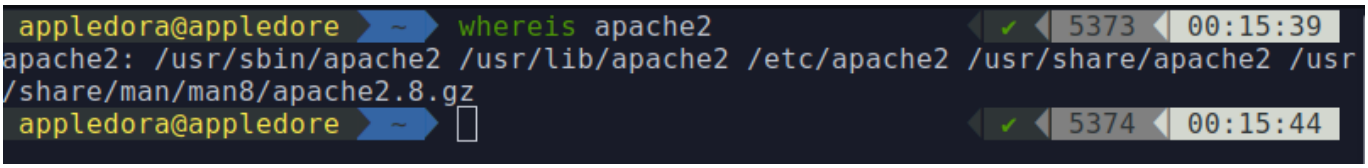
Task 1 Checkpoint 1

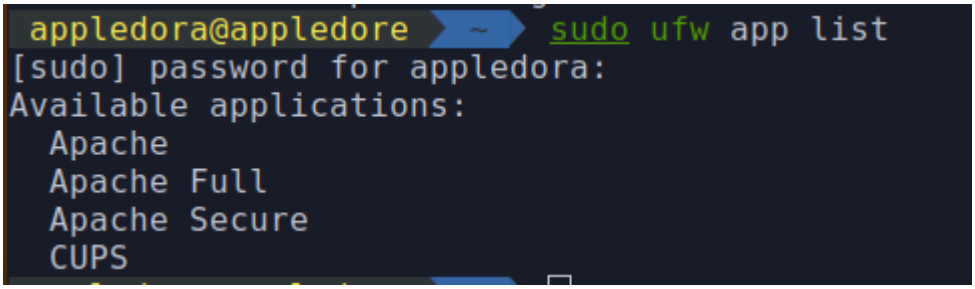
1. Install Apache

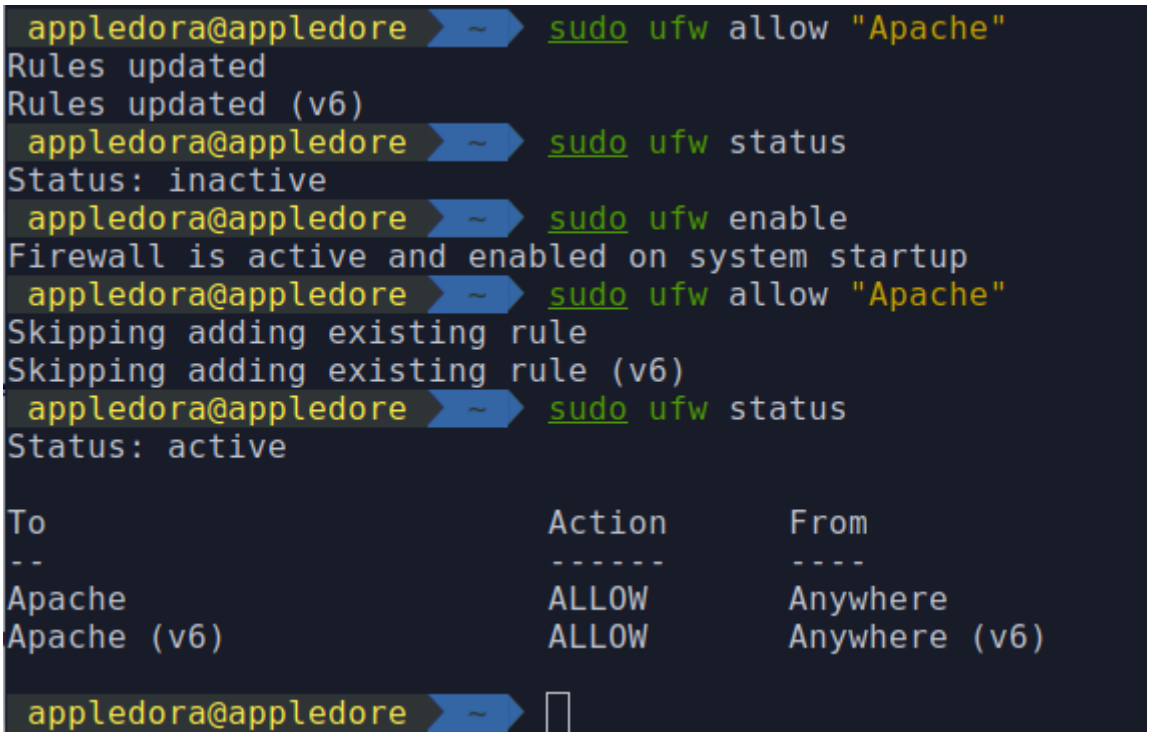
```
sudo apt update
sudo apt install apache2
```



2. Adjusting Firewall

Check existing firewall profiles and enable "Apache" firewall





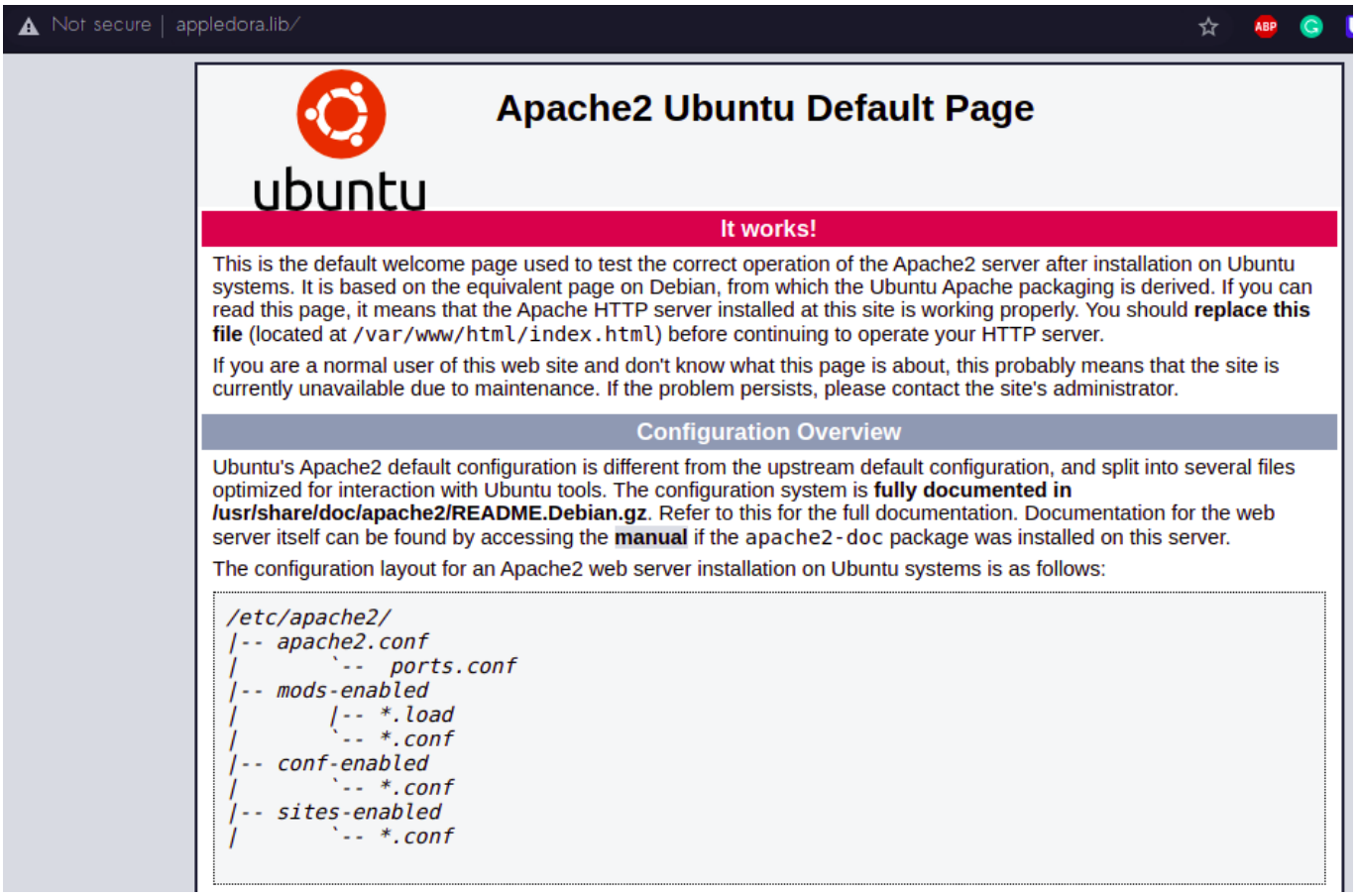
3. Check the status of the apache server if it is running or not.

```
appledora@appledore ~ sudo systemctl status apache2 ✔ 5381 00:19:46

● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset:
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Sun 2021-04-04 18:00:11 +06; 1 weeks 5 days ag
  Process: 21399 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/
 Main PID: 1994 (apache2)
    Tasks: 6 (limit: 4915)
   CGroup: /system.slice/apache2.service
           ├─ 1994 /usr/sbin/apache2 -k start
           ├─21416 /usr/sbin/apache2 -k start
           ├─21417 /usr/sbin/apache2 -k start
           ├─21418 /usr/sbin/apache2 -k start
           ├─21419 /usr/sbin/apache2 -k start
           └─21420 /usr/sbin/apache2 -k start

Apr 13 00:06:15 appledore systemd[1]: Reloading The Apache HTTP Server.
Apr 13 00:06:15 appledore systemd[1]: Reloaded The Apache HTTP Server.
Apr 14 00:07:00 appledore systemd[1]: Reloading The Apache HTTP Server.
Apr 14 00:07:00 appledore systemd[1]: Reloaded The Apache HTTP Server.
Apr 15 00:09:31 appledore systemd[1]: Reloading The Apache HTTP Server.
Apr 15 00:09:32 appledore systemd[1]: Reloaded The Apache HTTP Server.
Apr 16 00:05:13 appledore systemd[1]: Reloading The Apache HTTP Server.
lines 1-23...skipping...
```

Map `localhost` to `appledora.lib` __by editing the `/etc/hosts` file

```
  GNU nano 2.9.3                                                /etc/hosts

127.0.0.1       localhost
127.0.1.1       appledora-HP-Notebook
127.0.0.1       appledora.lib
127.0.1.1       naziattttt.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

By visiting `appledora.lib` __the default apache webpage can be found.


Not secure | appledora.lib/
Apache2 Ubuntu Default Page
ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

Task 1 Checkpoint 2

We need to create a new virtual host to deploy a new domain from our webserver. For our purposes, we create `naziattttt.com` as the new domain.

```
appledora@appledore / sudo mkdir -p /var/www/naziattttt.com/html
appledora@appledore / sudo chown -R $USER:$USER /var/www/naziattttt.com/html
appledora@appledore / sudo chmod -R 755 /var/www/naziattttt.com
appledora@appledore / nano /var/www/naziattttt.com/html/index.html
appledora@appledore / sudo nano /etc/apache2/sites-available/naziattttt.com.conf
appledora@appledore / sudo a2ensite naziattttt.com.conf
Site naziattttt.com already enabled
appledora@appledore / sudo a2dissite 000-default.conf
Site 000-default already disabled
appledora@appledore / sudo apache2ctl configtest
Syntax OK
appledora@appledore / sudo systemctl restart apache2
appledora@appledore /
```

Configuration file for the domain

```
appledora@appledore /etc/apache2/sites-available cat naziattttt.com.conf

<VirtualHost *:80>
ServerAdmin admin@naziattttt.com
ServerName naziattttt.com
ServerAlias www.naziattttt.com
DocumentRoot /var/www/naziattttt.com/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

Default index.html for the new domain

```
appledora@appledore /var/www cd naziattttt.com/                    ✔ 6031 15:36:32
appledora@appledore /var/www/naziattttt.com ls                     ✔ 6032 15:36:41
html
appledora@appledore /var/www/naziattttt.com cd html                ✔ 6033 15:36:42
appledora@appledore /var/www/naziattttt.com/html cat index.html    ✔ 6034 15:36:49
<html>
<head>
<title>Welcome to naziattttt.com!</title>
</head>
<body>
<h1>Success! The naziattttt.com server block is working!</h1>
</body>
</html>
appledora@appledore /var/www/naziattttt.com/html                   ✔ 6035 15:36:53
```

The new domain will not directly work because it is not a registered domain. To direct traffic to this url we need to assign an ip address to the domain by mapping an ip address in our `/etc/hosts` file. After that restart the apache server

```
  GNU nano 2.9.3                                                /etc/hosts

127.0.0.1       localhost
127.0.1.1       appledora-HP-Notebook
127.0.0.1       appledora.lib
127.0.1.1       naziatttttt.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Visiting the link `naziatttttt.com` the following page shows up:

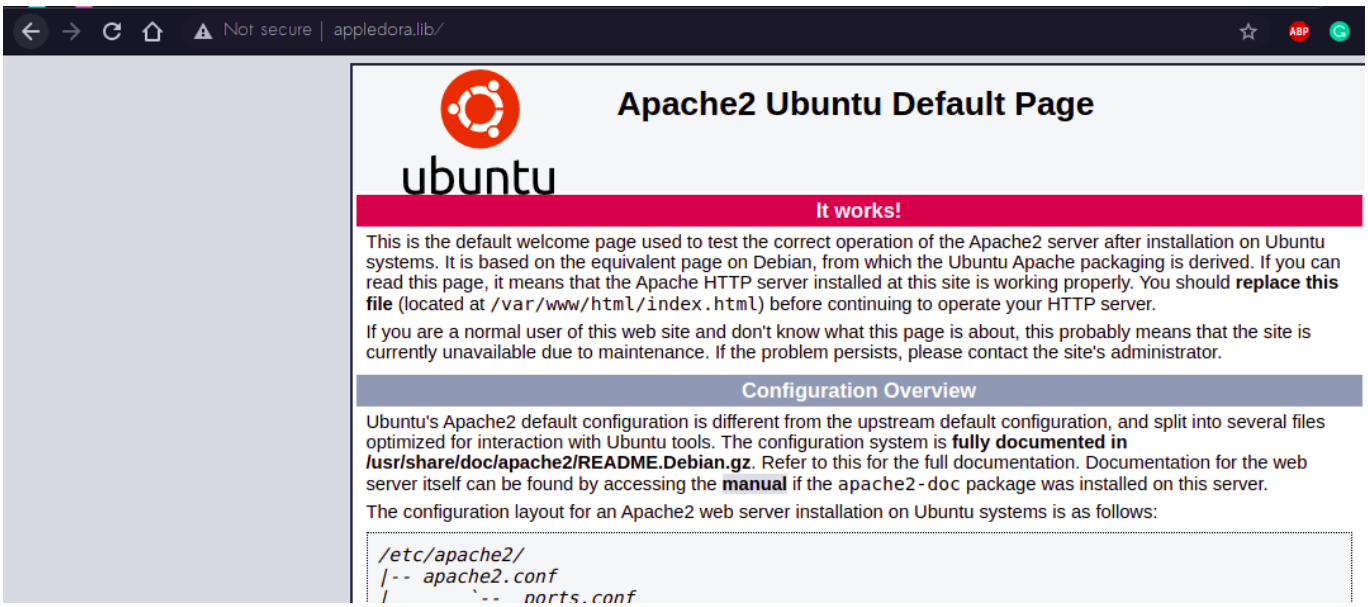
Success! The naziatttttt.com server block is working!

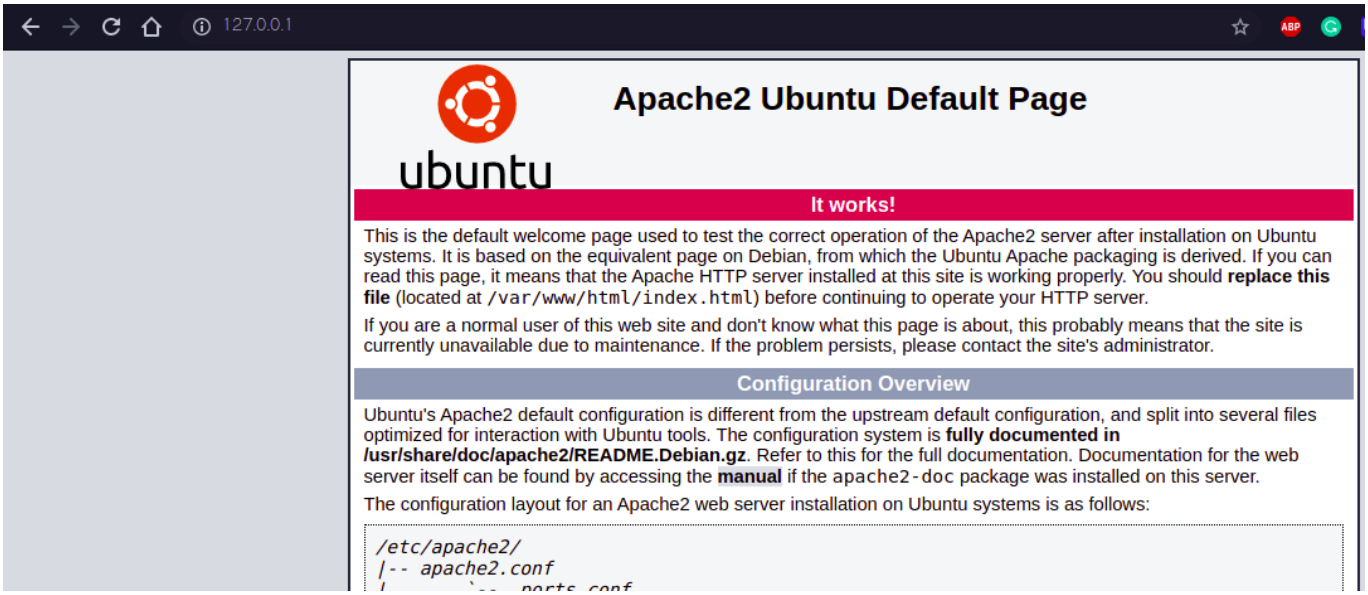
Task 1 Checkpoint 3

After running the following command,

```
sudo a2ensite 000-default.conf
sudo systemctl restart apache2
```

When we visit `appledora.lib` or `127.0.0.1` it serves the default apache page.





This is happening because each url or domain has its own configuration. We set up different virtual hosts which run in their own containers. So, our apache server is hosting both domains independently.

Task 2 Checkpoint 4

First we copy `/usr/lib/ssl/openssl.cnf` in our working directory as `jedissl.cnf`. We also created the required subdirectories inside `./jediCA`

We run the following command by passing in our `jedissl.cnf` to generate the self-signed certificate:

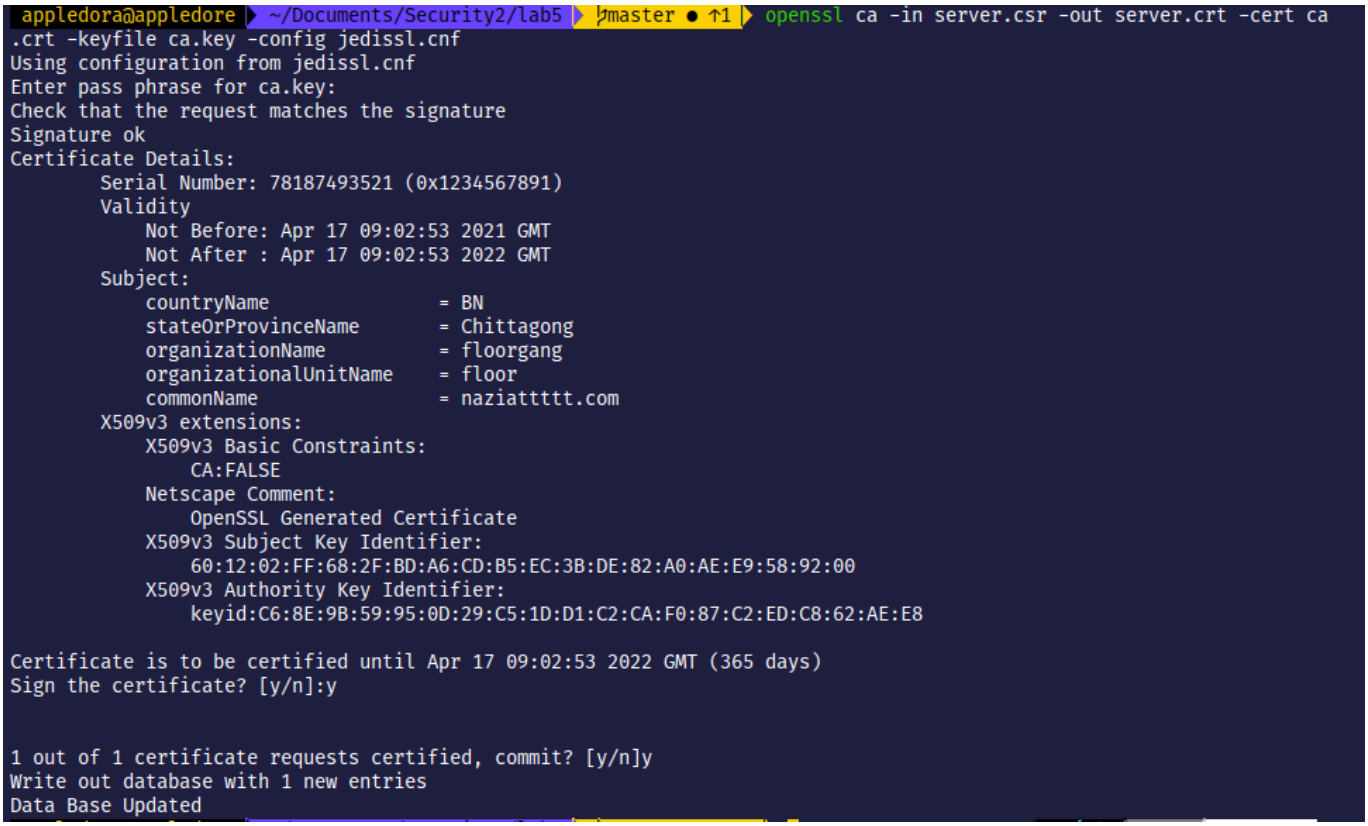
```
appledora@appledore ~/Documents/Security2/lab5 master ● ↑1 openssl req -new -x509 -keyout ca.key -out ca.crt
-config jedissl.cnf
Generating a RSA private key
.....................................................+++++
...+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:BN
State or Province Name (full name) [Some-State]:Chittagong
Locality Name (eg, city) []:ctg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:floorgang
Organizational Unit Name (eg, section) []:floor
Common Name (e.g. server FQDN or YOUR name) []:floorgang
Email Address []:.
```

Generating certificate for naziattttt.com

Now we follow the 3 steps to generate a certificate for `naziattttt.com`

```
appledora@appledore ~/Documents/Security2/lab5 master ● ↑1 openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.................................+++++
.....................+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

```
appledora@appledore ~/Documents/Security2/lab5 master ● ↑1 openssl req -new -key server.key -out server.csr -
config jedissl.cnf
Enter pass phrase for server.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]:BD
State or Province Name (full name) [Some-State]:Chittagong
Locality Name (eg, city) []:ctg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:floorgang
Organizational Unit Name (eg, section) []:floor
Common Name (e.g. server FQDN or YOUR name) []:naziattttt.com
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:root
An optional company name []:.
```

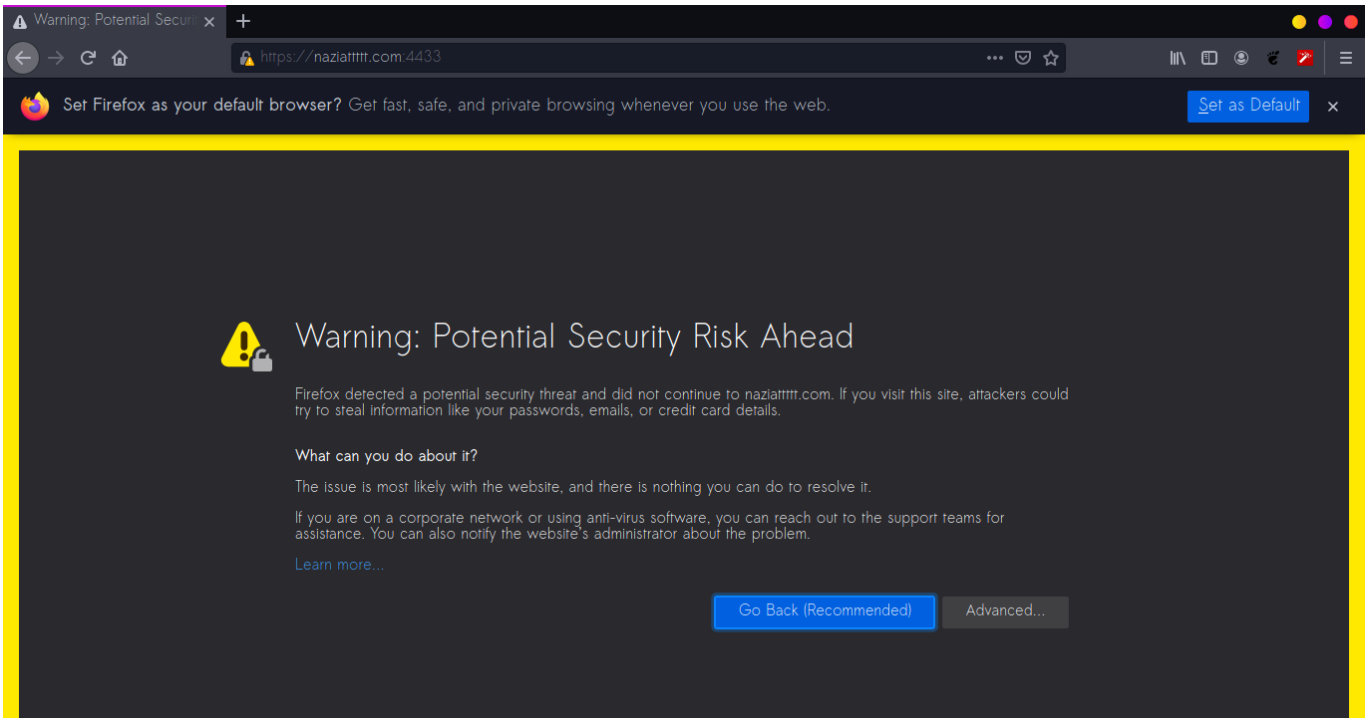


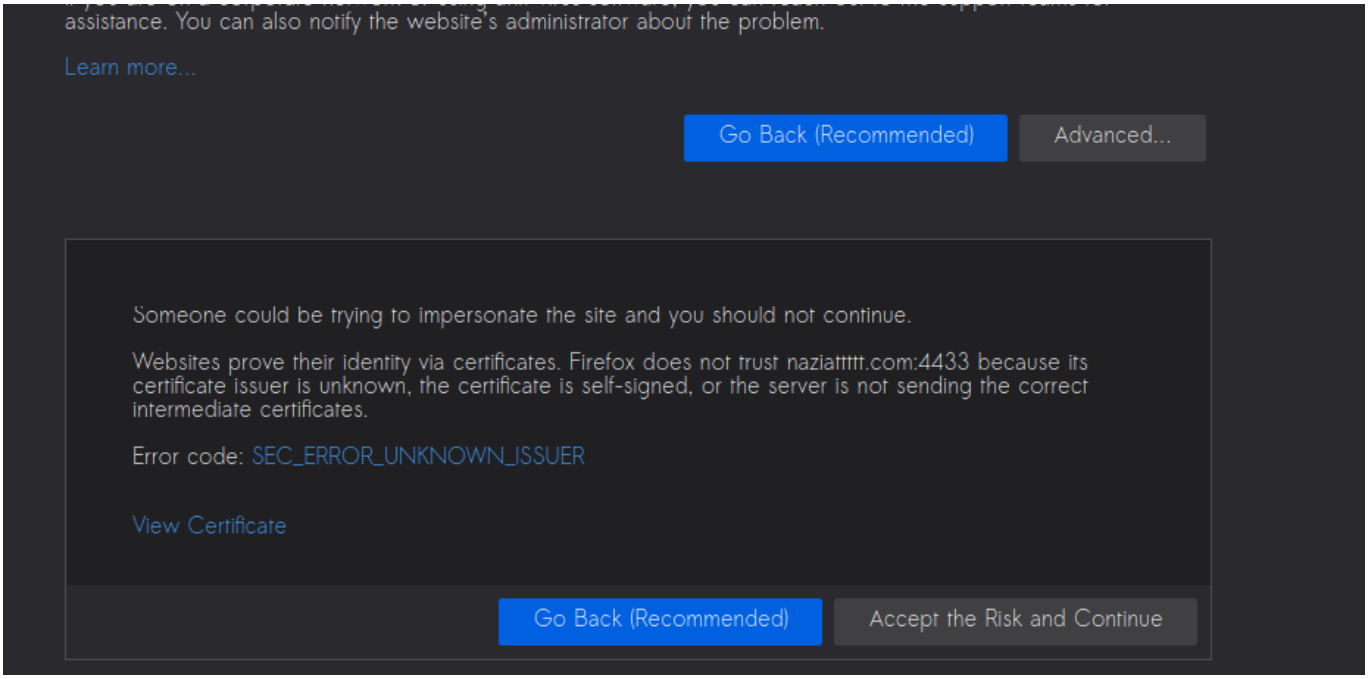
Using OpenSSL to demonstrate HTTPS

We run the following code to combine the certificate and key files and then launch the server using the certificate.

```
cp server.key server.pem
cat server.crt >> server.pem
openssl s_server -cert server.pem -www
```

When we visit `https://naziattttt.com:4433` the following error is shown in mozilla. This is certificate issuer not found error.


Warning: Potential Secur
https://naziatttttt.com:4433
Set Firefox as your default browser? Get fast, safe, and private browsing whenever you use the web.
Set as Default
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to naziatttttt.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...


assistance. You can also notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates. Firefox does not trust naziatttttt.com:4433 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.
Error code: SEC_ERROR_UNKNOWN_ISSUER
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

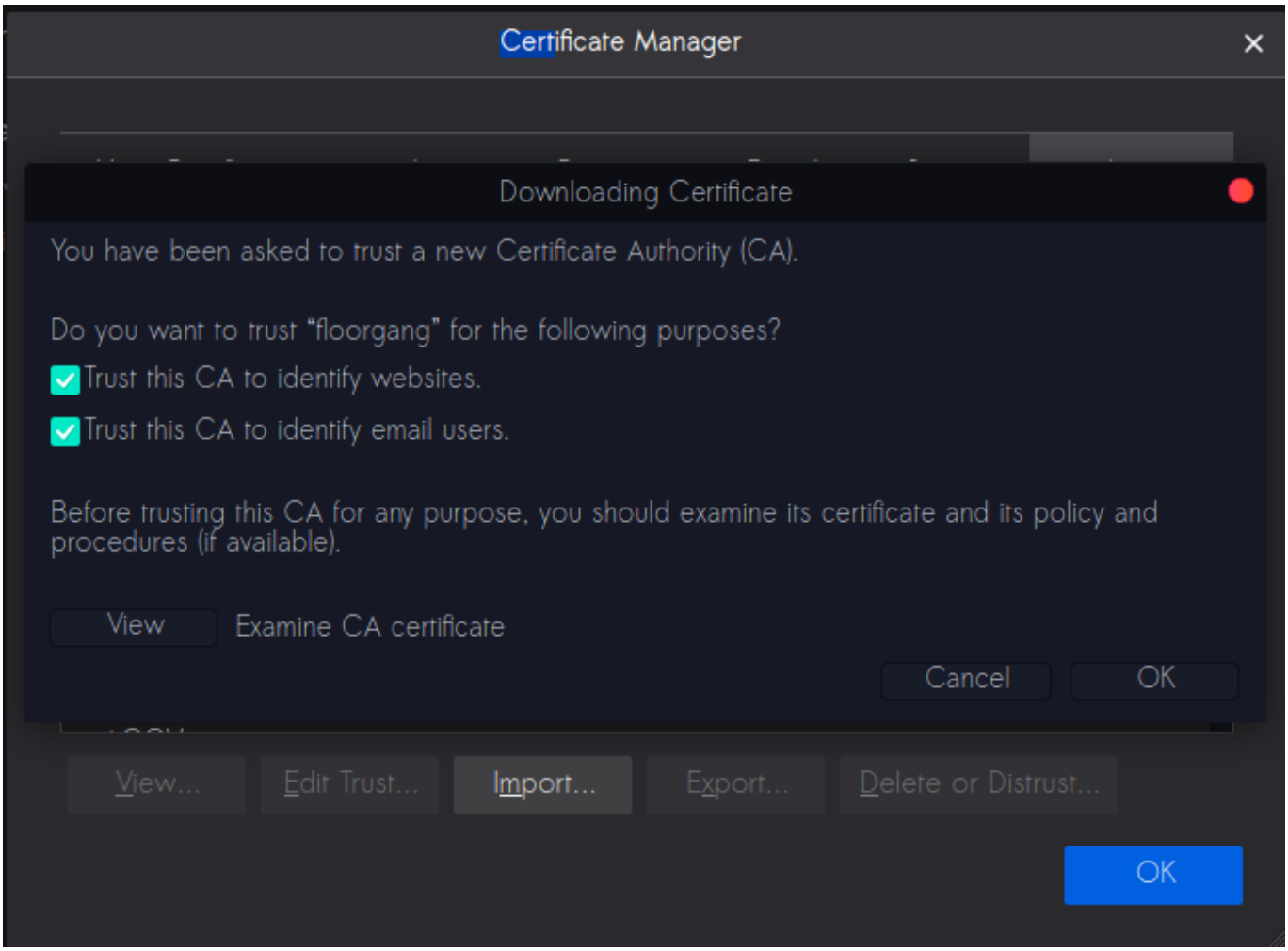
—

Task 3 Checkpoint 5

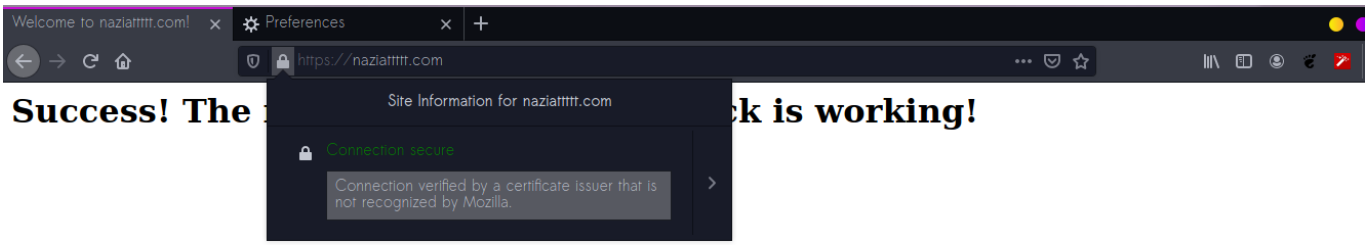
We update the configuration file at `etc/apache2/sites-available/naziattttt.com.conf` by adding the provided content.

```
appledora@appledore /etc/apache2/sites-available cat naziattttt.com.conf

<VirtualHost *:80>
ServerAdmin admin@naziattttt.com
ServerName naziattttt.com
ServerAlias www.naziattttt.com
DocumentRoot /var/www/naziattttt.com/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerAdmin admin@naziattttt.com
        ServerName naziattttt.com
        ServerAlias www.naziattttt.com
        DocumentRoot /var/www/naziattttt.com/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on
        SSLCertificateFile /home/appledora/Documents/Security2/lab5/server.crt
        SSLCertificateKeyFile /home/appledora/Documents/Security2/lab5/server.key

</VirtualHost>
```

Next, we import the certificate into mozilla.



Finally, when we visit `https://naziattttt.com` we can see the HTTPS secured tag.



Task 4 Checkpoint 6

To ensure the webserver always uses HTTPS, we will redirect the `http://naziattttt.com` to `https://naziattttt.com`. We add the following lines to the configuration file at `/etc/apache2/sites-available/naziattttt.com.conf`

After restarting the apache server, the http link successfully redirects to https.

Task 5 Checkpoint 7

We add users to our server using the given commands,

```
 appledora@appledore  /  sudo htpasswd -c /etc/apache2/.htpasswd sowmenD
New password:
Re-type new password:
Adding password for user sowmenD
 appledora@appledore  /  sudo htpasswd /etc/apache2/.htpasswd naziaT
New password:
Re-type new password:
Adding password for user naziaT
```

```
 appledora@appledore  /  cat /etc/apache2/.htpasswd
sowmenD:$apr1$BJiLx//x$hRgIs8f1Z1c7MeHcajjaQ.
naziaT:$apr1$flraJGnO$FamUACwZeVPTpWTb.nY7b0
```

Next, we add the new lines,

```
 GNU nano 2.9.3                          /etc/apache2/sites-available/naziattttt.com.conf

<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerAdmin admin@naziattttt.com
        ServerName naziattttt.com
        ServerAlias www.naziattttt.com
        DocumentRoot /var/www/naziattttt.com/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on
        SSLCertificateFile /home/appledora/Documents/Security2/lab5/server.crt
        SSLCertificateKeyFile /home/appledora/Documents/Security2/lab5/server.key

        <Directory "/var/www/naziattttt.com/html">
                AuthType Basic
                AuthName "Restricted Content"
                AuthUserFile /etc/apache2/.htpasswd
                Require valid-user
        </Directory>
</VirtualHost>
</IfModule>
```

Now, to access the site we need to provide a username and password.