SSL Certificate for Apache in Ubuntu

sudo apt update
sudo apt install apache2

```
root@server:~# systemctl start apache2
root@server:~# systemctl restart apache2
```

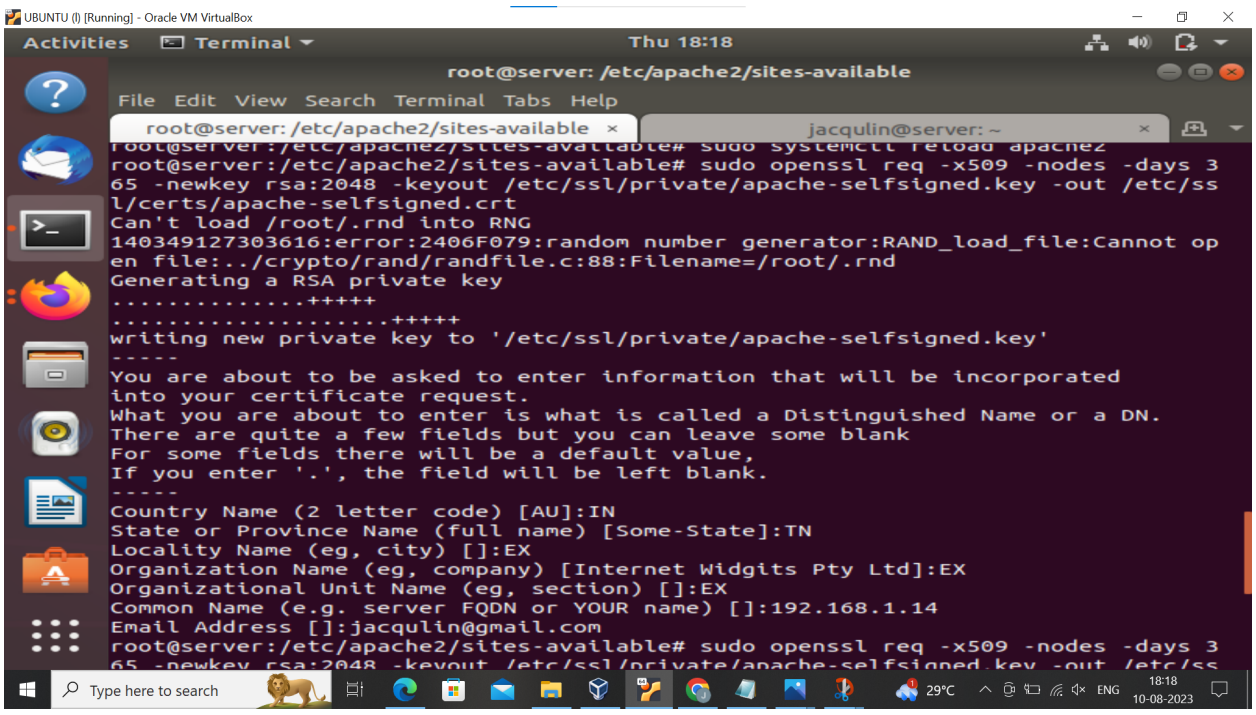
sudo ufw allow "Apache Full"

```
root@server:~# sudo ufw allow "Apache Full "
ERROR: Could not find a profile matching 'Apache Full '
root@server:~# sudo ufw allow "Apache Full"
Rules updated
Rules updated (v6)
```

sudo a2enmod ssl
sudo systemctl restart apache2

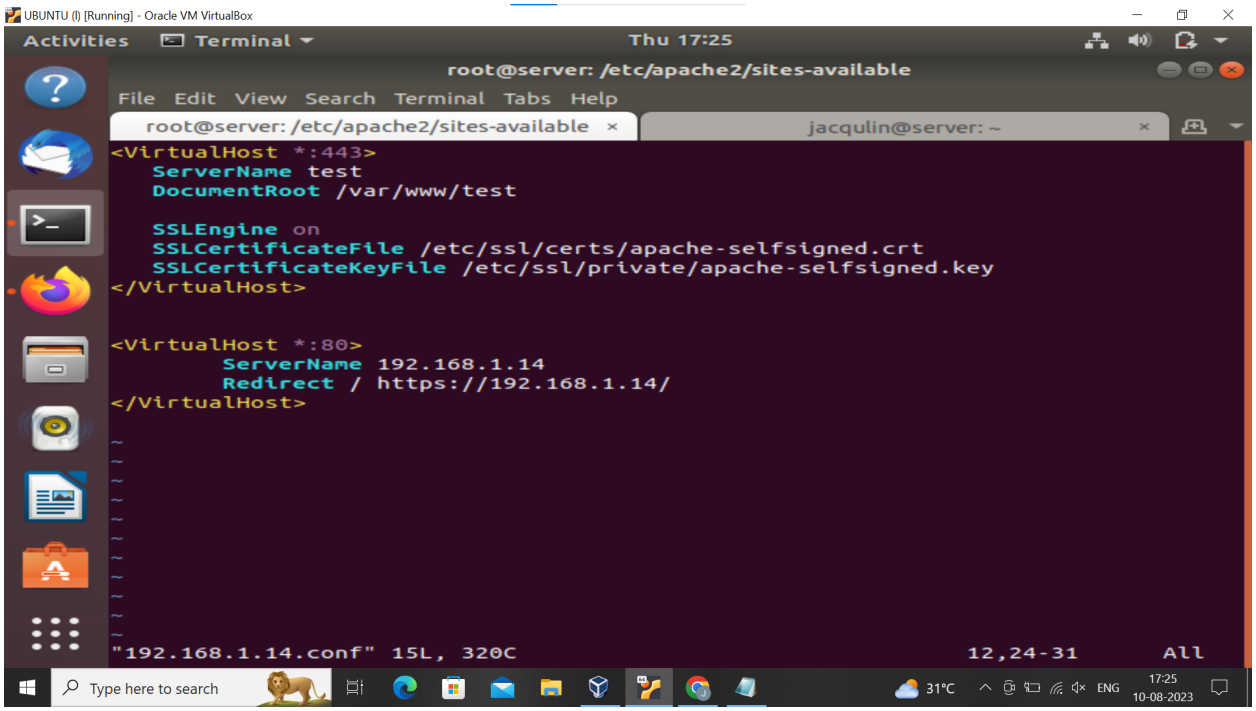
```
root@server:~# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
root@server:~# sudo systemctl restart apache2
root@server:~#
```

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



- openssl: This is the command line tool for creating and managing OpenSSL certificates, keys, and other files.
- req -x509: This specifies that we want to use X.509 certificate signing request (CSR) management. X.509 is a public key infrastructure standard that TLS adheres to for key and certificate management.
- -nodes: This tells OpenSSL to skip the option to secure our certificate with a passphrase. We need Apache to be able to read the file, without user intervention, when the server starts up. A passphrase would prevent this from happening, since we would have to enter it after every restart.
- -days 365: This option sets the length of time that the certificate will be considered valid. We set it for one year here. Many modern browsers will reject any certificates that are valid for longer than one year.
- -newkey rsa:2048: This specifies that we want to generate a new certificate and a new key at the same time. We did not create the key that is required to sign the certificate in a previous step, so we need to create it along with the certificate. The rsa:2048 portion tells it to make an RSA key that is 2048 bits long.
- -keyout: This line tells OpenSSL where to place the generated private key file that we are creating.
- -out: This tells OpenSSL where to place the certificate that we are creating.

sudo nano /etc/apache2/sites-available/192.168.1.14.conf

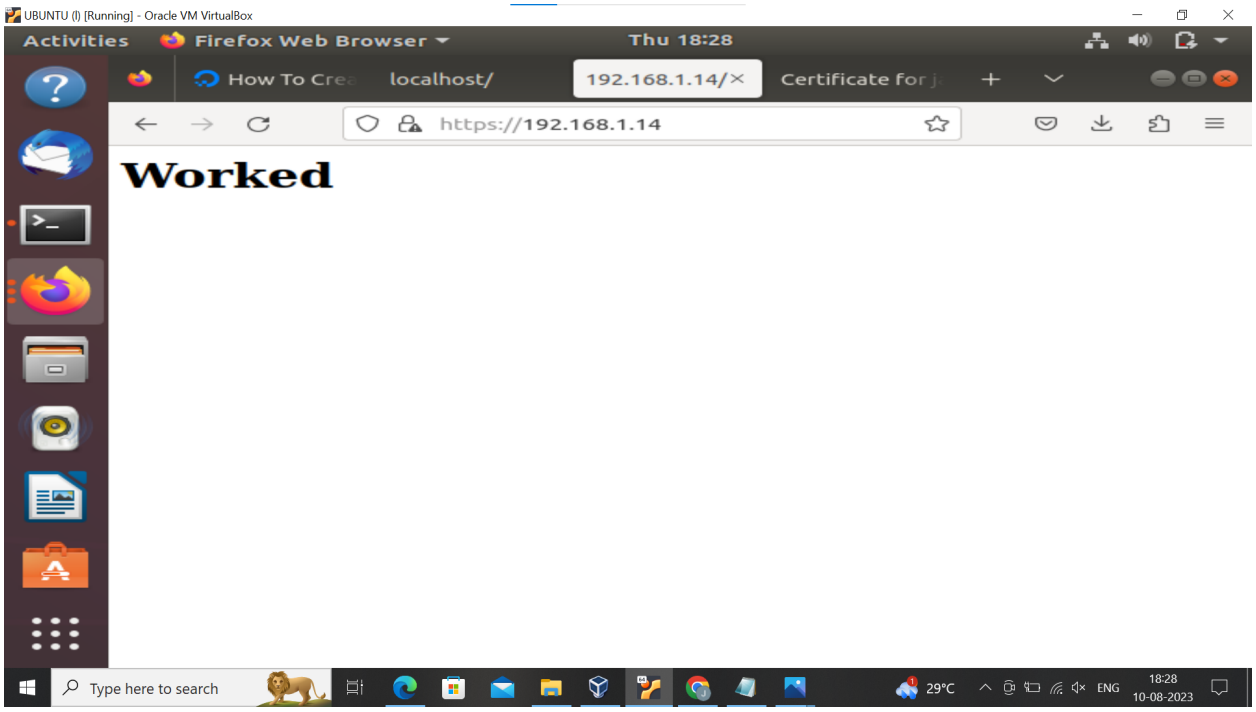


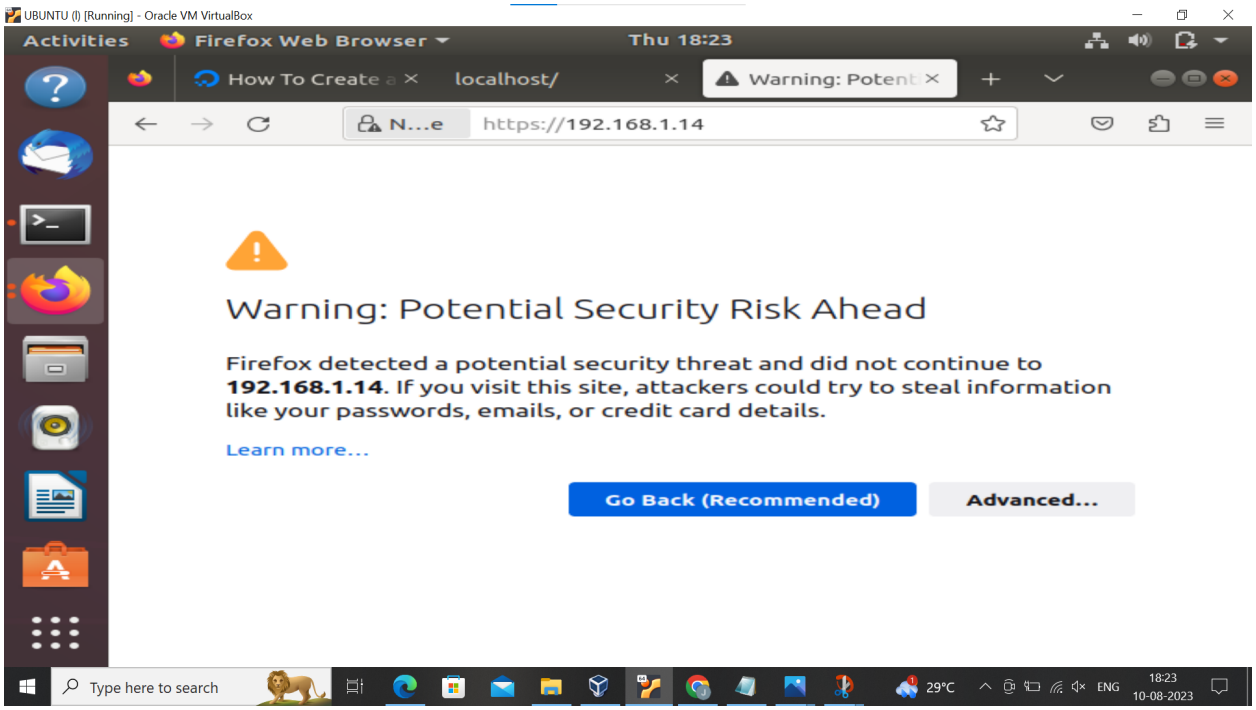
Create Directory:
sudo mkdir /var/www/192.168.1.14

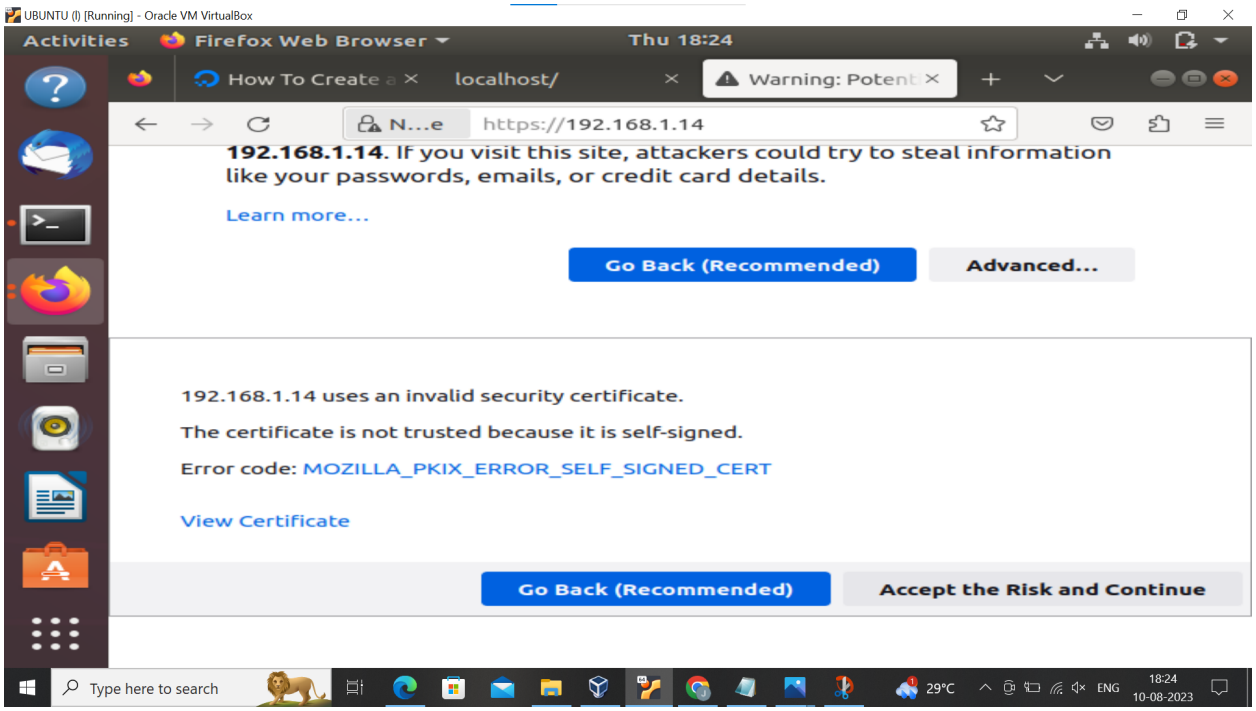
sudo nano /var/www/192.168.1.14/index.html

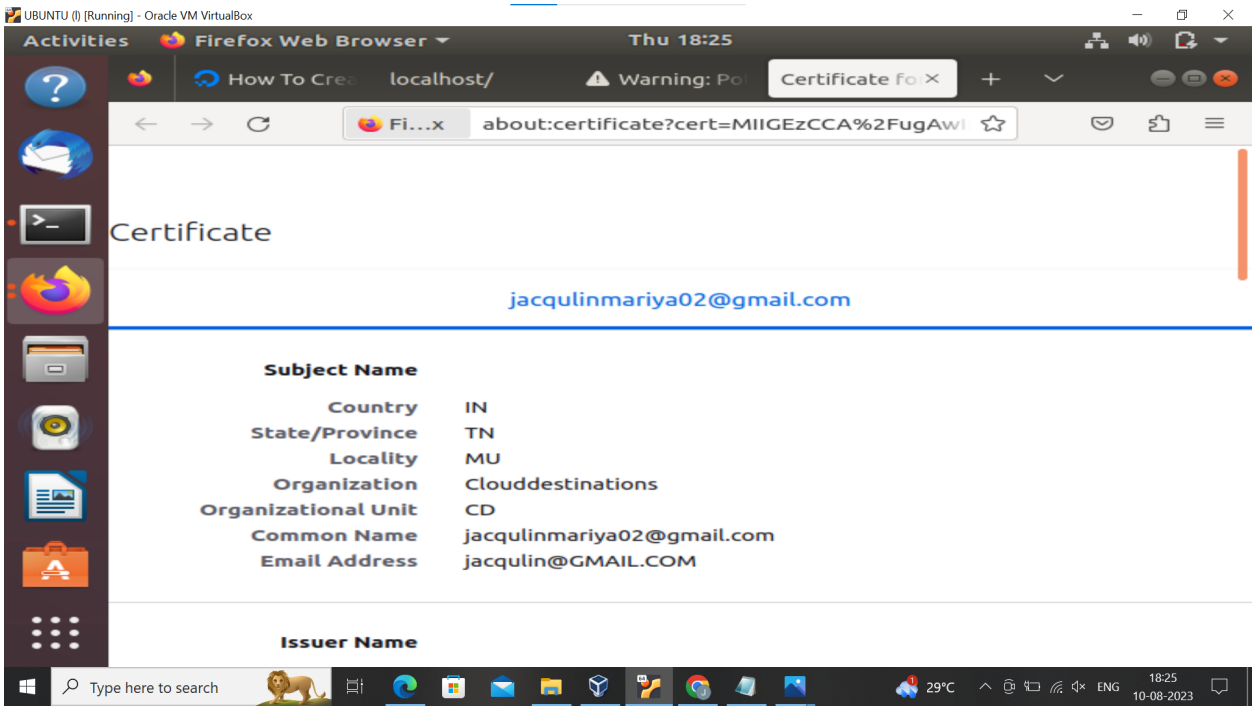
```
Unset

<h1>it worked!</h1>
```




UBUNTU (I) [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Thu 18:23
How To Create a
localhost/
Warning: Potent
N...e
https://192.168.1.14
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 192.168.1.14. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
Type here to search
29°C
ENG
18:23
10-08-2023


UBUNTU (I) [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Thu 18:24
How To Create a
localhost/
Warning: Potent
N...e
https://192.168.1.14
192.168.1.14. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
192.168.1.14 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue
Type here to search
29°C
ENG
18:24
10-08-2023



sudo a2ensite .conf

```
root@server:/etc/apache2/sites-available# sudo a2ensite 192.168.1.14.conf
Enabling site 192.168.1.14.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@server:/etc/apache2/sites-available# systemctl reload apache2
root@server:/etc/apache2/sites-available#
```

sudo systemctl reload apache2

```
root@server:/etc/apache2/sites-available# sudo a2ensite 192.168.1.14.conf
Enabling site 192.168.1.14.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@server:/etc/apache2/sites-available# systemctl reload apache2
root@server:/etc/apache2/sites-available#
```

sudo apachectl configtest

```
  -X                  : debug mode (only one worker, do not detach)
root@server:/etc/apache2/sites-available# cd
root@server:~# sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified dom
ain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress
this message
Syntax OK
root@server:~#
```

sudo systemctl reload apache2