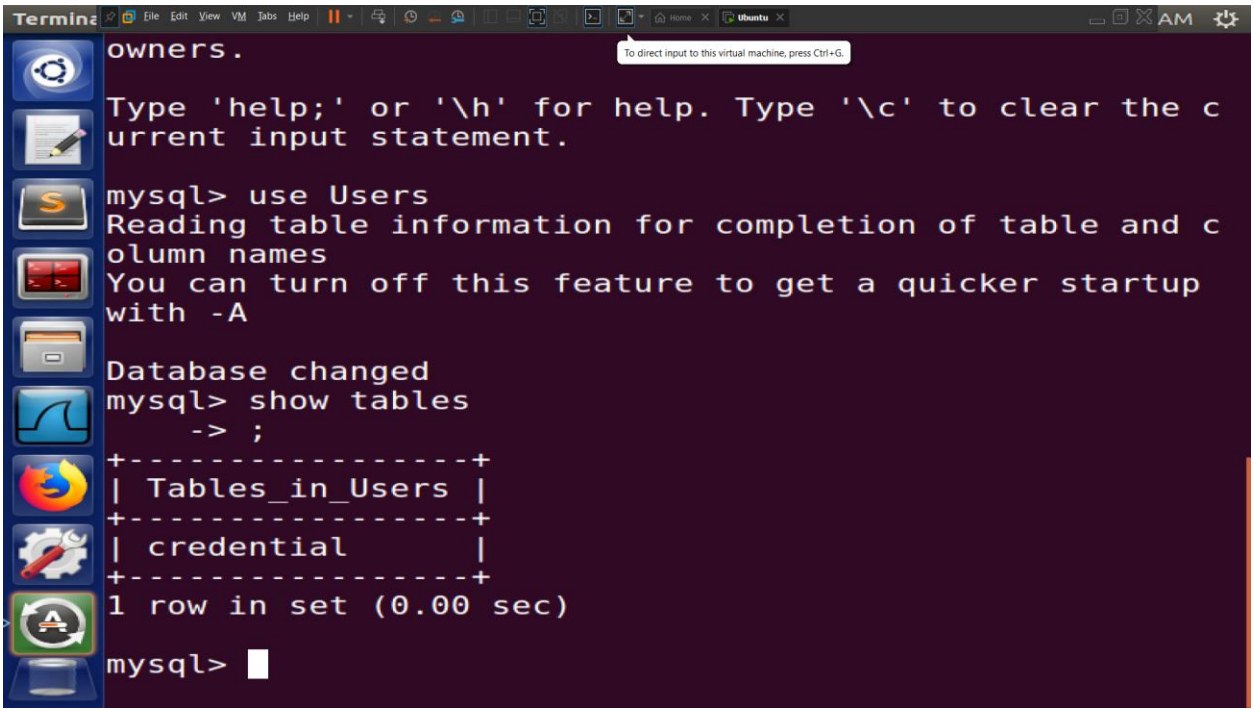
I. SQL Injection

1. Xem xét môi trường làm việc

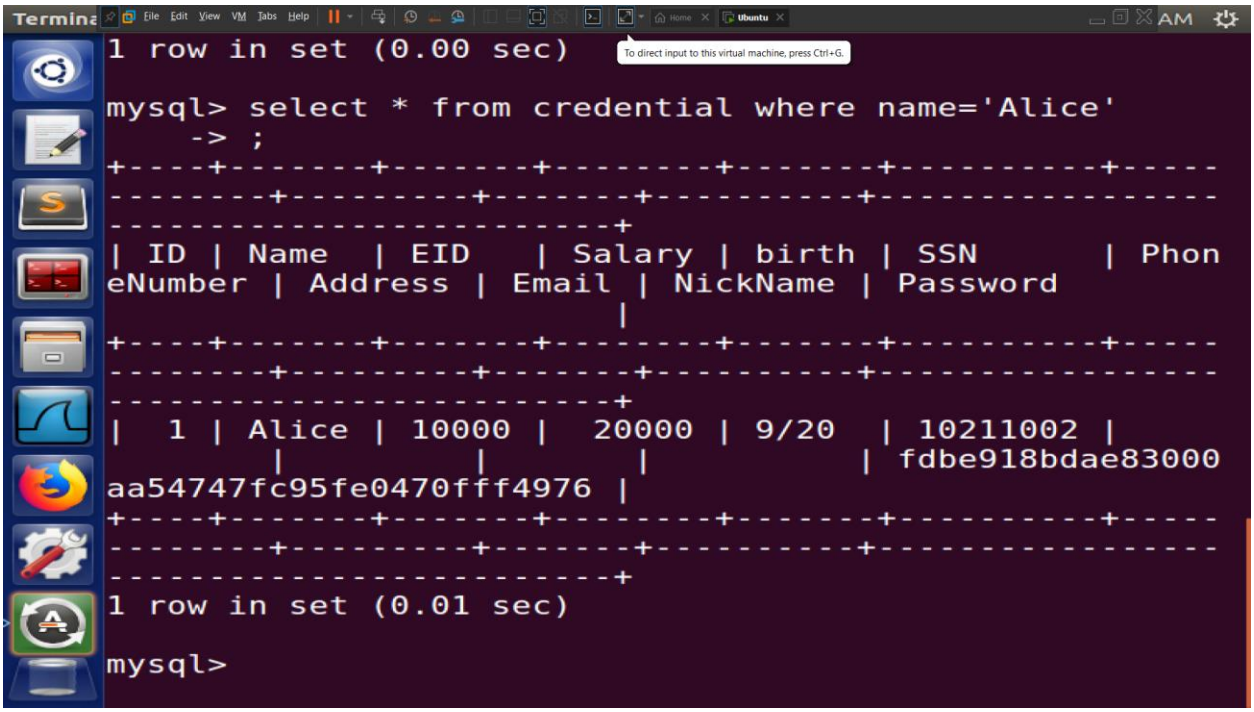




2. Làm quen với câu lệnh SQL

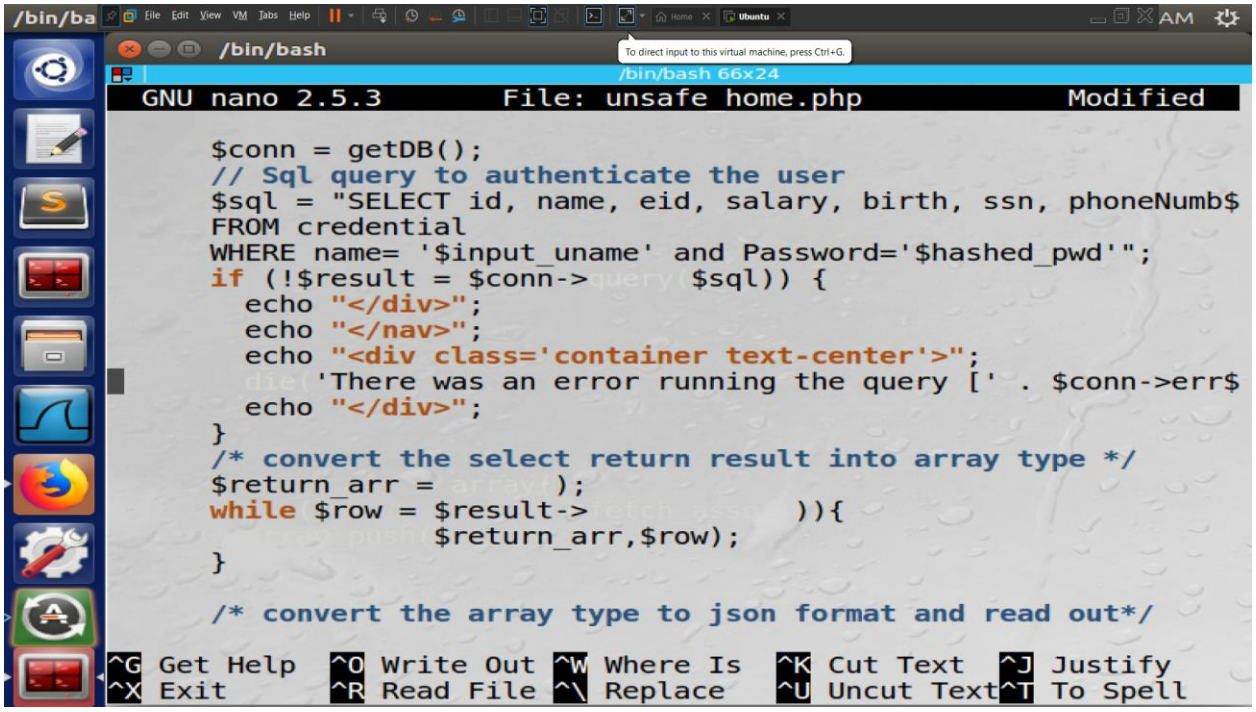


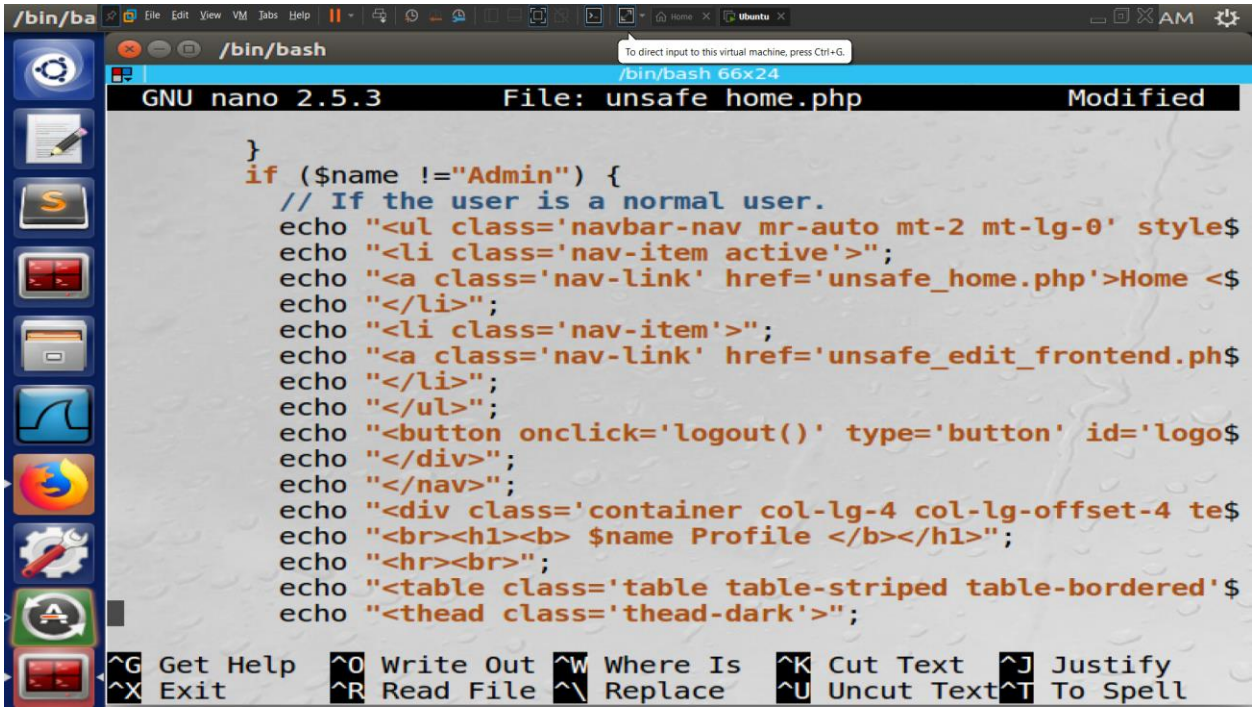
- In thông tin hồ sơ của nhân viên Alice



3. Tấn công SQL Injection dựa trên câu lệnh SELECT

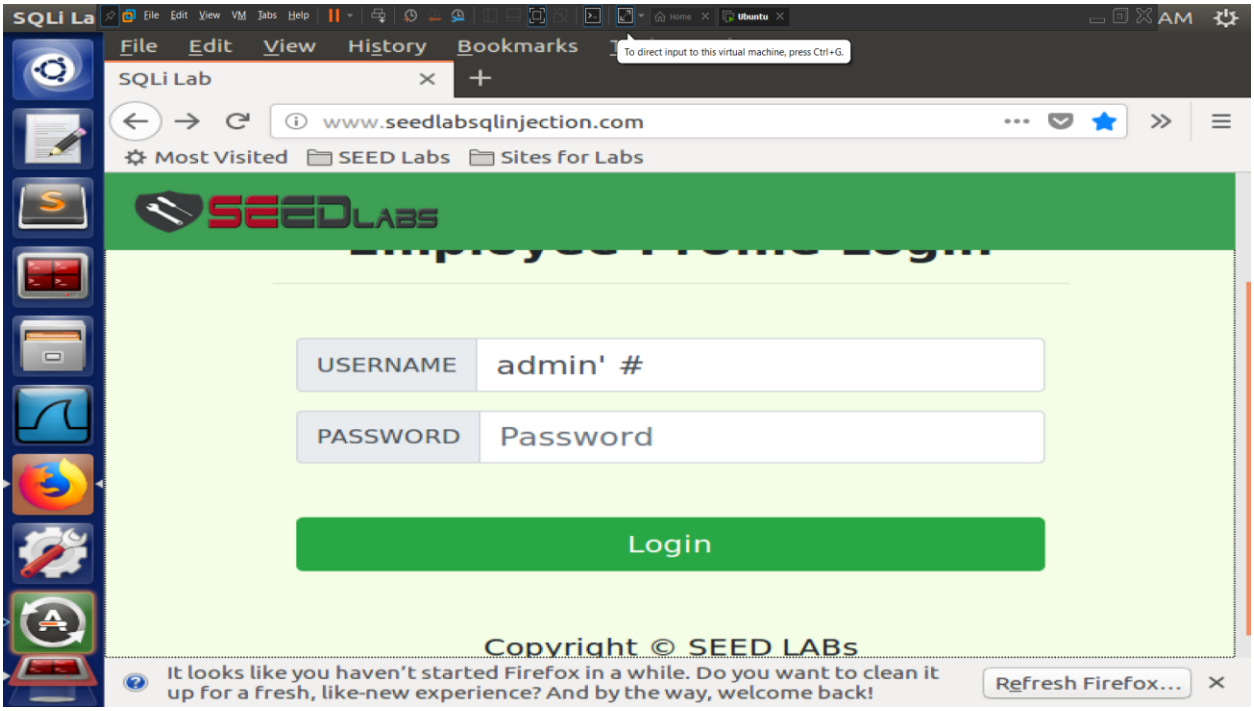
- Lấy tài khoản admin bằng mã PHP home.php không an toàn nằm trong thư mục var/www/SQLInjection



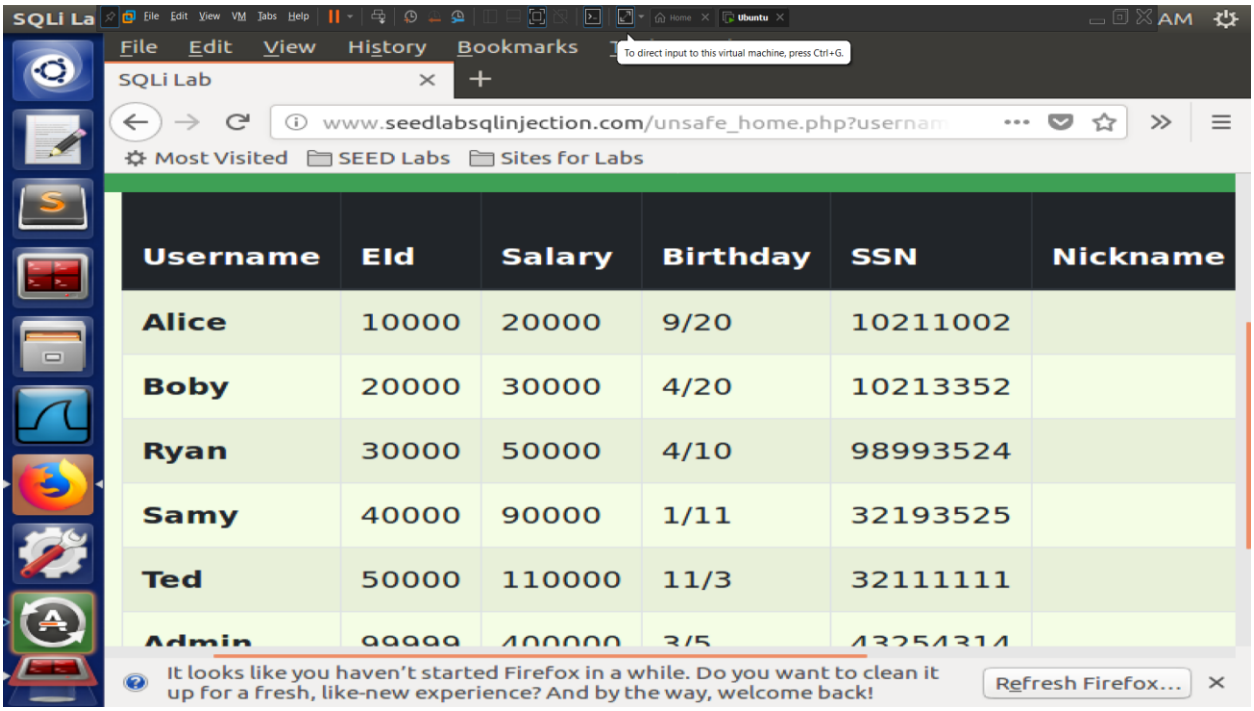


4. Tấn công SQL Injection từ trang web

- Đăng nhập vào trang web bằng tài khoản admin lấy được



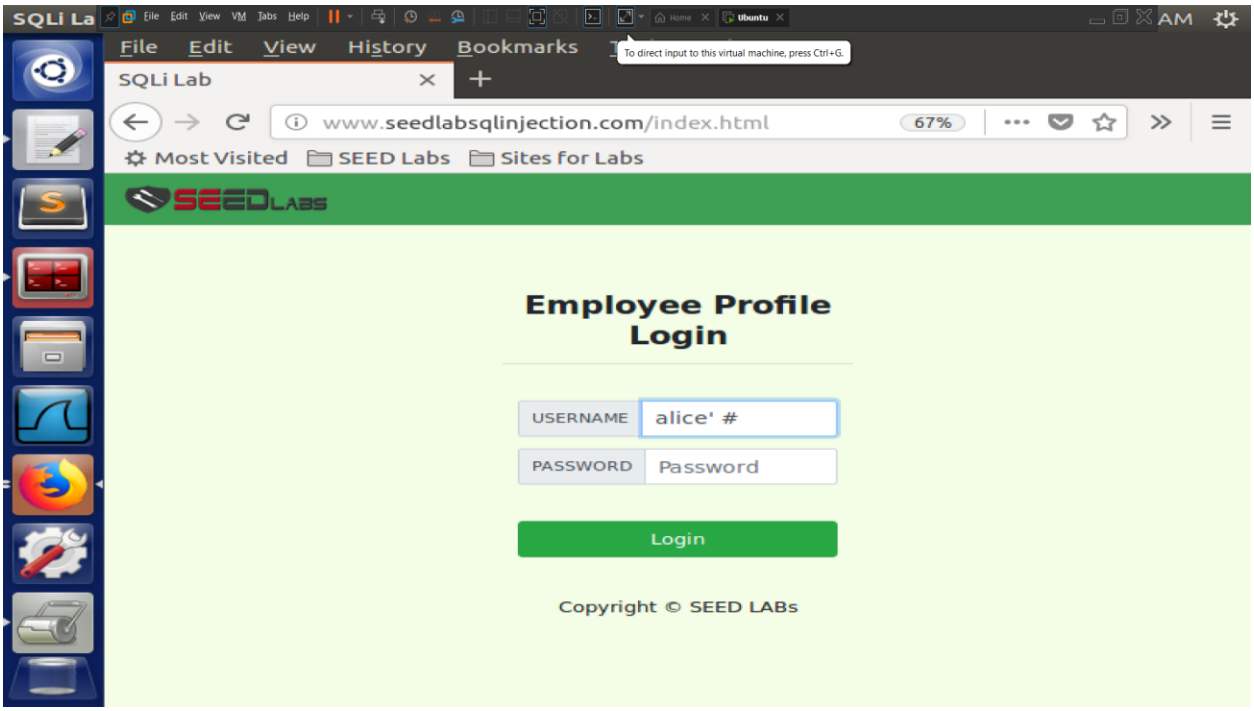
- Lấy được thông tin của tất cả các nhân viên



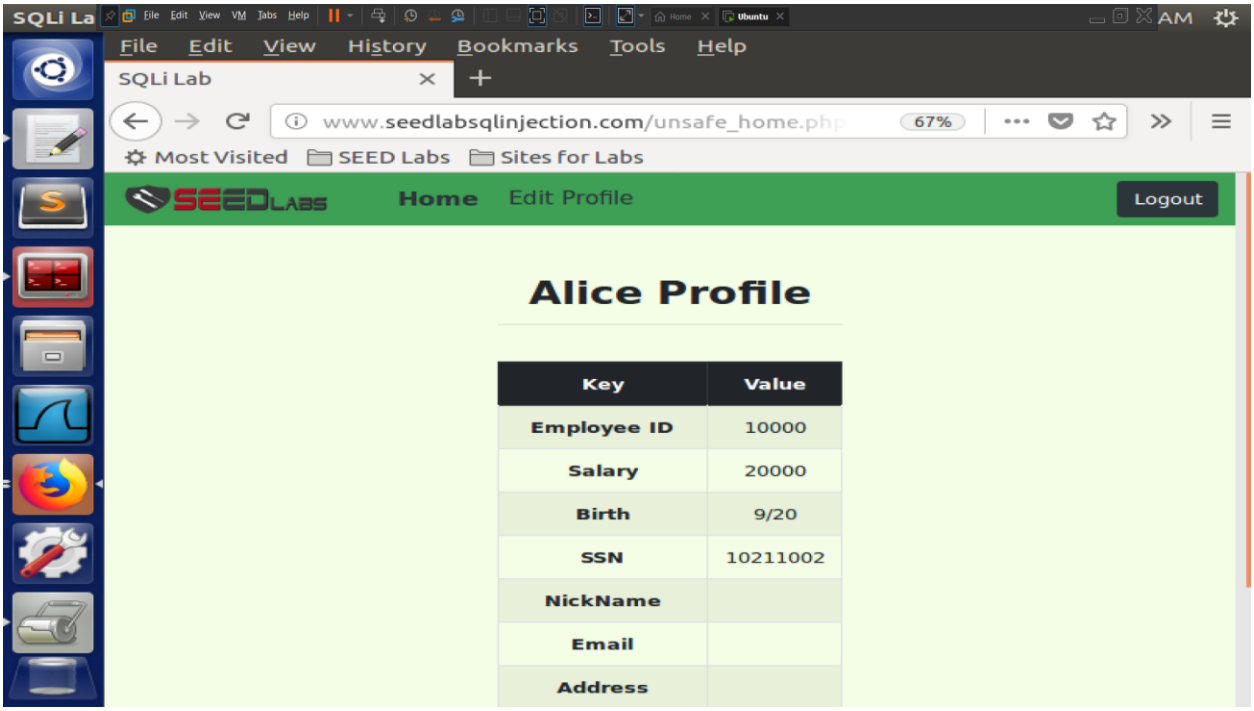
5. Tấn công SQL Injection dựa trên câu lệnh UPDATE

5.1 Chỉnh sửa thông tin nhân viên "Alice" từ trang web

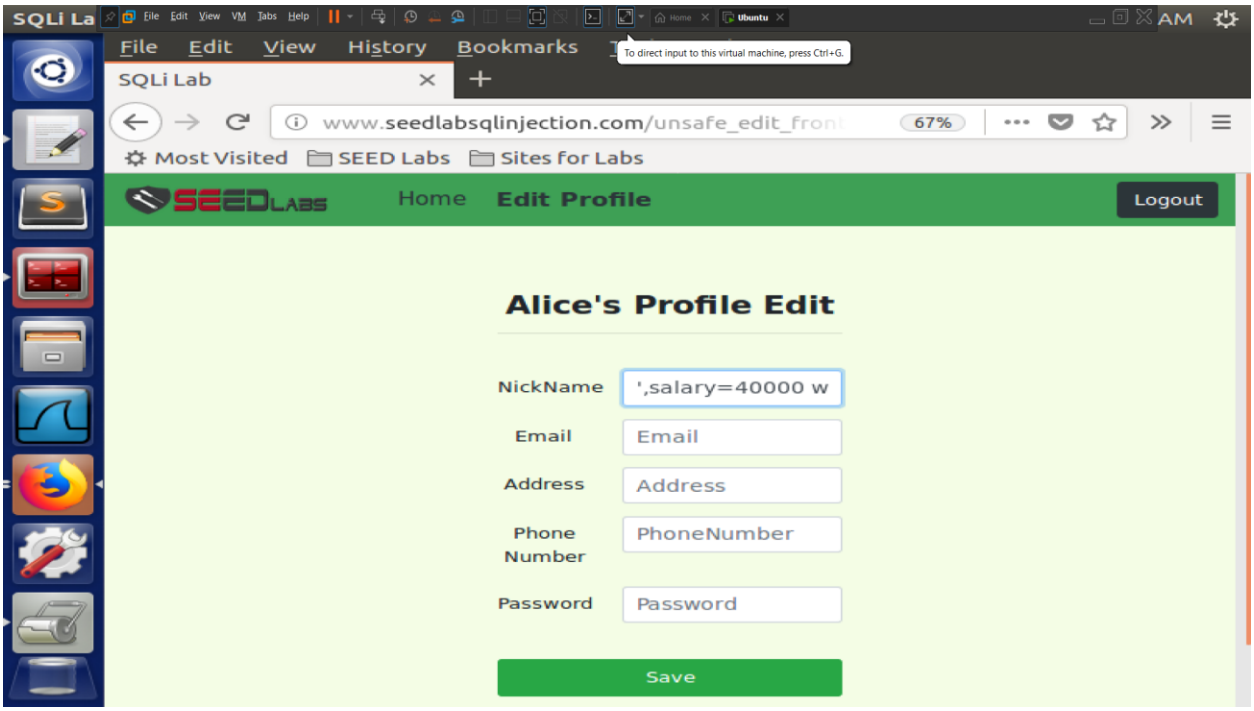
- Đăng nhập vào tài khoản nhân viên Alice:



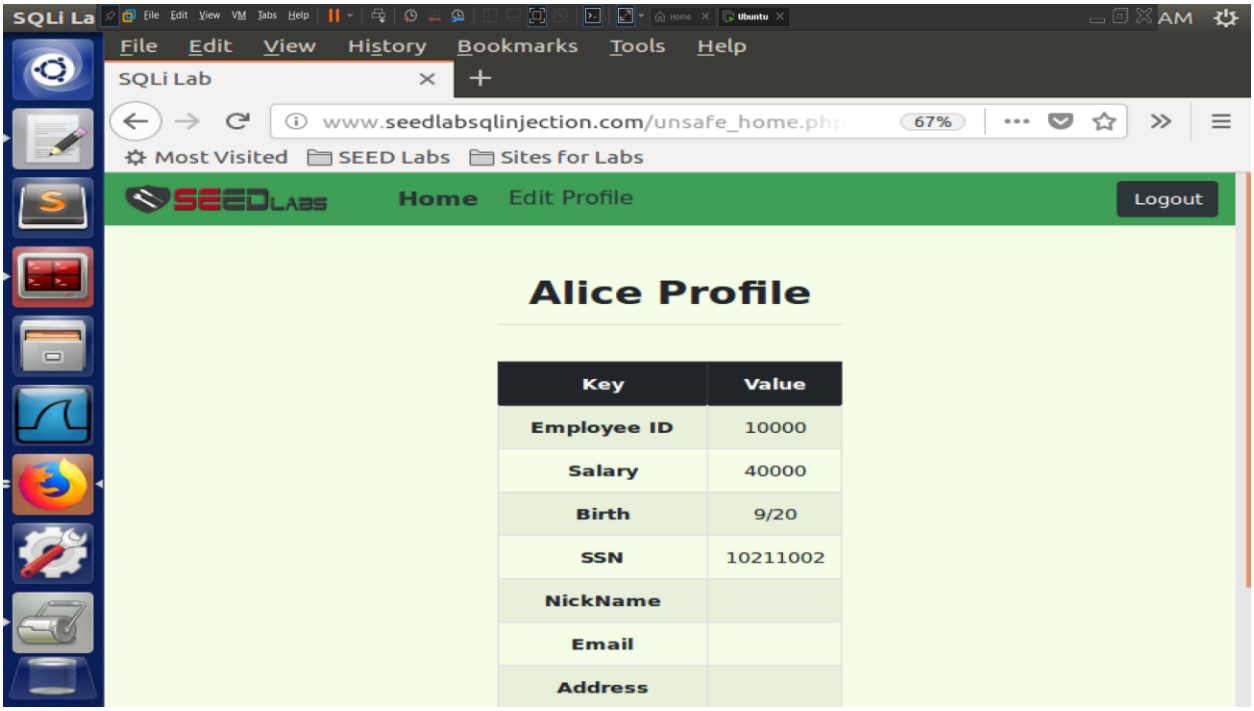
- Lương ban đầu là 20000



- Sửa lương thành 40000
  - Điền vào ô NickName: ***',salary=40000 where EID=10000;#***

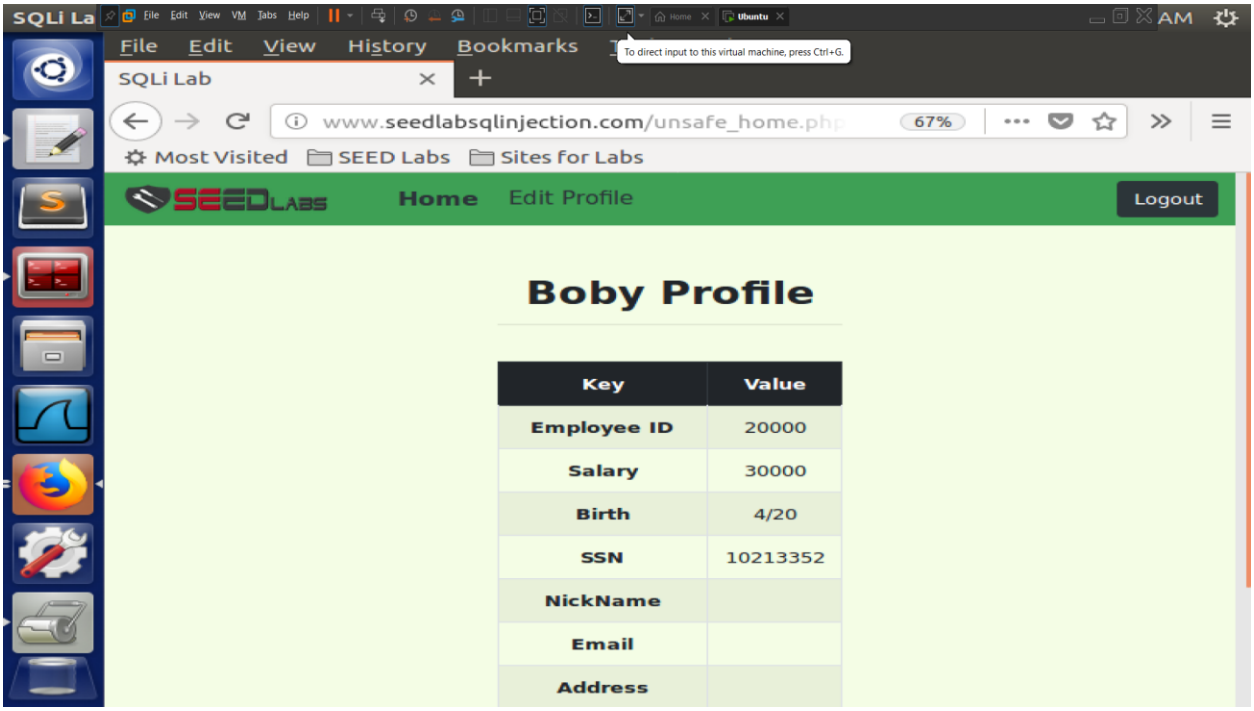

File Edit View History Bookmarks
To direct input to this virtual machine, press Ctrl+G.
SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_front
67%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Alice's Profile Edit
NickName
',salary=40000 w
Email
Email
Address
Address
Phone Number
PhoneNumber
Password
Password
Save

- Kết quả

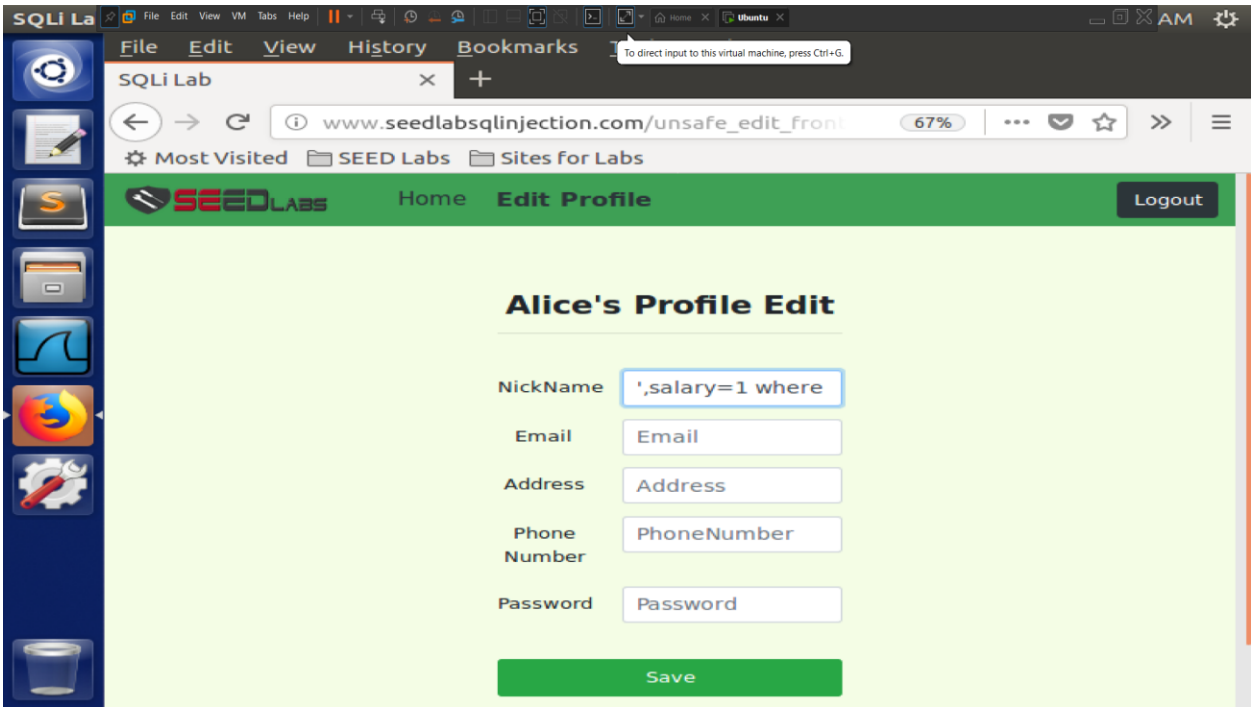

File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
67%
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Alice Profile
Key
Value
Employee ID
10000
Salary
40000
Birth
9/20
SSN
10211002
NickName
Email
Address

5.2 Trừng phạt ông chủ Boby bằng cách giảm lương xuống 0

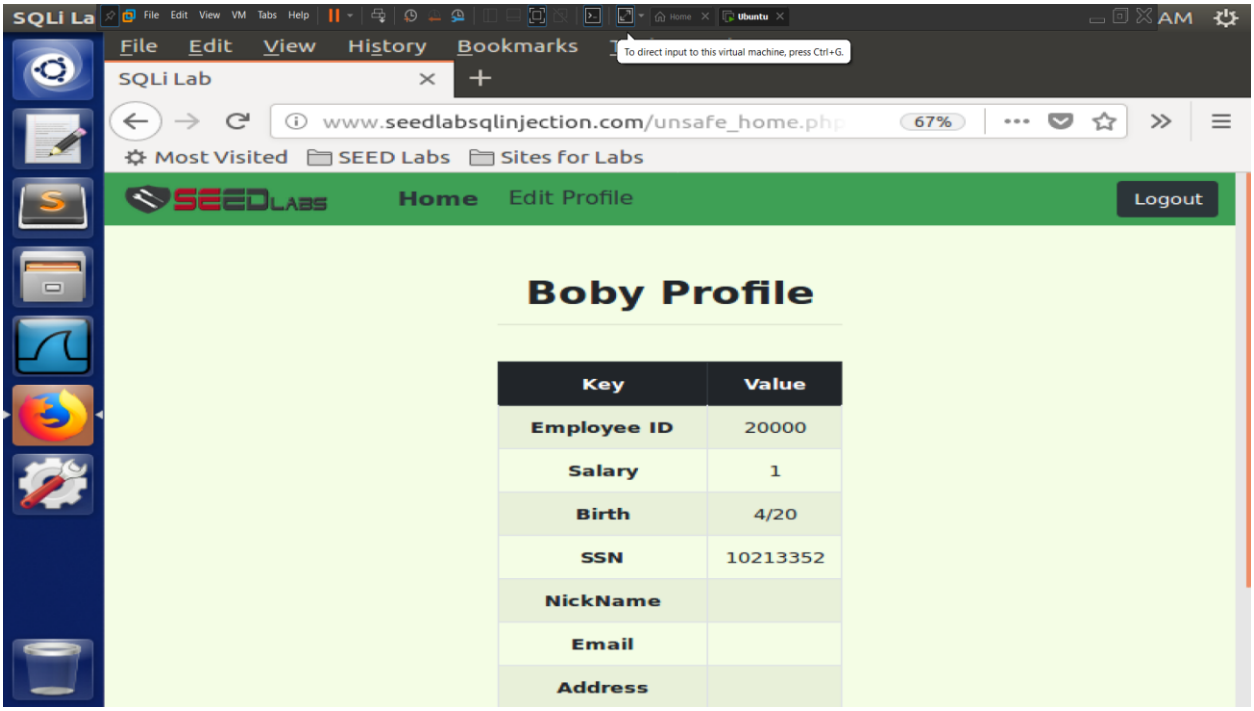
- Vào tài khoản Boby xem mức lương hiện tại và EID



- Vào tại tài khoản của Alice và bắt đầu chỉnh sửa lương của Boby
  - Điền vào ô NickName: ***',salary=1 where EID=20000;#***

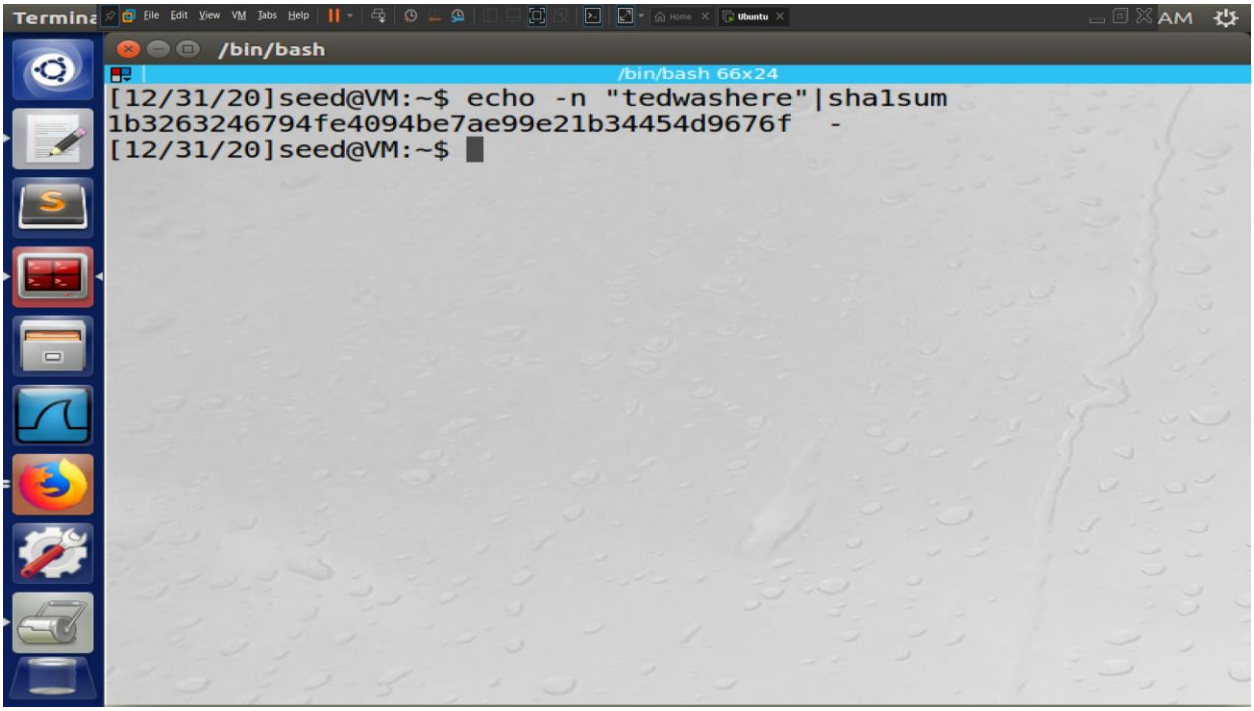

SQLi Lab
www.seedlabsqlinjection.com/unsafe_edit_front
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Alice's Profile Edit
NickName
',salary=1 where
Email
Email
Address
Address
Phone Number
PhoneNumber
Password
Password
Save

- **Kết quả**

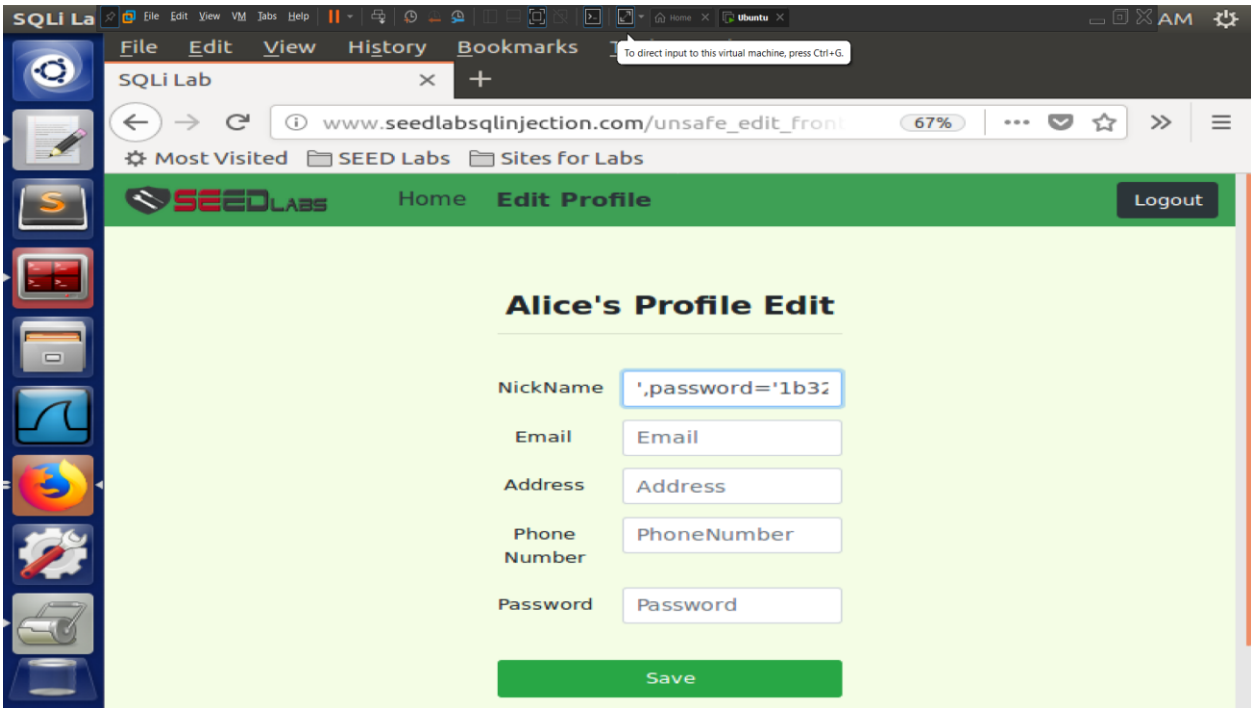

SQLi Lab
www.seedlabsqlinjection.com/unsafe_home.php
Most Visited
SEED Labs
Sites for Labs
Home
Edit Profile
Logout
Boby Profile
Key
Value
Employee ID
20000
Salary
1
Birth
4/20
SSN
10213352
NickName
Email
Address

5.3 Đổi password của Boby

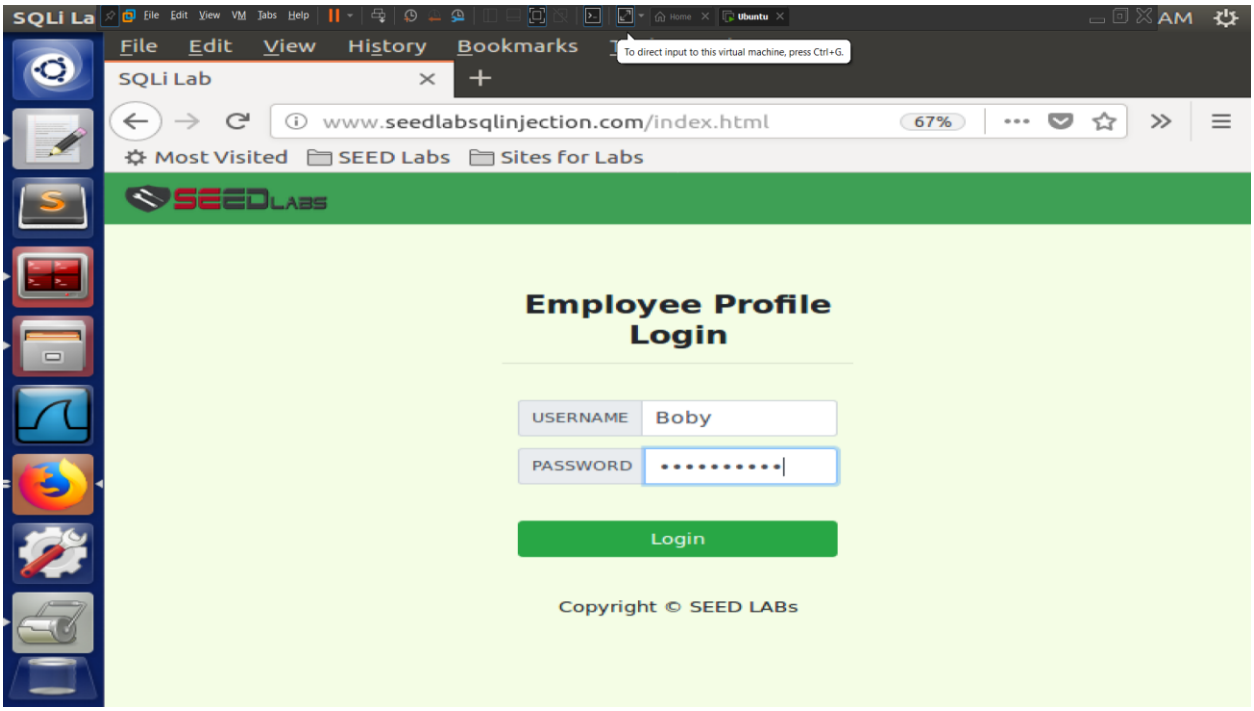
- Tìm password của Boby



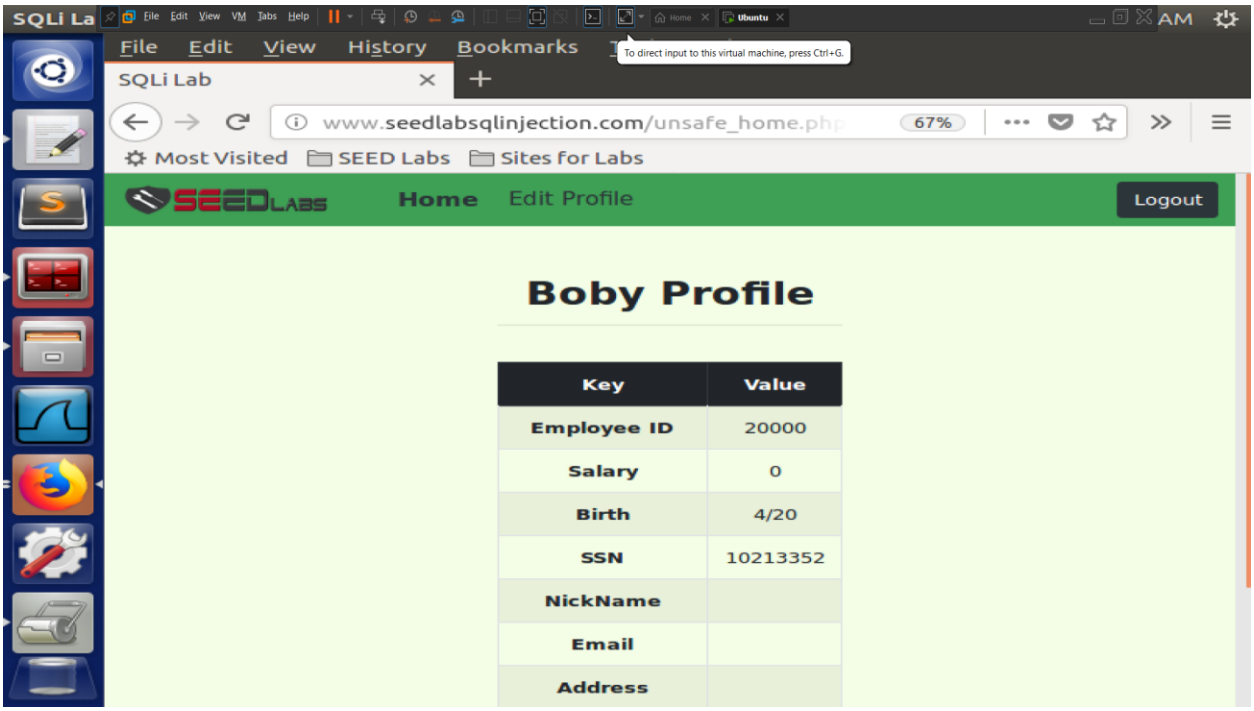
- Vào tài khoản Alice để đổi password sau đó save lại



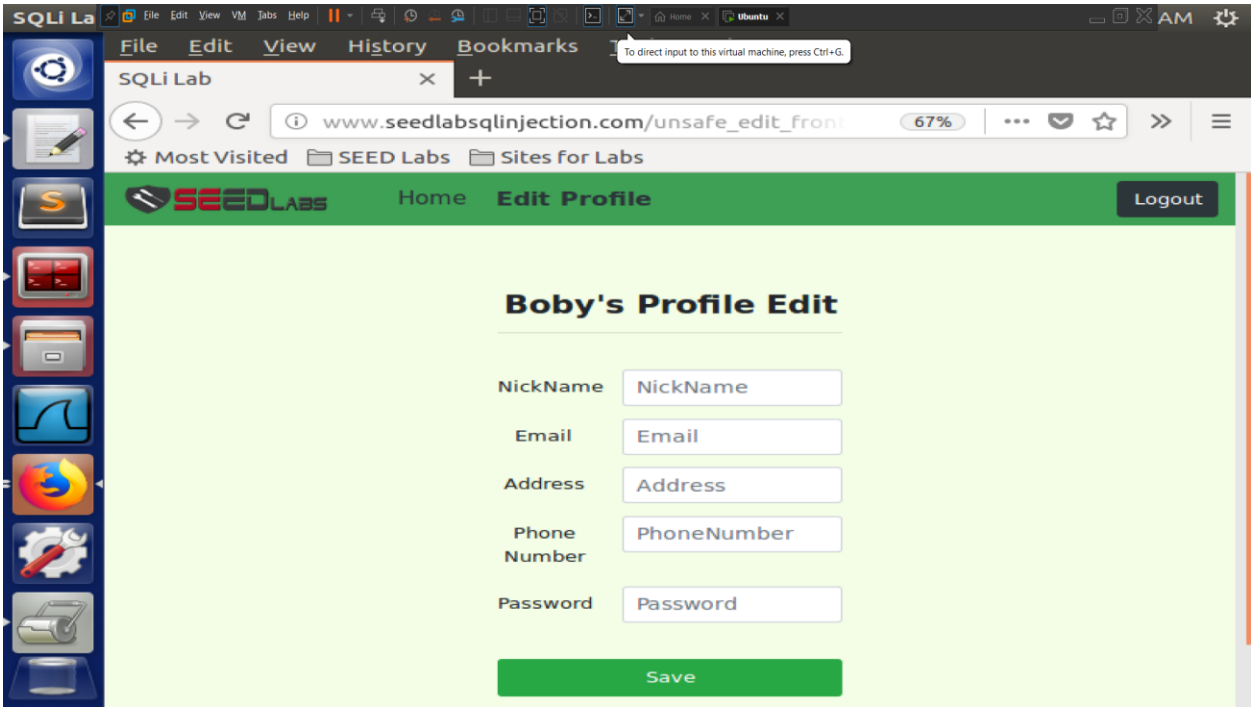
- Giờ chúng ta đã có thể đăng nhập vào tài khoản của Boby
  - USERNAME: **Boby**
  - PASSWORD: **tedwashere**



- Kết quả



- Giờ ta có thể thay đổi mật khẩu của Boby tùy thích



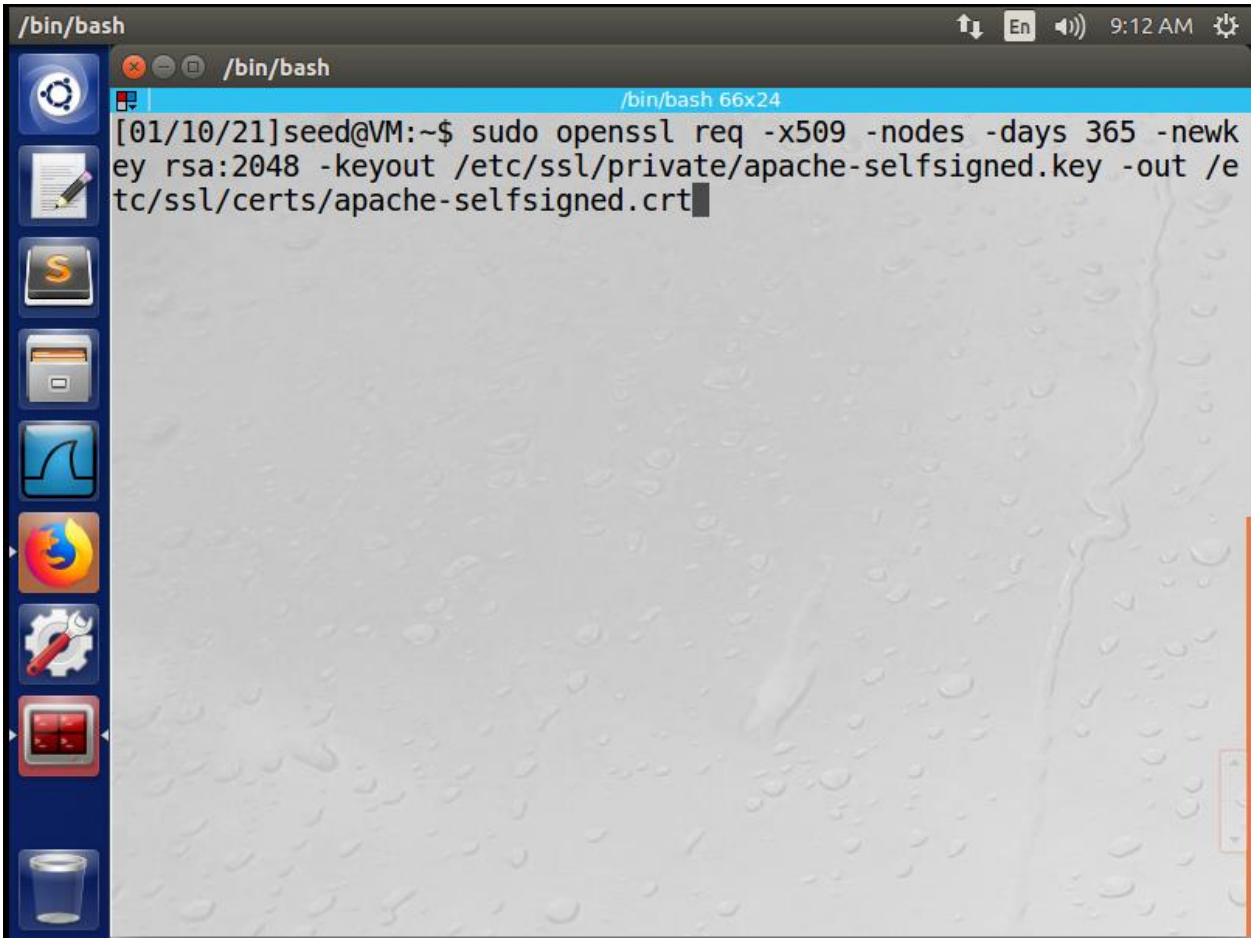
II. Sử dụng openSSL để tạo CA cho máy chủ web dùng apache trên Linux

Nguồn tham khảo: *https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-18-04*

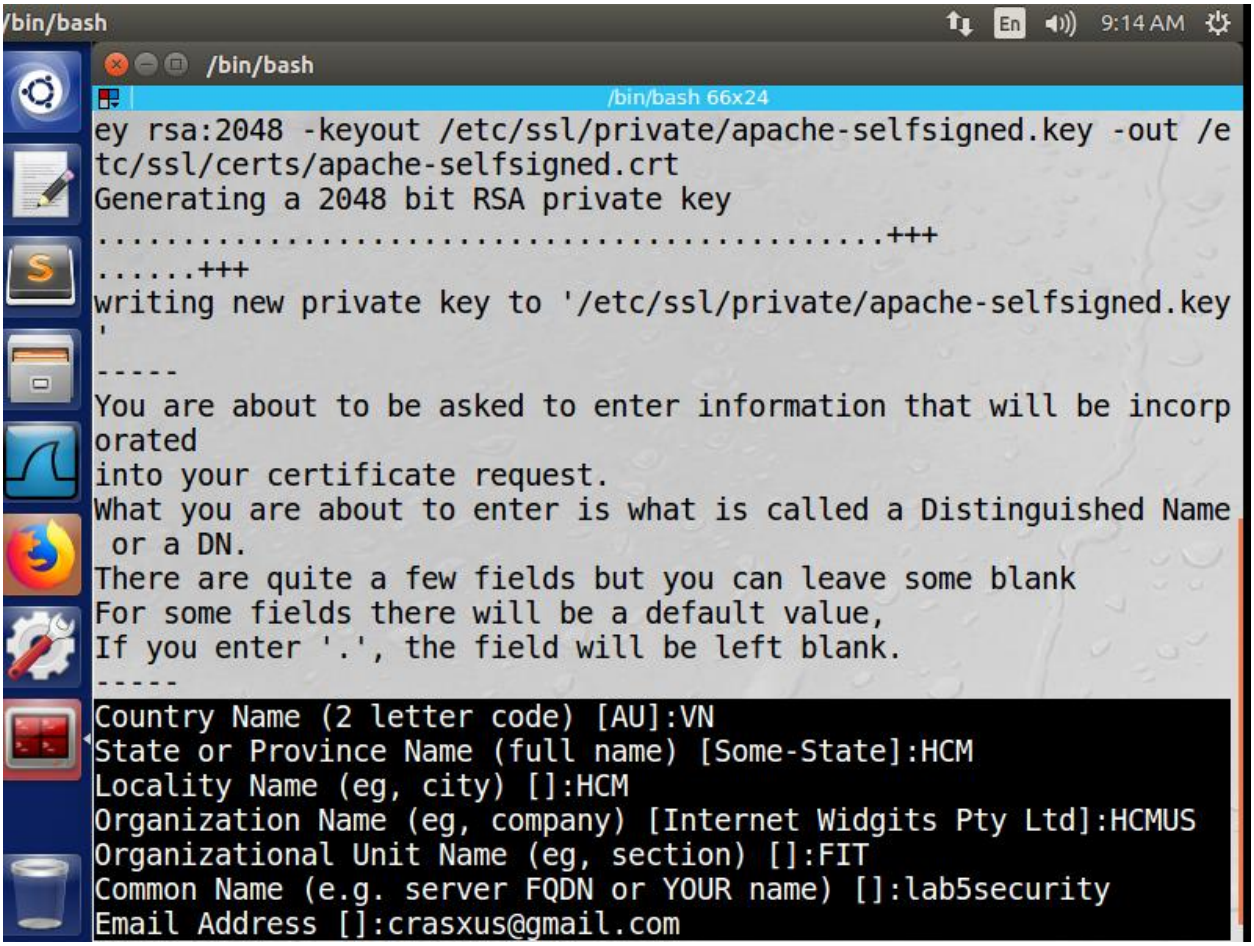
1. Tạo 1 CA bằng openSSL

1.1 Tạo file key và file crt

Câu lệnh: *sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt*

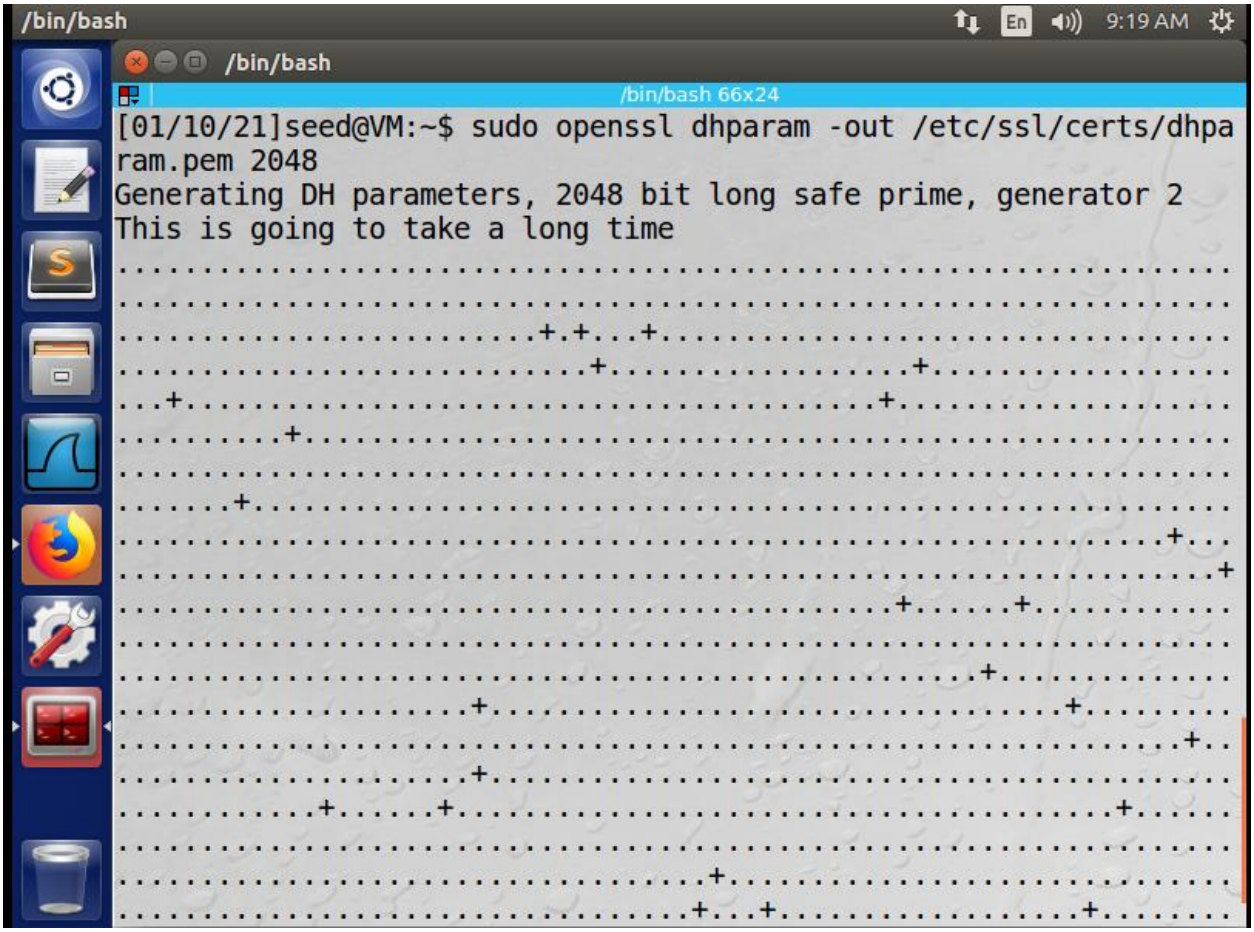


- **Điền thông tin**



1.2 Tạo file dhparam

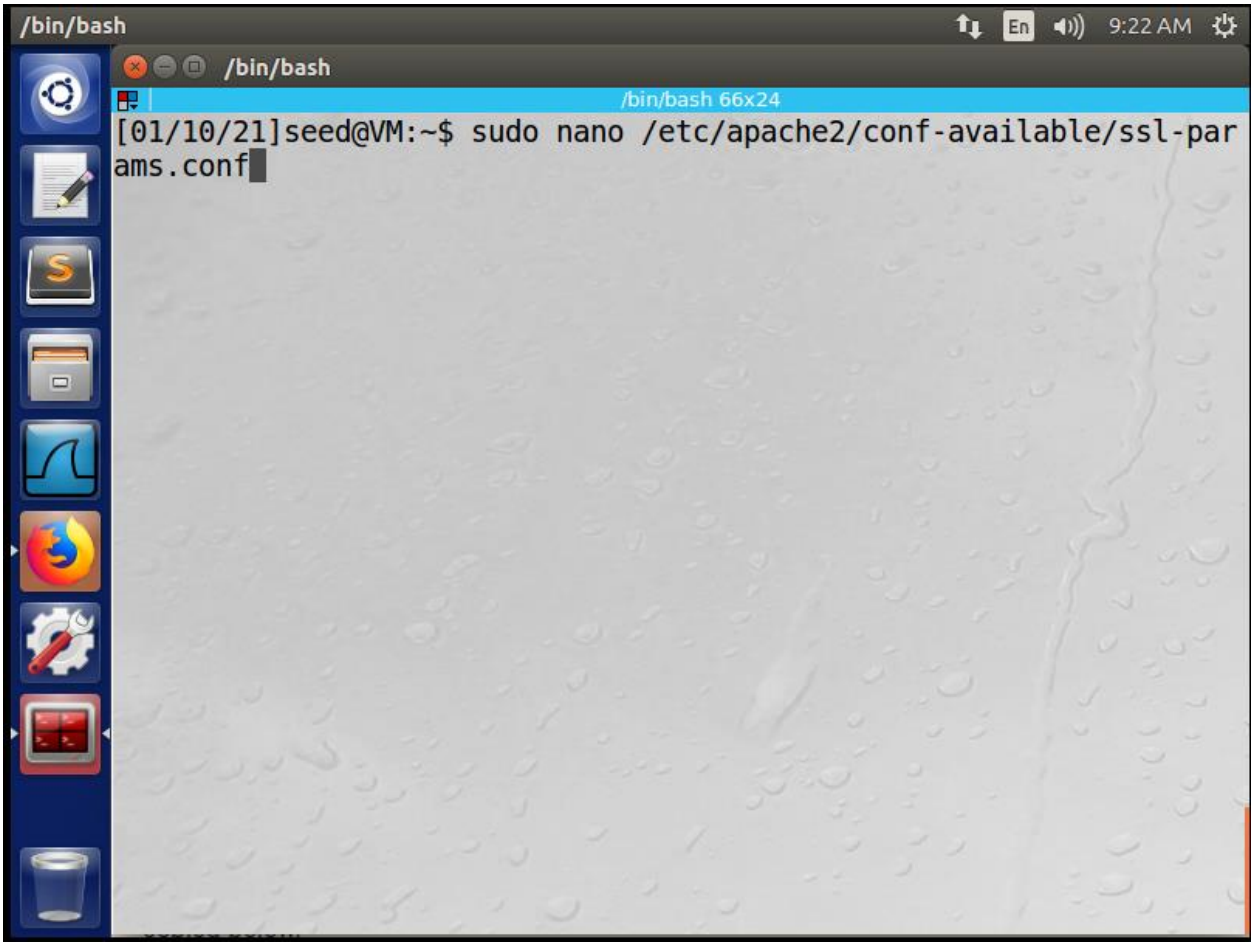
- **Câu lệnh:** *openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048*

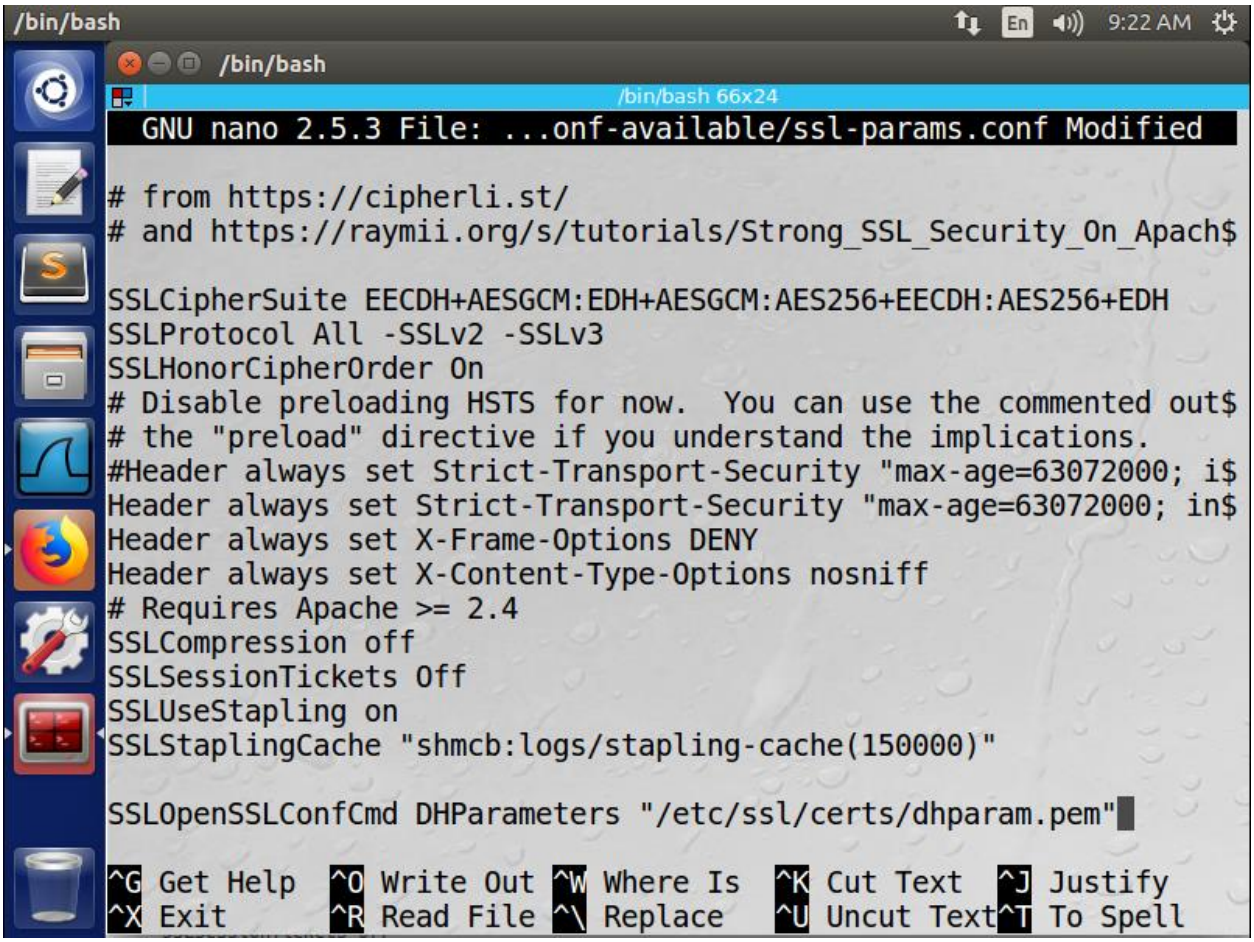


2. Cấu hình apache để sử dụng SSL

2.1 Tạo Apache Configuration Snippet với Strong Encyption Settings

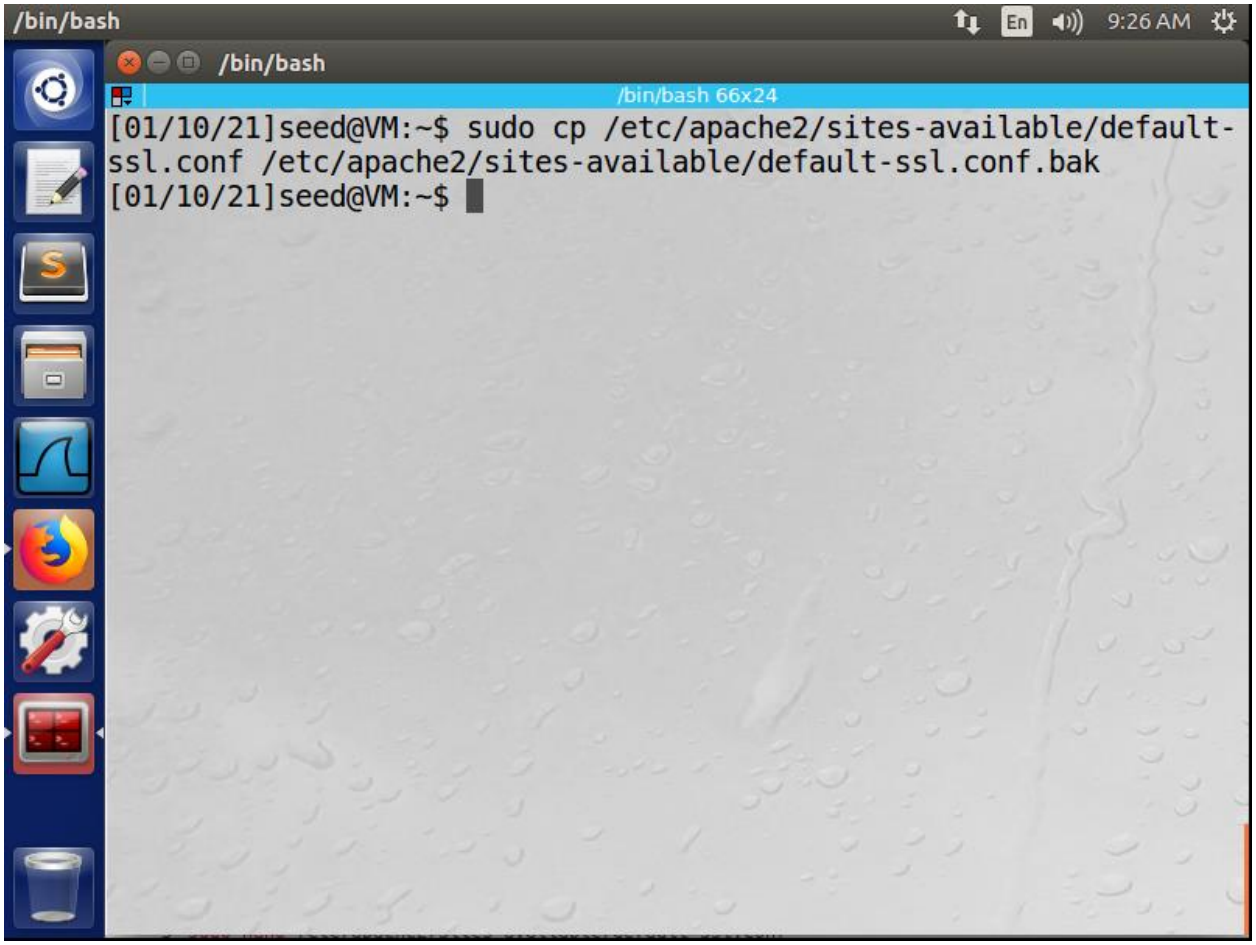
- **Câu lệnh:** *sudo nano /etc/apache2/conf-available/ssl-params.conf*


/bin/bash
En
9:22 AM
/bin/bash
/bin/bash 66x24
[01/10/21]seed@VM:~$ sudo nano /etc/apache2/conf-available/ssl-par
ams.conf

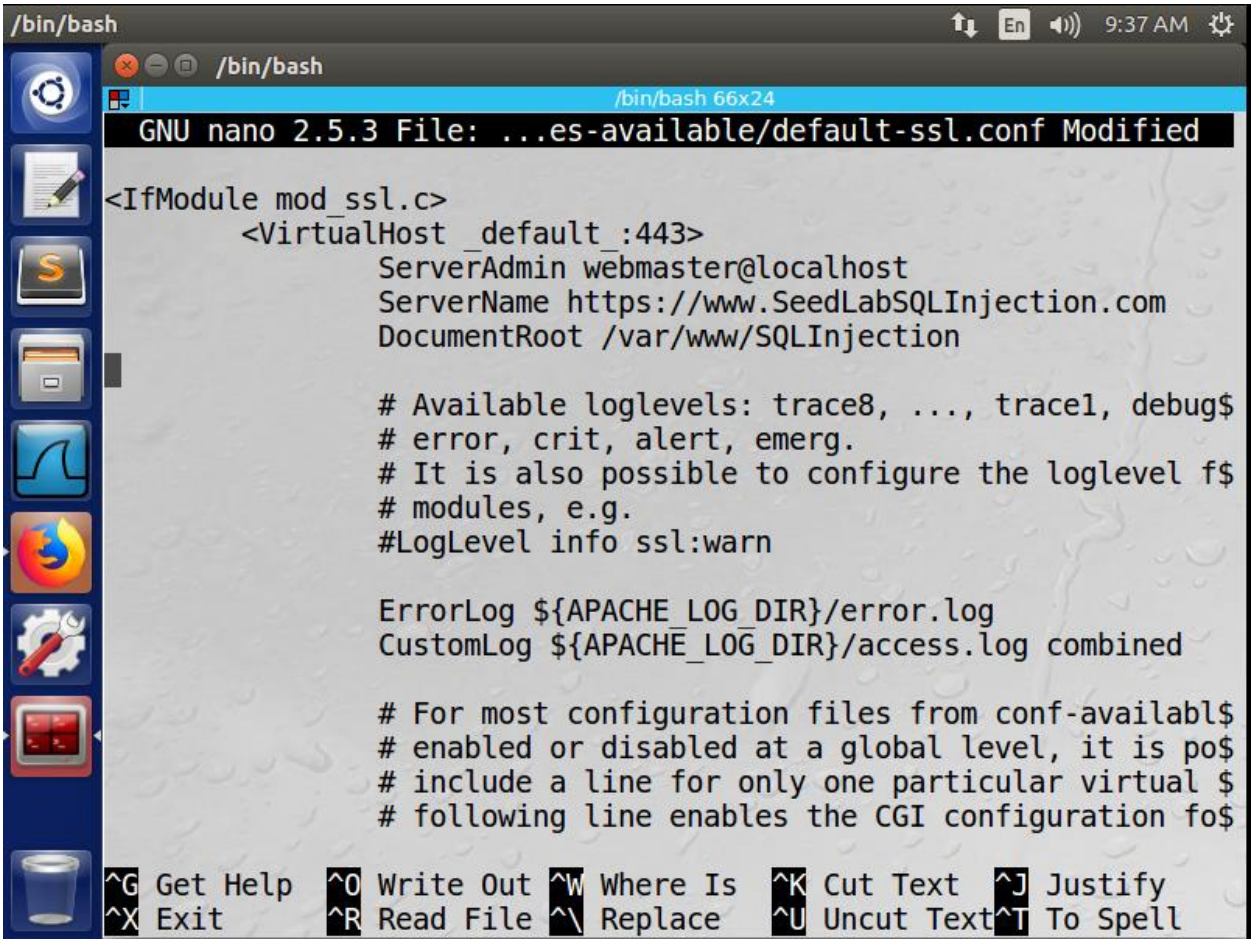


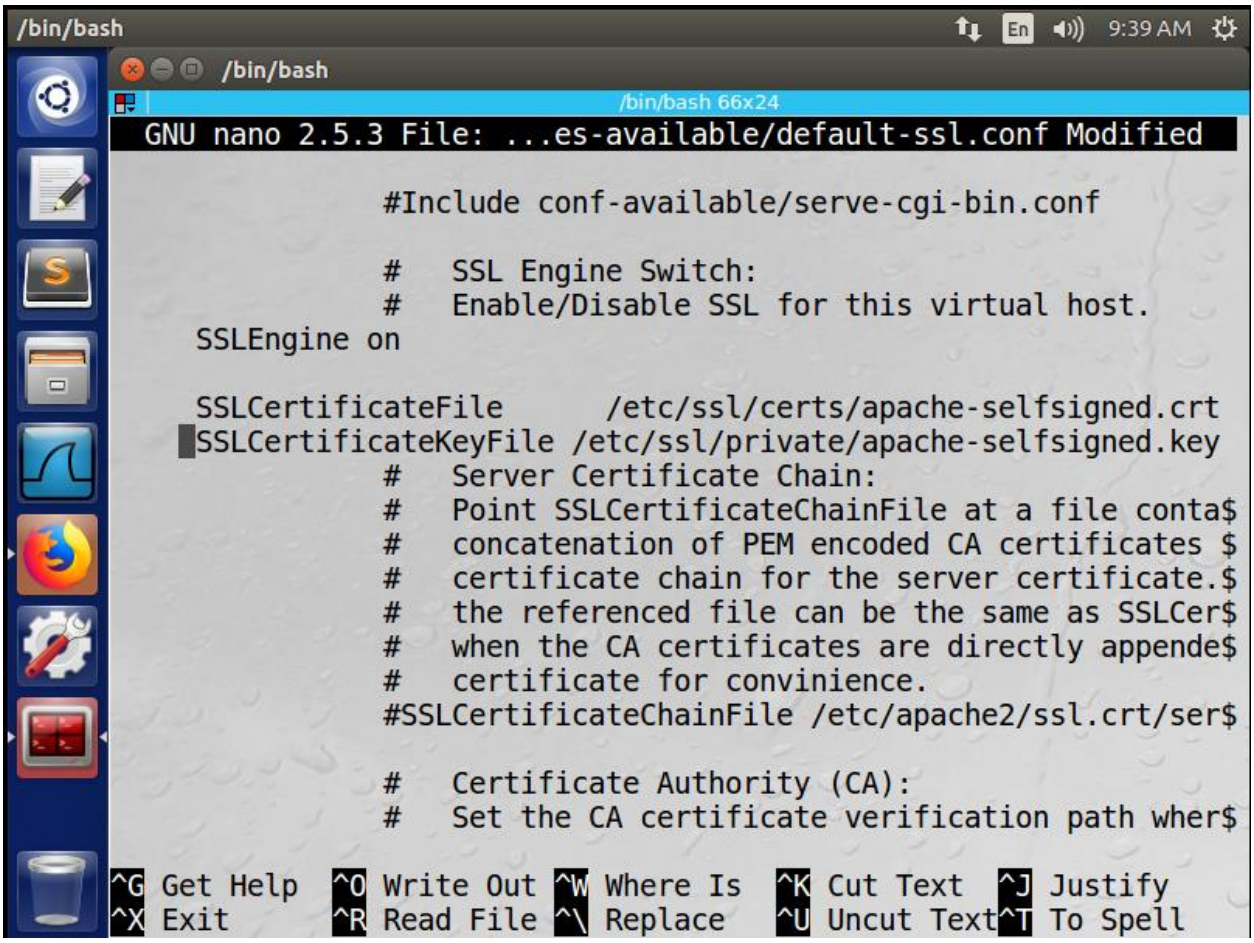
2.2 Tạo file backup và chỉnh sửa file default-ssl.conf

- **Tạo file backup để đề phòng trường hợp lỗi xảy ra:**
  - **Câu lệnh:** *cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak*



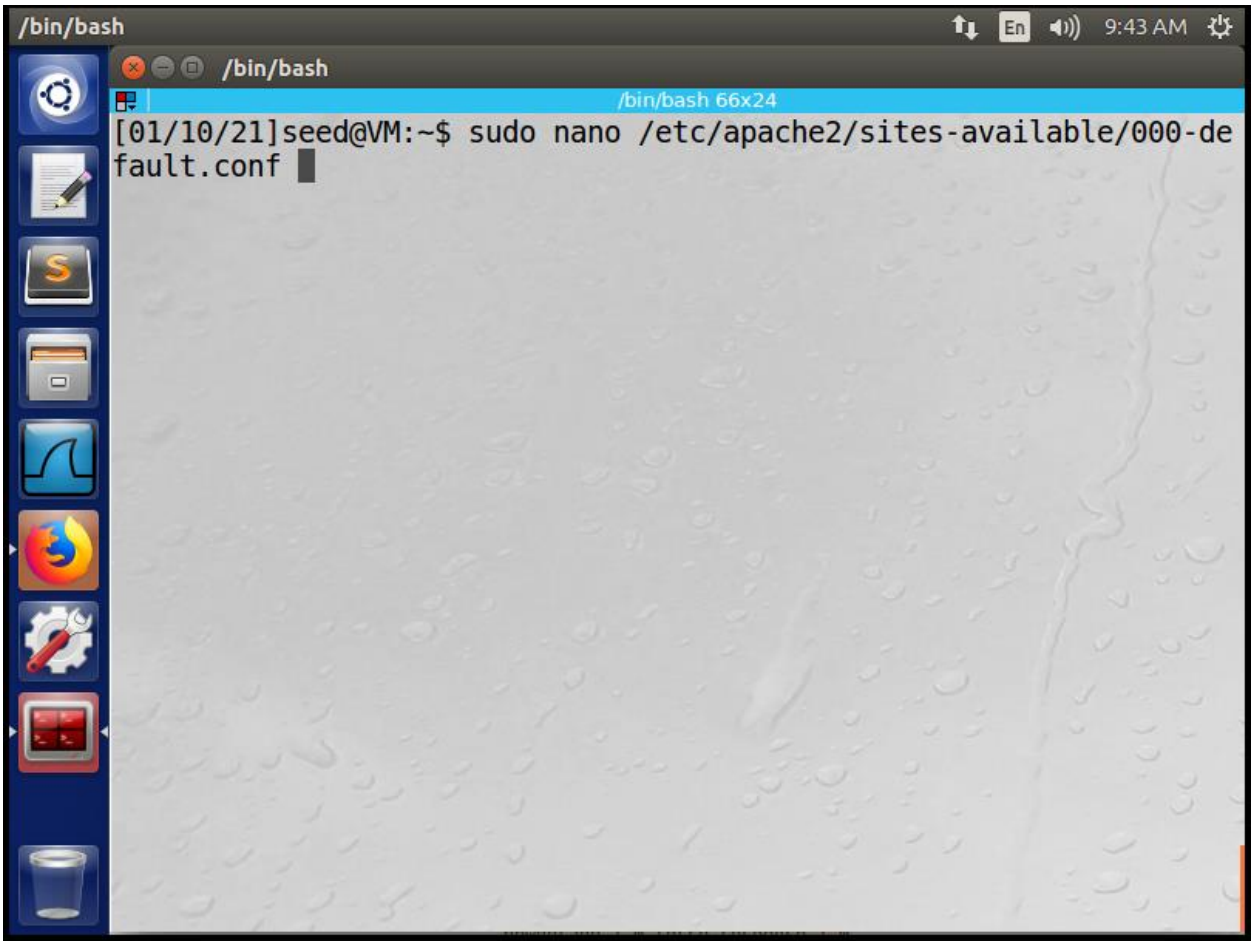
- **Chỉnh sửa file default-sst.conf theo như hình dưới đây**
  - **Câu lệnh:** *sudo nano /etc/apache2/sites-available/default-ssl.conf*

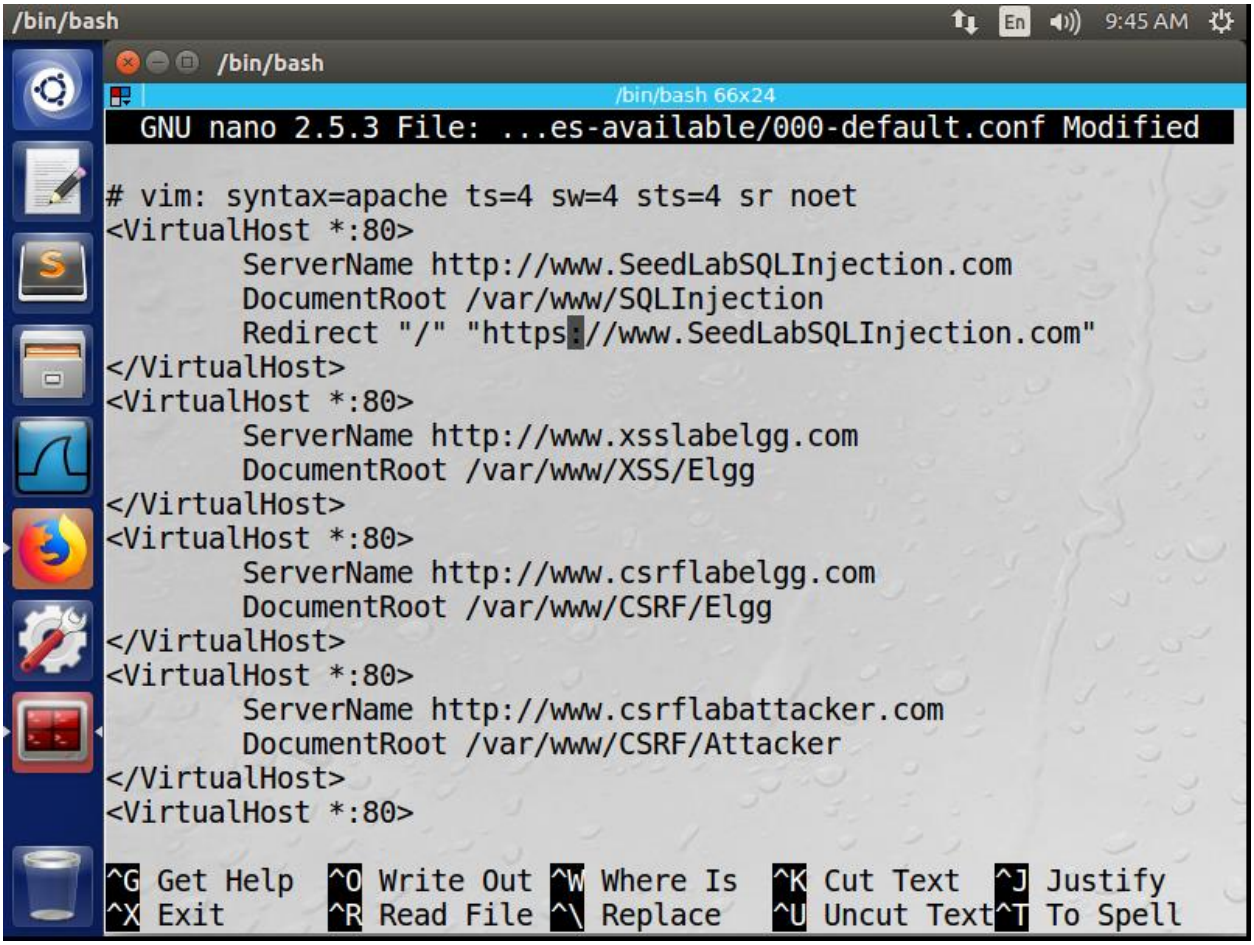

/bin/bash
En
9:37 AM
/bin/bash
/bin/bash 66x24
GNU nano 2.5.3 File: ...es-available/default-ssl.conf Modified
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
ServerAdmin webmaster@localhost
ServerName https://www.SeedLabSQLInjection.com
DocumentRoot /var/www/SQLInjection
Available loglevels: trace8, ..., trace1, debug$
error, crit, alert, emerg.
It is also possible to configure the loglevel f$
modules, e.g.
#LogLevel info ssl:warn
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
For most configuration files from conf-availabl$
enabled or disabled at a global level, it is po$
include a line for only one particular virtual $
following line enables the CGI configuration fo$
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell



2.3 Vào file /etc/apache2/sites-available/000-default.conf để thêm dòng chuyển hướng đến trang web

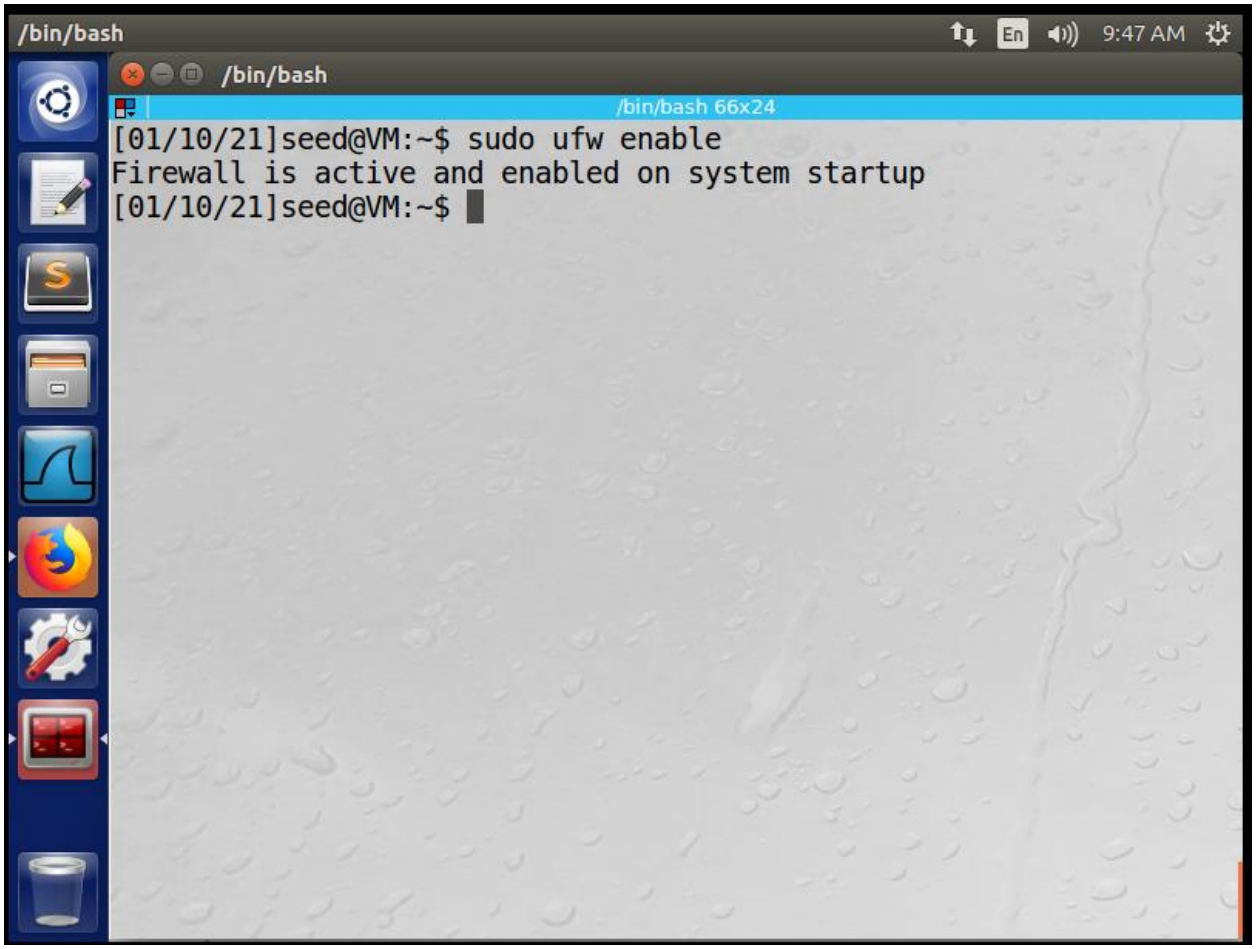
- **Câu lệnh:** *sudo nano /etc/apache2/sites-available/000-default.conf*


/bin/bash
En
9:43 AM
/bin/bash
/bin/bash 66x24
[01/10/21]seed@VM:~$ sudo nano /etc/apache2/sites-available/000-default.conf



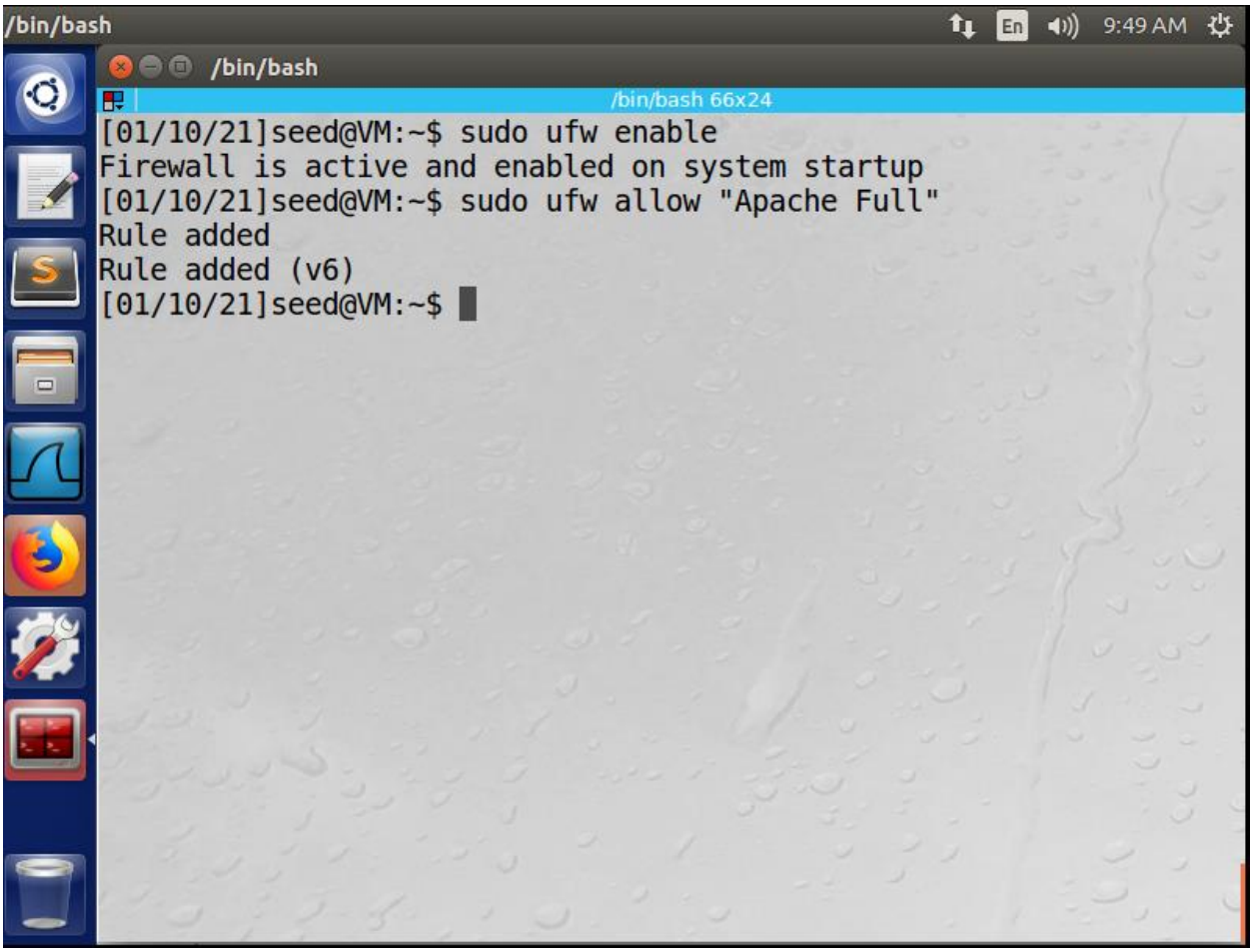
2.4 Điều chỉnh Firewall

- **Kích hoạt firewall:** *sudo ufw enable*



- **Cho phép tất cả mọi thứ của Apache**

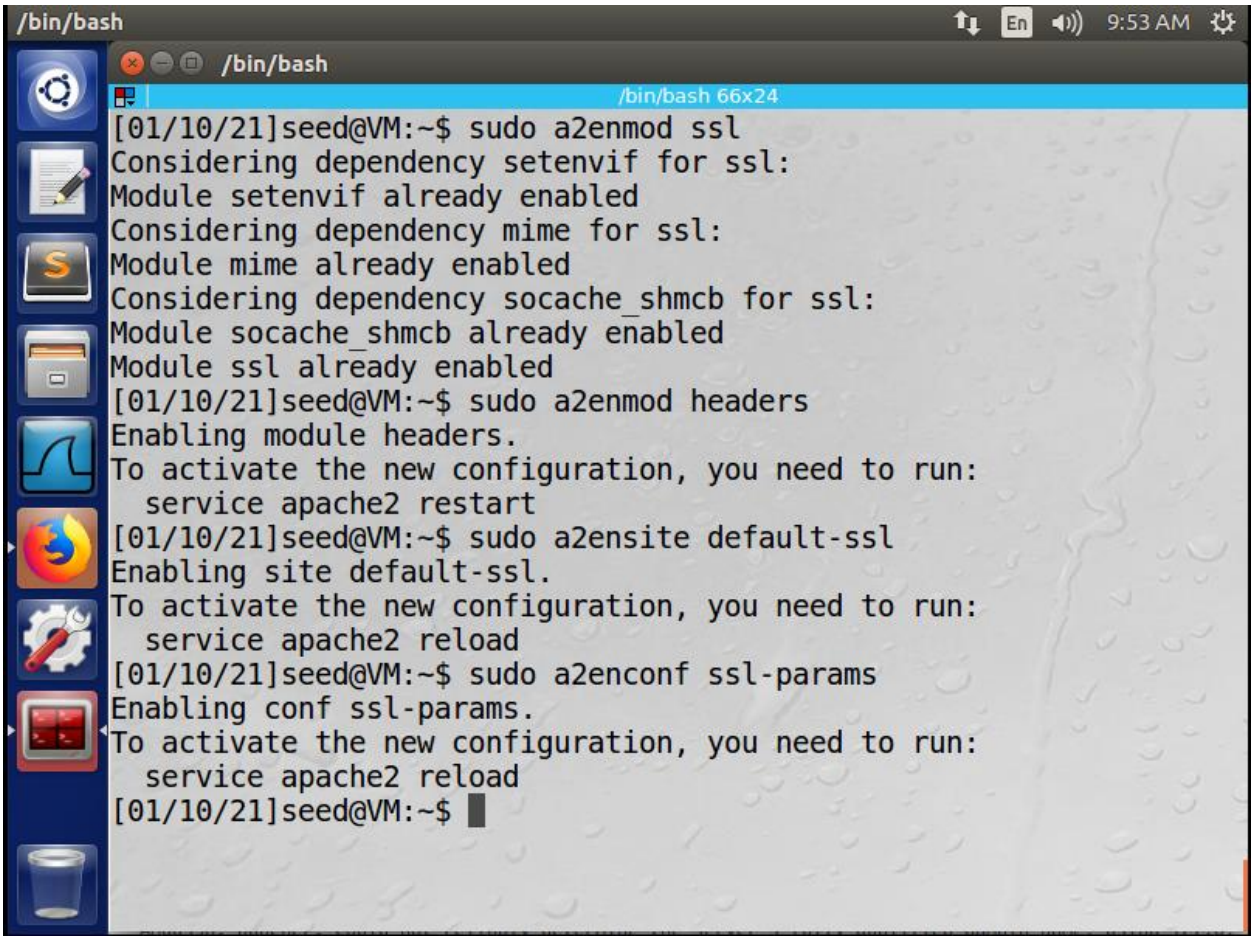
  sudo ufw allow "Apache Full"



2.5 Kích hoạt SSL trên Apache

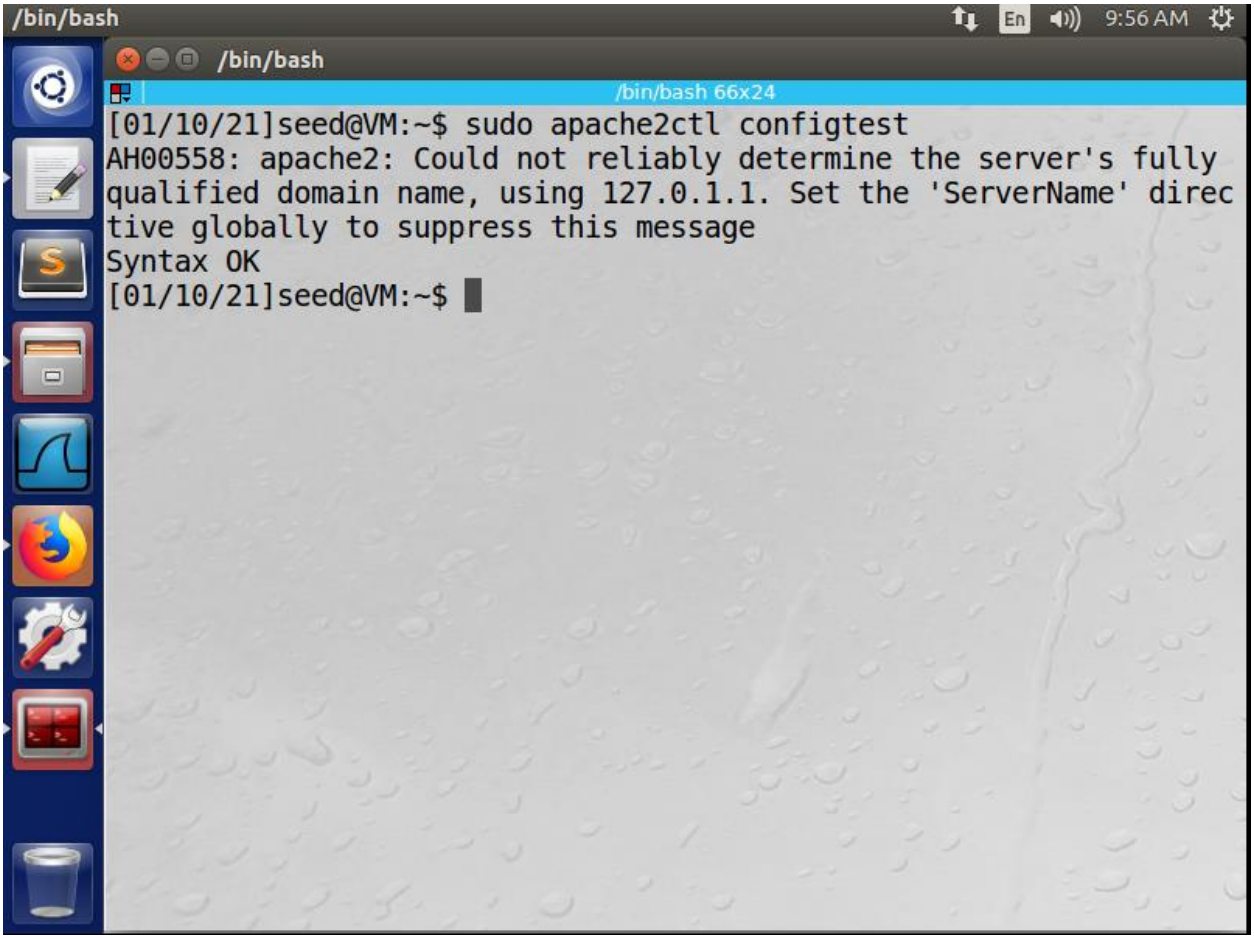
- **Câu lệnh :**

sudo a2enmod ssl
sudo a2enmod headers
sudo a2ensite default-ssl
sudo a2enconf ssl-params



- **Kiểm tra syntax error**

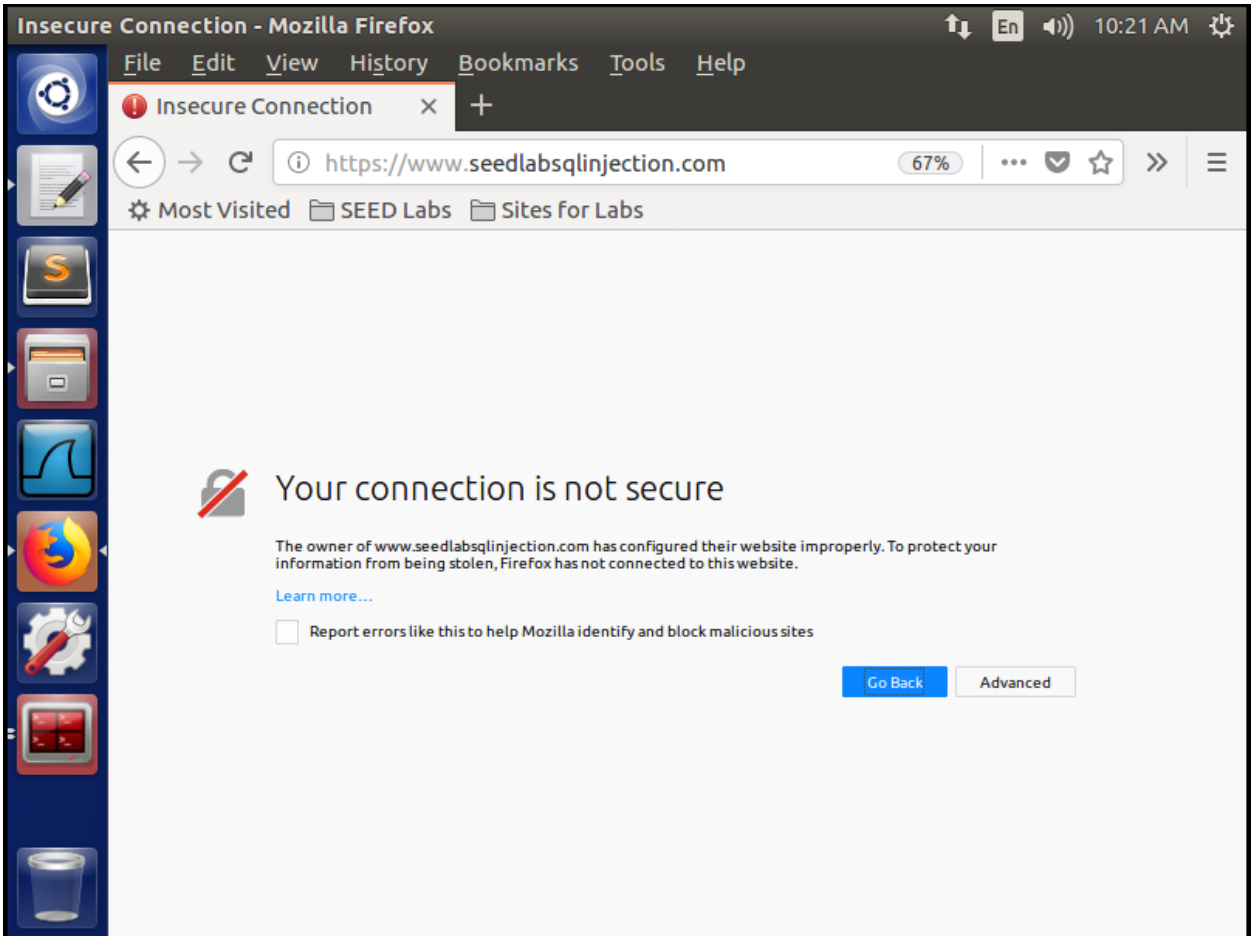
  sudo apache2ctl configtest



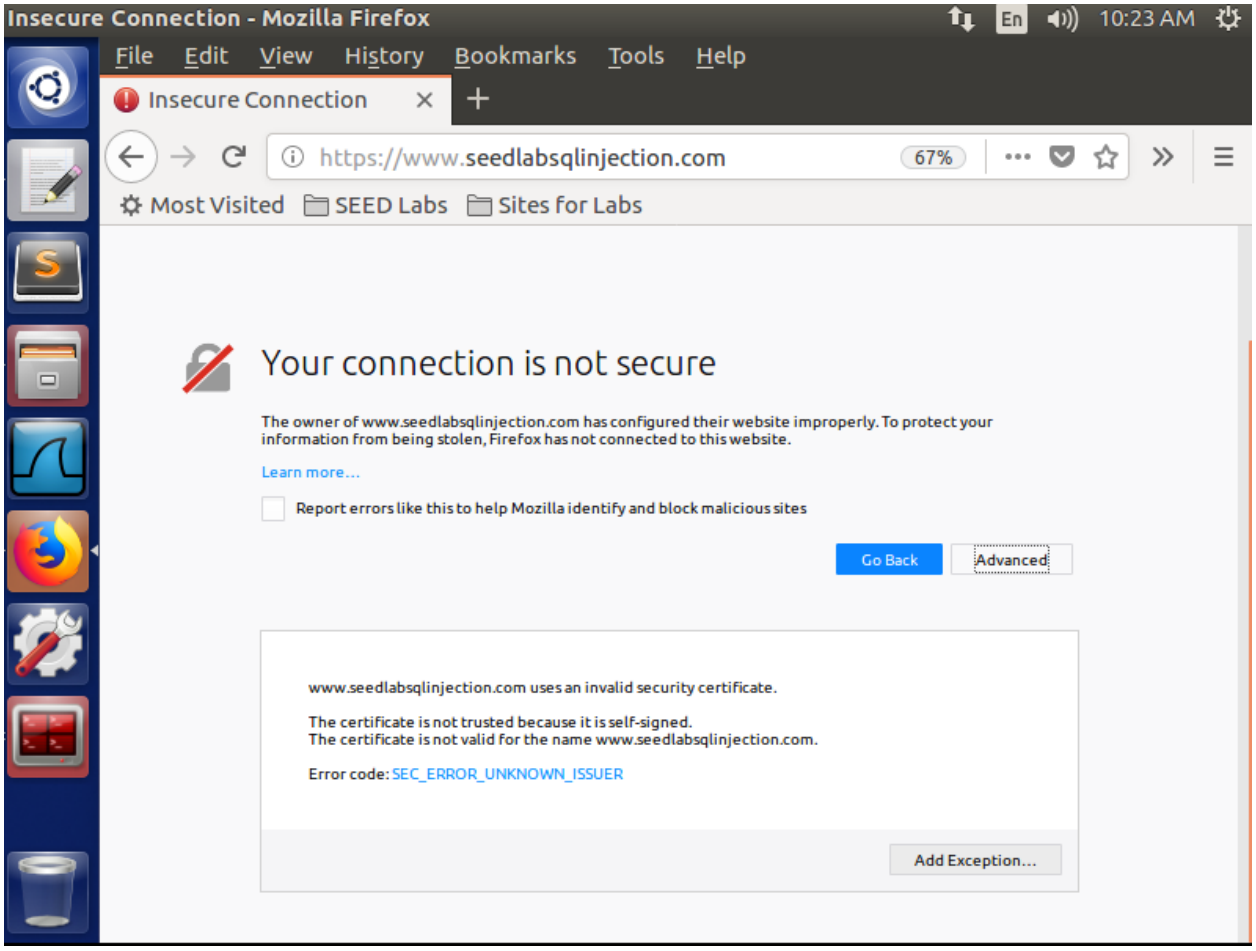
- **Khởi động lại apache2:** *sudo systemctl restart apache2*

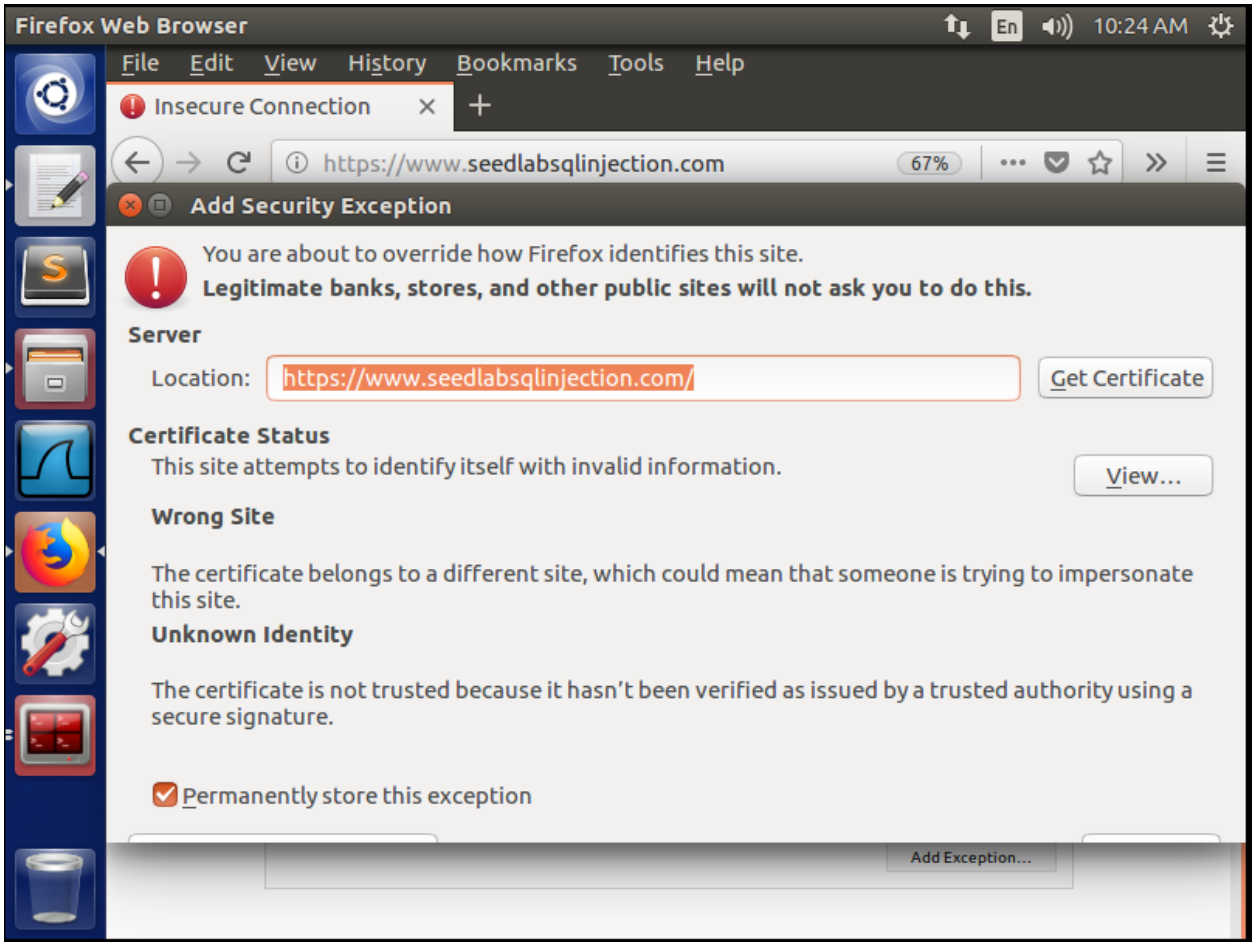
2.6 Kiểm tra chứng chỉ đã tạo

- Mở trình duyệt và vào trang đã gắn chứng chỉ *https://SeedLabSQLInjection.com*

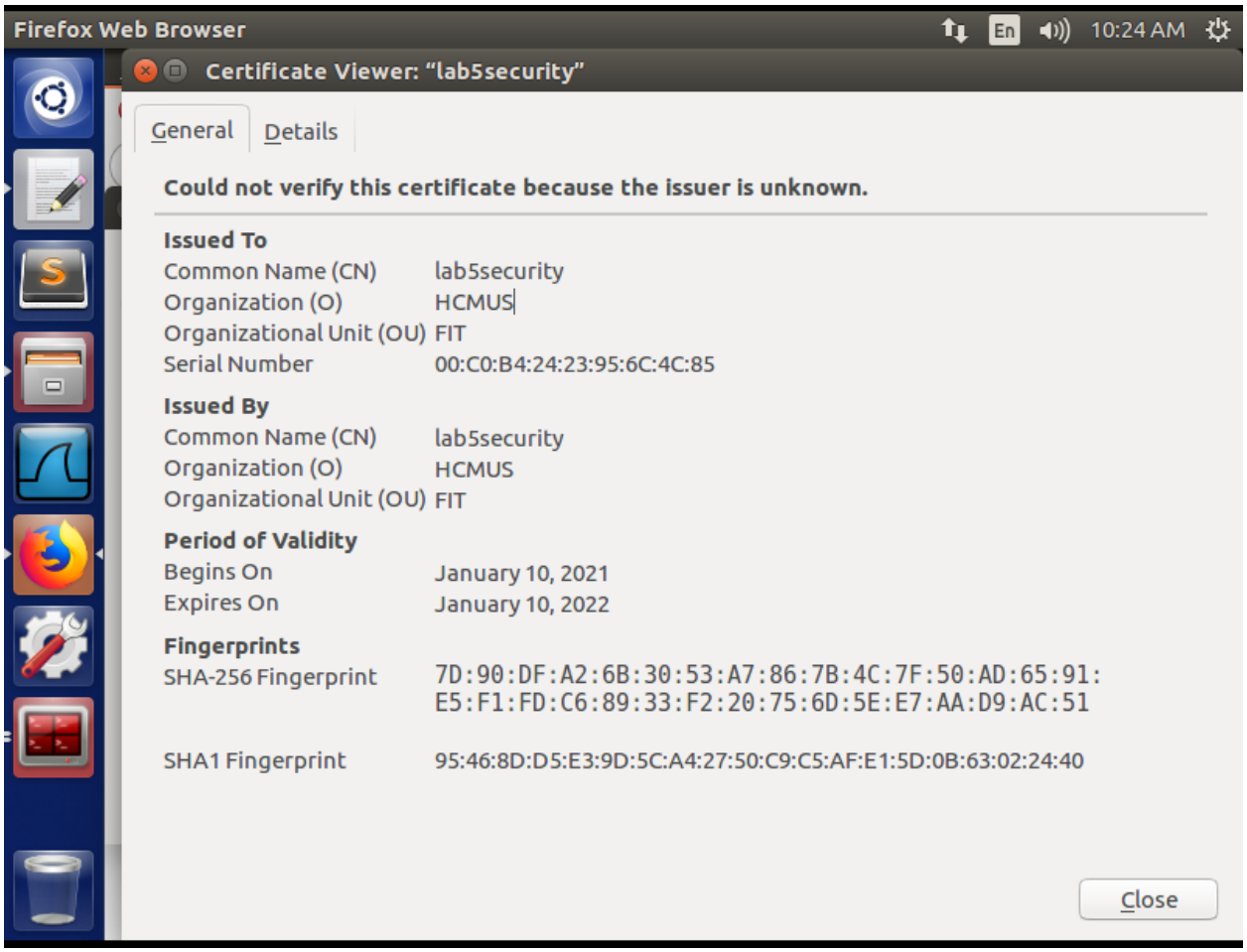


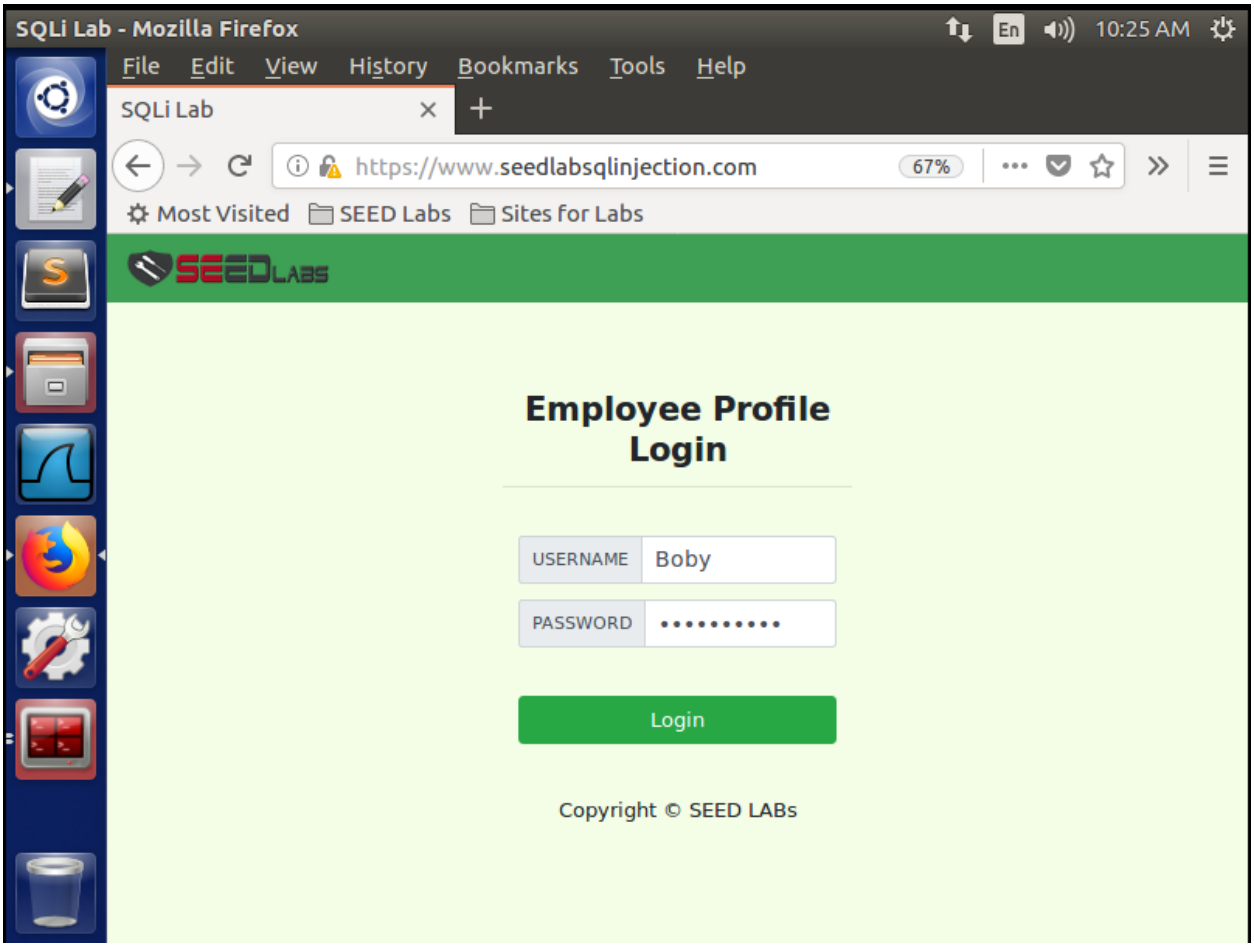
- Ta thấy nó hiện lên cảnh báo do chứng chỉ ta cấp cho trang web này không được chứng thực bởi một tổ chức đáng tin cậy
- Để sửa lỗi này ta vào thẻ **Advanced -> Add Exception -> Get Certificate** để cấp quyền sử dụng chứng chỉ


Insecure Connection - Mozilla Firefox
En
10:23 AM
File Edit View History Bookmarks Tools Help
Insecure Connection
https://www.seedlabsqlinjection.com
67%
Most Visited
SEED Labs
Sites for Labs
Your connection is not secure
The owner of www.seedlabsqlinjection.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced
www.seedlabsqlinjection.com uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
The certificate is not valid for the name www.seedlabsqlinjection.com.
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception...


Firefox Web Browser
10:24 AM
File Edit View History Bookmarks Tools Help
Insecure Connection
https://www.seedlabsqlinjection.com
67%
Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://www.seedlabsqlinjection.com/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Add Exception...

- Ta đã cấp quyền sử dụng thành công




SQLi Lab - Mozilla Firefox
10:25 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
https://www.seedlabsqlinjection.com
67%
Most Visited
SEED Labs
Sites for Labs
Employee Profile Login
USERNAME
Boby
PASSWORD
Login
Copyright © SEED LABs