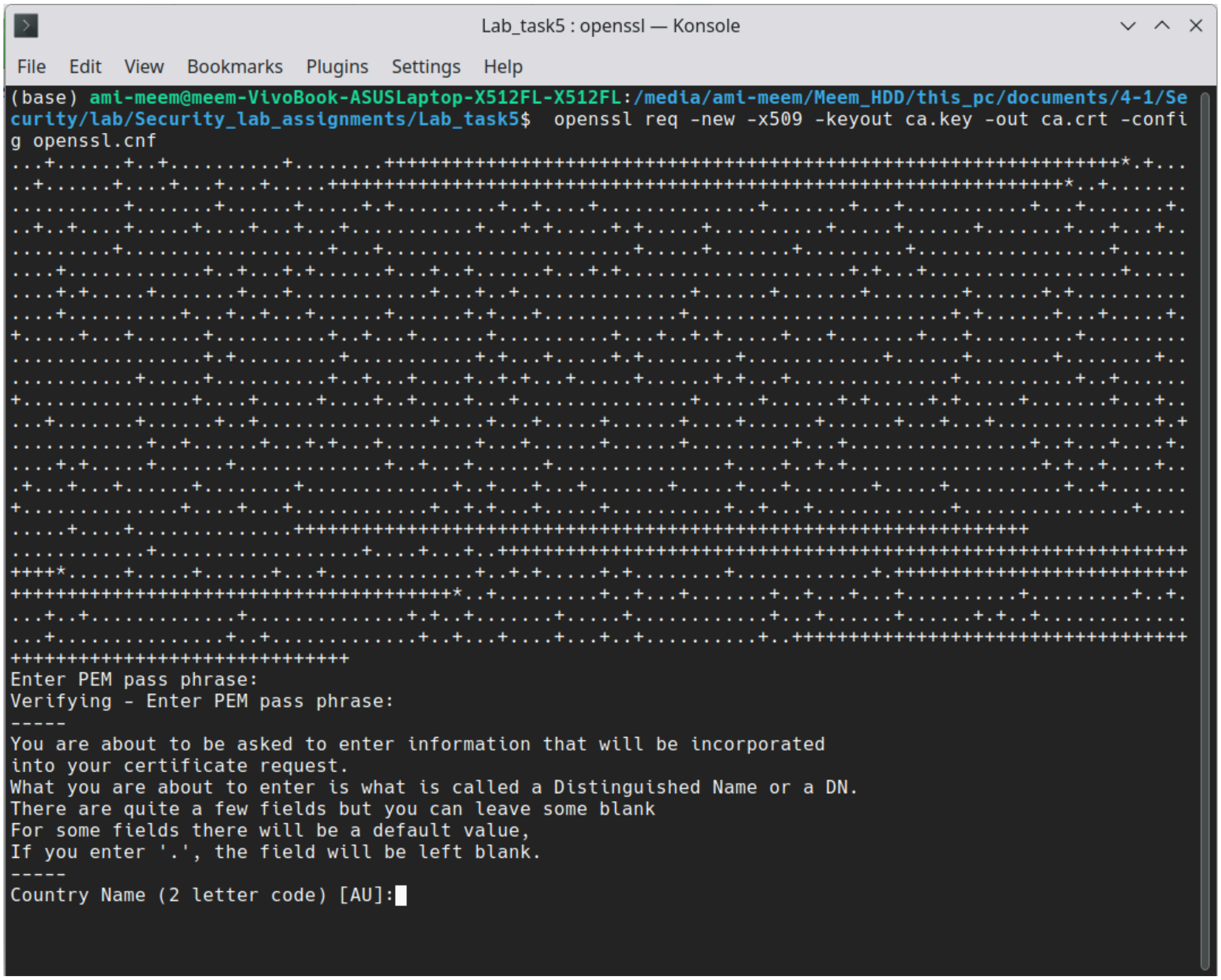
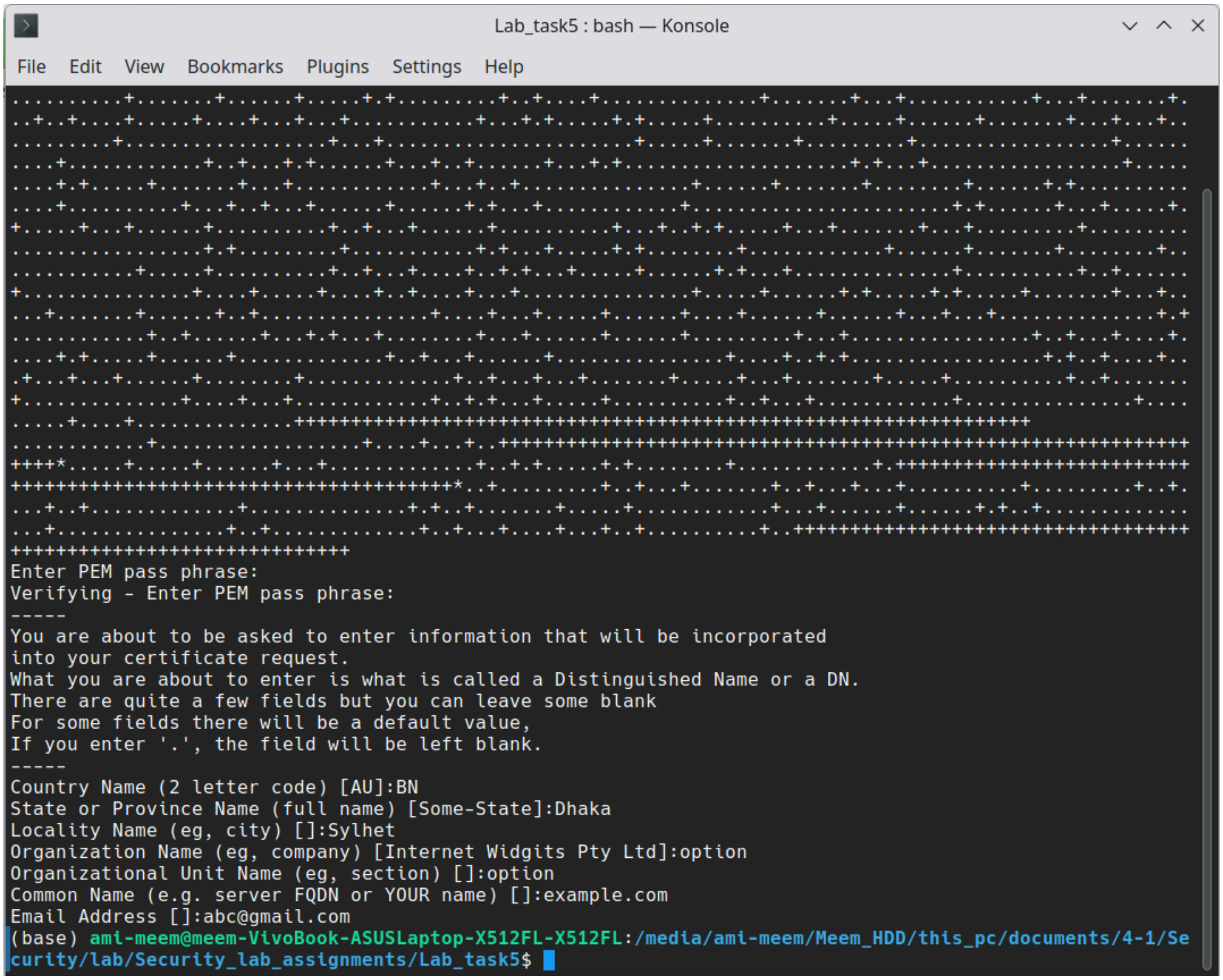
Task 1

1. Configure openssl.cnf
2. Generating certificate for CA

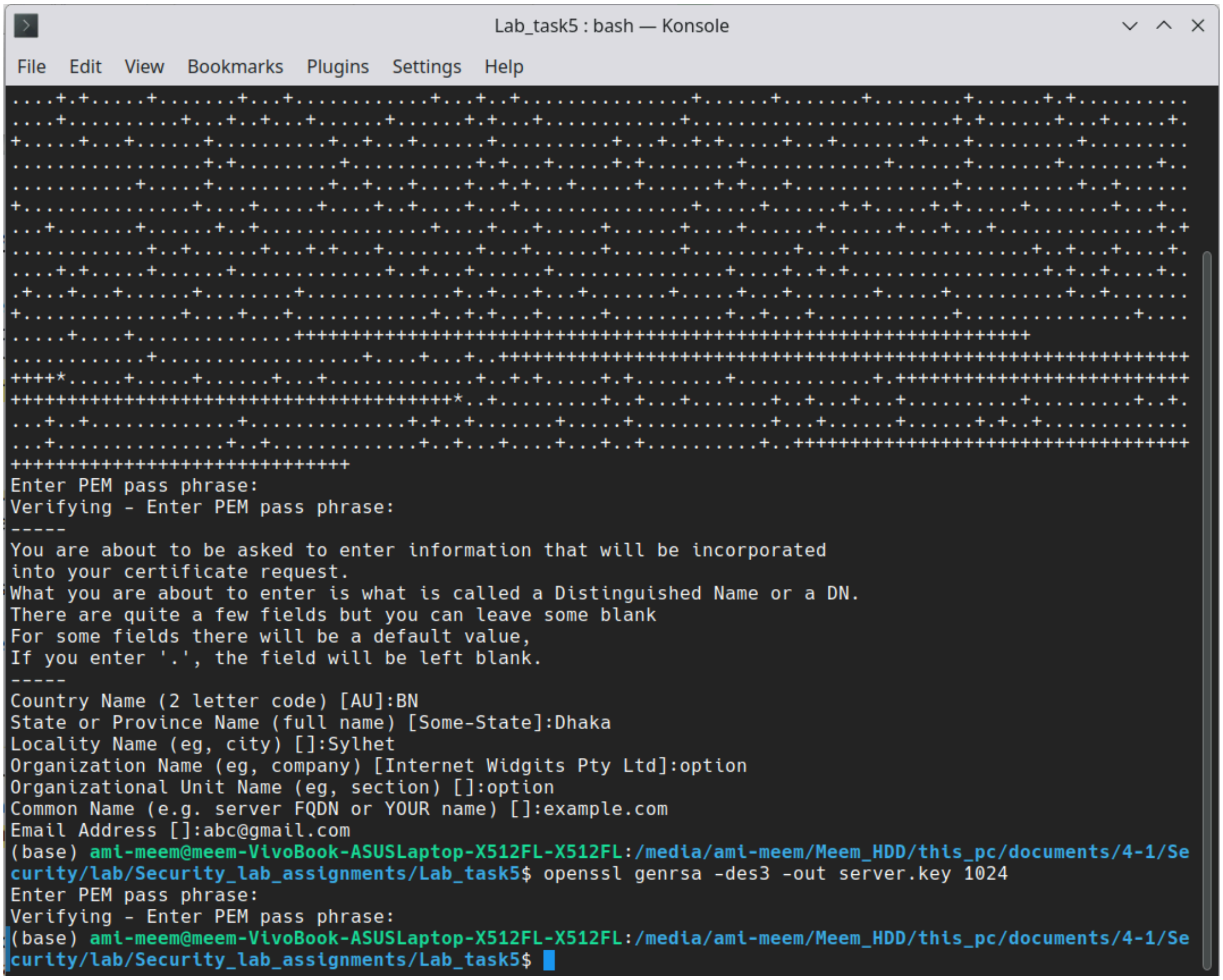

Lab_task5 : openssl — Konsole
File Edit View Bookmarks Plugins Settings Help

```
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$  openssl req -new -x509 -keyout ca.key -out ca.crt -confi
g openssl.cnf
...+......+..+..........+........+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+...
..+......+....+...+...+.....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+.......
..........+.......+......+.....+.+.........+..+....+..............+.......+...+...........+...+.......+.
..+..+....+.....+....+...+...+...........+...+.+.....+.+.....+..........+.....+......+.......+...+...+..
.........+..................+...+......................+.....+.......+.........+.................+......
....+............+..+...+.+......+...+..+......+...+.+....................+.+...+.................+.....
....+.+.....+.......+...+............+...+..+...............+......+.......+........+......+.+..........
....+..........+...+..+...+......+......+.+...+............+.......................+.+......+...+.....+.
+.....+...+......+..........+..+...+......+..........+...+.+..+.....+...+.......+...+.........+.........
.................+.+.........+...........+.+...+.....+.+........+............+......+.......+........+..
...........+.....+..........+..+...+....+..+.+...+.....+......+.+...+..............+..........+..+......
+...............+....+.....+....+..+....+...+...............+.....+......+.+.....+.+.....+.......+...+..
...+.......+......+..+...............+....+...+.....+......+....+......+......+...+...+..............+.+
............+..+......+...+.+...+........+...+......+......+.........+...+................+.+....+....+.
....+.+.....+......+.............+..+...+......+...............+....+..+.+.................+.+..+....+..
.+...+...+......+........+.............+..+...+...+.......+.....+...+.......+.....+..........+..+.......
+..............+....+...+............+..+.+...+.....+..........+..+...+............+...............+....
.....+....+..............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
............+..................+....+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++*.....+.....+......+...+.............+..+.+.....+.+........+............+.++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++*..+.........+..+...+.......+..+...+...+..........+.........+..+.
...+..+.............+..............+.+..+.......+.....+............+...+......+......+.+..+.............
...+...............+..+.............+..+...+....+...+.+...........+..+++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++
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]:
```

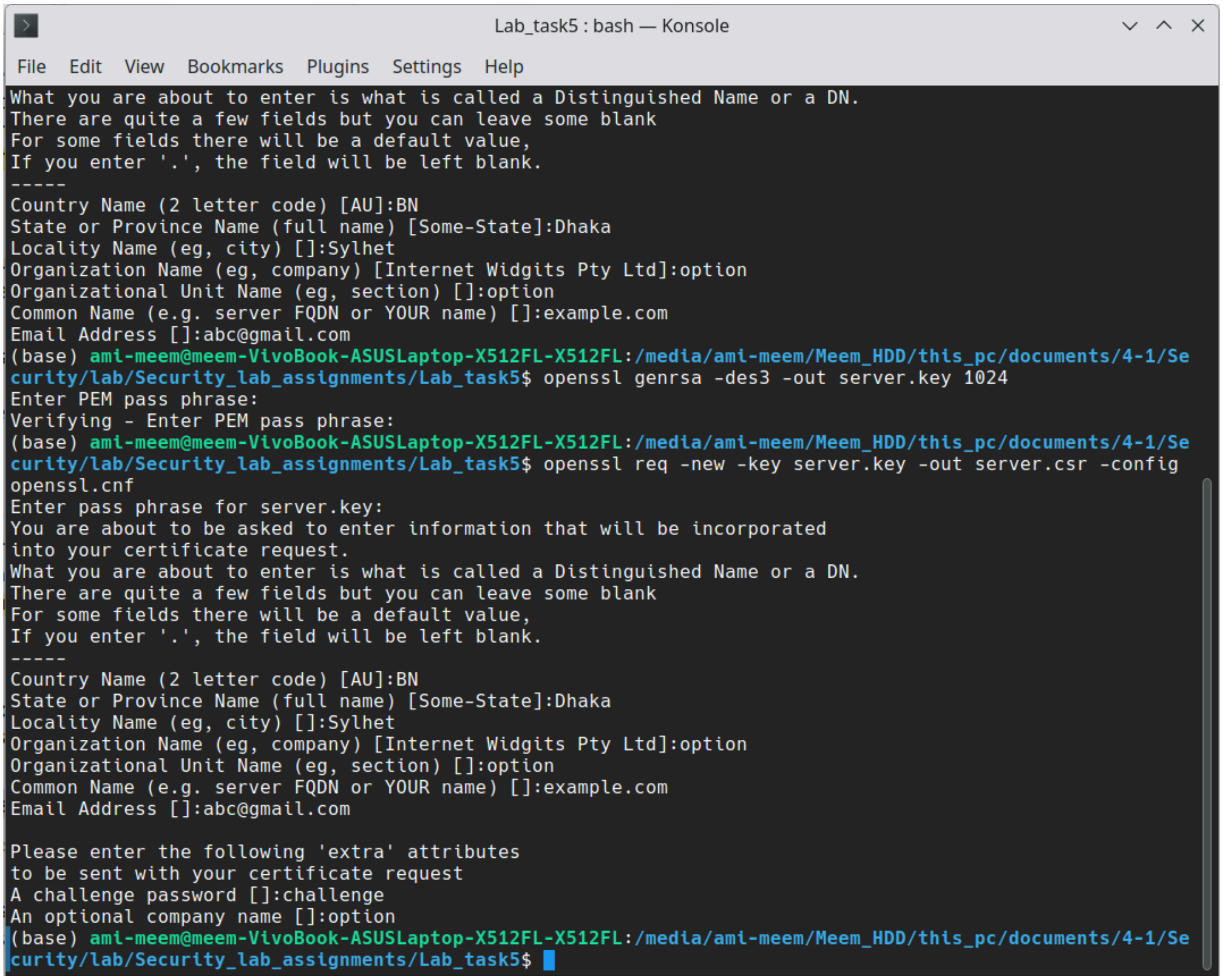

Lab_task5 : bash — Konsole
File Edit View Bookmarks Plugins Settings Help

```
..........+.......+......+.....+.+.........+..+....+..............+.......+...+...........+...+.......+.
..+..+....+.....+....+...+...+...........+...+.+.....+.+.....+..........+.....+......+.......+...+...+..
.........+..................+...+......................+.....+.......+.........+.................+......
....+............+..+...+.+......+...+..+......+...+.+....................+.+...+.................+.....
....+.+.....+.......+...+............+...+..+...............+......+.......+........+......+.+..........
....+..........+...+..+...+......+......+.+...+............+.......................+.+......+...+.....+.
+.....+...+......+..........+..+...+......+..........+...+..+.+.....+...+.......+...+.........+.........
.................+.+.........+...........+.+...+.....+.+........+............+......+.......+........+..
...........+.....+..........+..+...+....+..+.+...+.....+......+.+...+..............+..........+..+......
+...............+....+.....+....+..+....+...+...............+.....+......+.+.....+.+.....+.......+...+..
...+.......+......+..+...............+....+...+.....+......+....+......+......+...+...+..............+.+
............+..+......+...+.+...+........+..+.......+......+.........+...+................+..+...+....+.
....+.+.....+......+.............+..+...+......+...............+....+..+.+.................+.+..+....+..
.+...+...+......+........+.............+..+...+...+.......+.....+...+.......+.....+..........+..+.......
+..............+....+...+............+..+.+...+.....+..........+..+...+............+...............+....
.....+....+..............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
............+..................+....+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++*.....+.....+......+...+.............+..+.+.....+.+........+............+.++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++*..+.........+..+...+.......+..+...+...+..........+.........+..+.
...+..+.............+..............+.+..+.......+.....+............+...+......+......+.+..+.............
...+...............+..+.............+..+...+....+...+..+..........+..+++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++
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]:Dhaka
Locality Name (eg, city) []:Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:option
Organizational Unit Name (eg, section) []:option
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:abc@gmail.com
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$
```

3. Creating certificate for example.com



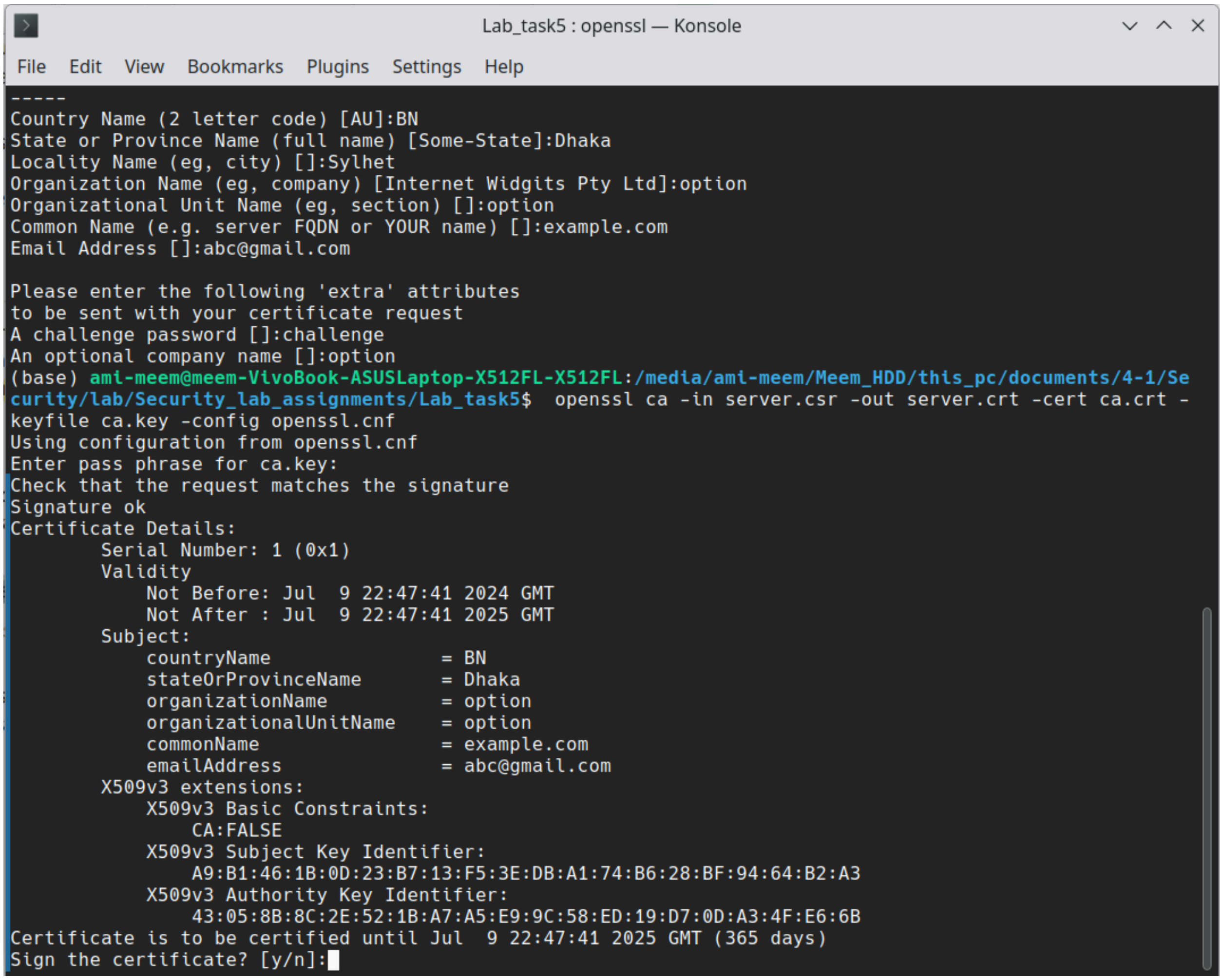
```
....+.+.....+.......+...+............+...+..+...............+......+.......+........+......+.+..........
....+..........+...+..+...+......+......+.+...+............+.......................+.+......+...+.....+.
+.....+...+......+..........+..+...+......+..........+...+..+.+.....+...+.......+...+.........+.........
.................+.+.........+...........+.+...+.....+.+........+............+......+.......+........+..
...........+.....+..........+..+...+....+..+.+...+.....+......+.+...+..............+..........+..+......
+...............+....+.....+....+..+....+...+...............+.....+......+.+.....+.+.....+.......+...+..
...+.......+......+..+...............+....+...+.....+......+....+......+......+...+...+..............+.+
............+..+......+...+.+...+........+...+......+......+.........+...+................+..+...+....+.
....+.+.....+......+.............+..+...+......+...............+....+..+.+.................+.+..+....+..
.+...+...+......+........+.............+..+...+...+.......+.....+...+.......+.....+..........+..+.......
+..............+....+...+............+..+.+...+.....+..........+..+...+............+...............+....
.....+....+..............+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
............+..................+....+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++*.....+.....+......+...+.............+..+.+.....+.+........+............+.++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++*..+.........+..+...+.......+..+...+...+..........+.........+..+.
...+..+.............+..............+.+..+.......+.....+............+...+......+......+.+..+.............
...+...............+..+.............+..+...+....+...+..+..........+..+++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++
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]:Dhaka
Locality Name (eg, city) []:Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:option
Organizational Unit Name (eg, section) []:option
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:abc@gmail.com
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ openssl genrsa -des3 -out server.key 1024
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$
```



Lab_task5 : bash — Konsole
File Edit View Bookmarks Plugins Settings Help

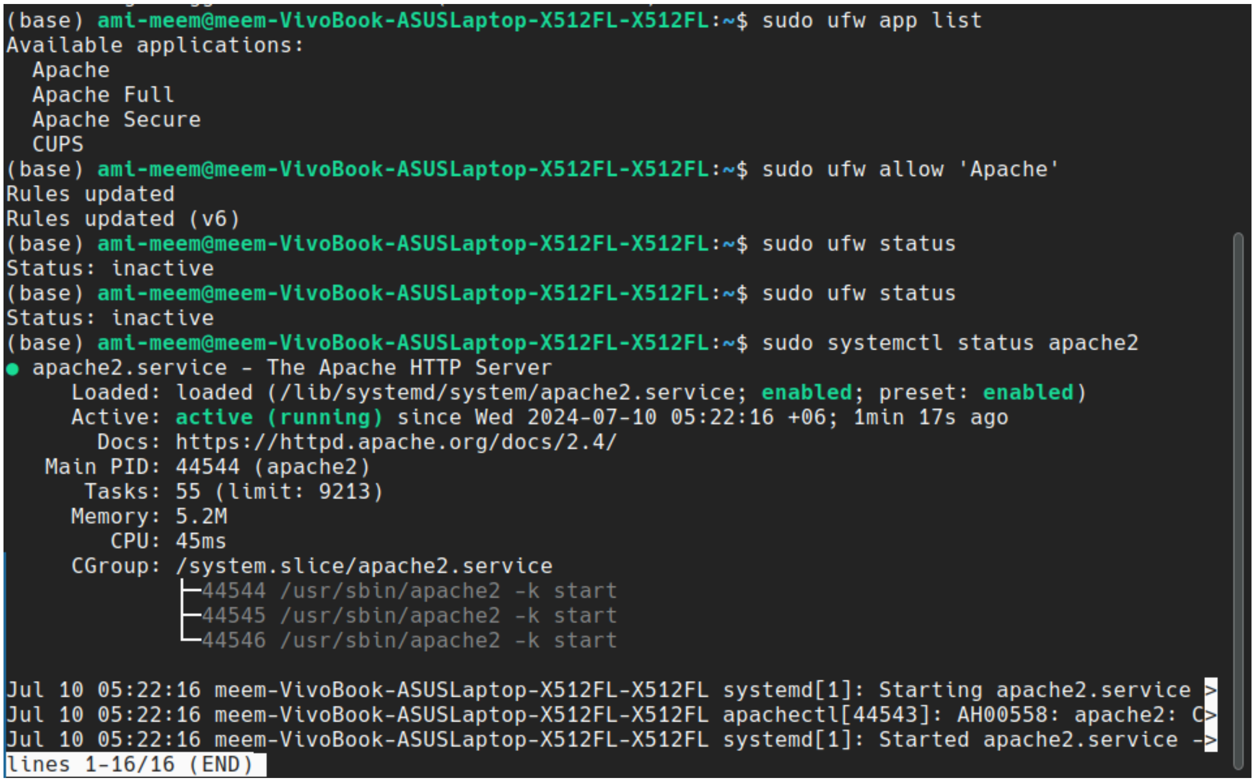
```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BN
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:option
Organizational Unit Name (eg, section) []:option
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:abc@gmail.com
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ openssl genrsa -des3 -out server.key 1024
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ openssl req -new -key server.key -out server.csr -config
openssl.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]:BN
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:option
Organizational Unit Name (eg, section) []:option
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:abc@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge
An optional company name []:option
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$
```

4. Generating certificates


Lab_task5 : openssl — Konsole
File Edit View Bookmarks Plugins Settings Help

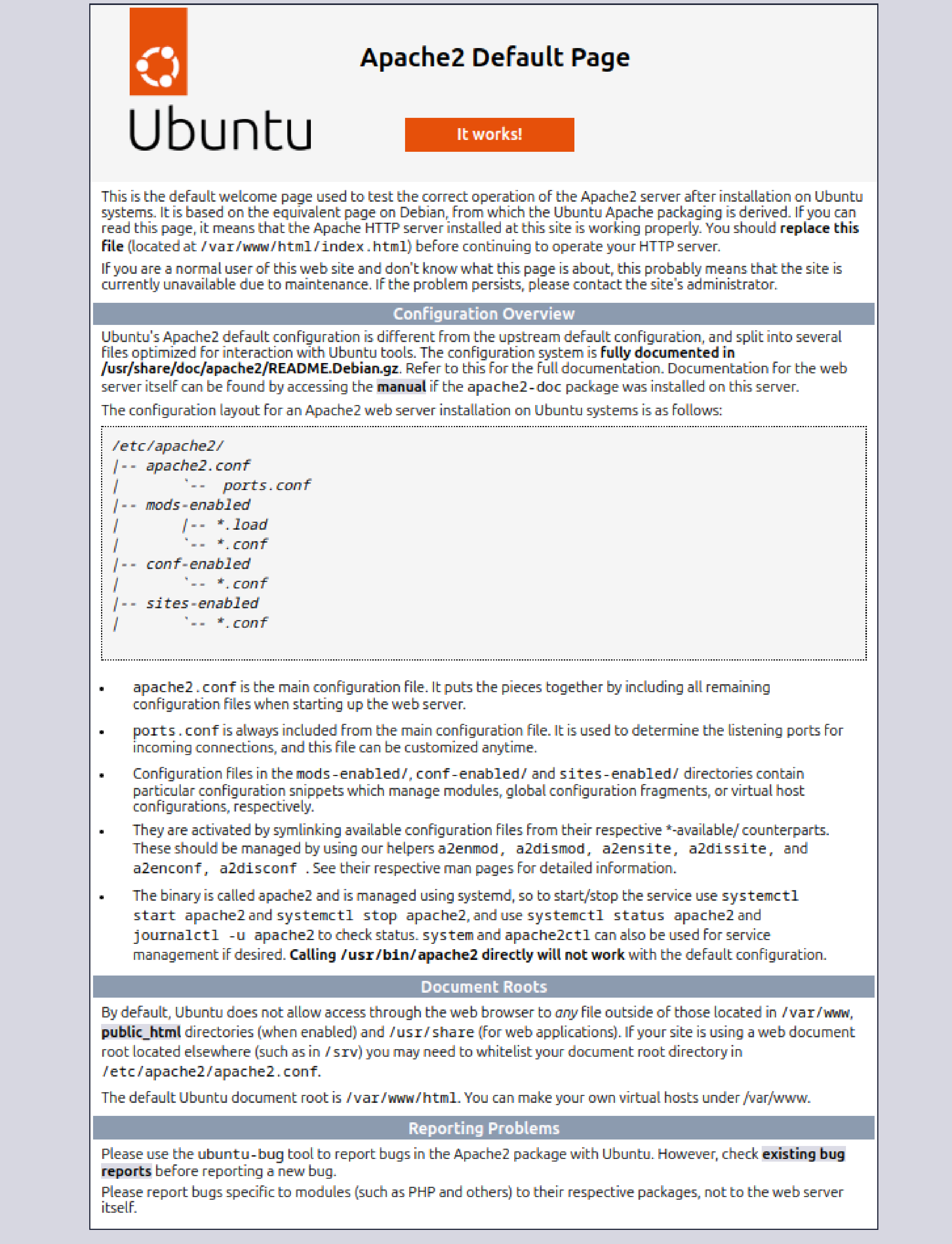
```
-----
Country Name (2 letter code) [AU]:BN
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Sylhet
Organization Name (eg, company) [Internet Widgits Pty Ltd]:option
Organizational Unit Name (eg, section) []:option
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:abc@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge
An optional company name []:option
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$  openssl ca -in server.csr -out server.crt -cert ca.crt -
keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jul  9 22:47:41 2024 GMT
            Not After : Jul  9 22:47:41 2025 GMT
        Subject:
            countryName               = BN
            stateOrProvinceName       = Dhaka
            organizationName          = option
            organizationalUnitName    = option
            commonName                = example.com
            emailAddress              = abc@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                A9:B1:46:1B:0D:23:B7:13:F5:3E:DB:A1:74:B6:28:BF:94:64:B2:A3
            X509v3 Authority Key Identifier:
                43:05:8B:8C:2E:52:1B:A7:A5:E9:9C:58:ED:19:D7:0D:A3:4F:E6:6B
Certificate is to be certified until Jul  9 22:47:41 2025 GMT (365 days)
Sign the certificate? [y/n]:
```

5. Setting up apache web server



```
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  CUPS
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ufw status
Status: inactive
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ufw status
Status: inactive
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-07-10 05:22:16 +06; 1min 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 44544 (apache2)
      Tasks: 55 (limit: 9213)
     Memory: 5.2M
        CPU: 45ms
     CGroup: /system.slice/apache2.service
             ├─44544 /usr/sbin/apache2 -k start
             ├─44545 /usr/sbin/apache2 -k start
             └─44546 /usr/sbin/apache2 -k start

Jul 10 05:22:16 meem-VivoBook-ASUSLaptop-X512FL-X512FL systemd[1]: Starting apache2.service >
Jul 10 05:22:16 meem-VivoBook-ASUSLaptop-X512FL-X512FL apachectl[44543]: AH00558: apache2: C>
Jul 10 05:22:16 meem-VivoBook-ASUSLaptop-X512FL-X512FL systemd[1]: Started apache2.service ->
lines 1-16/16 (END)
```

6.



Apache2 Default Page

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
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod, a2dismod, a2ensite, a2dissite,` and `a2enconf, a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2 and is managed using systemd, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `system` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

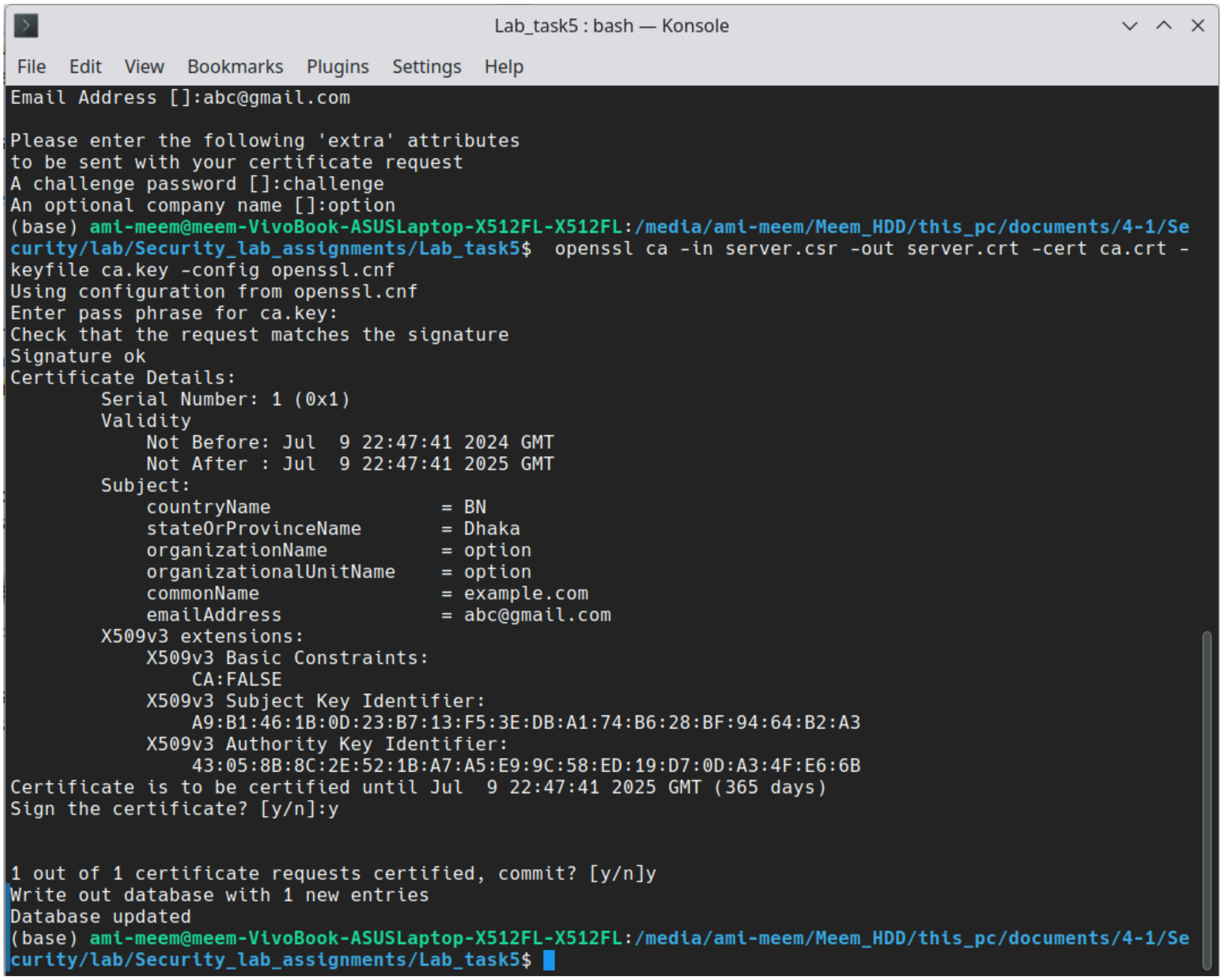
By default, Ubuntu does not allow access through the web browser to *any* file outside of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under /var/www.

Reporting Problems

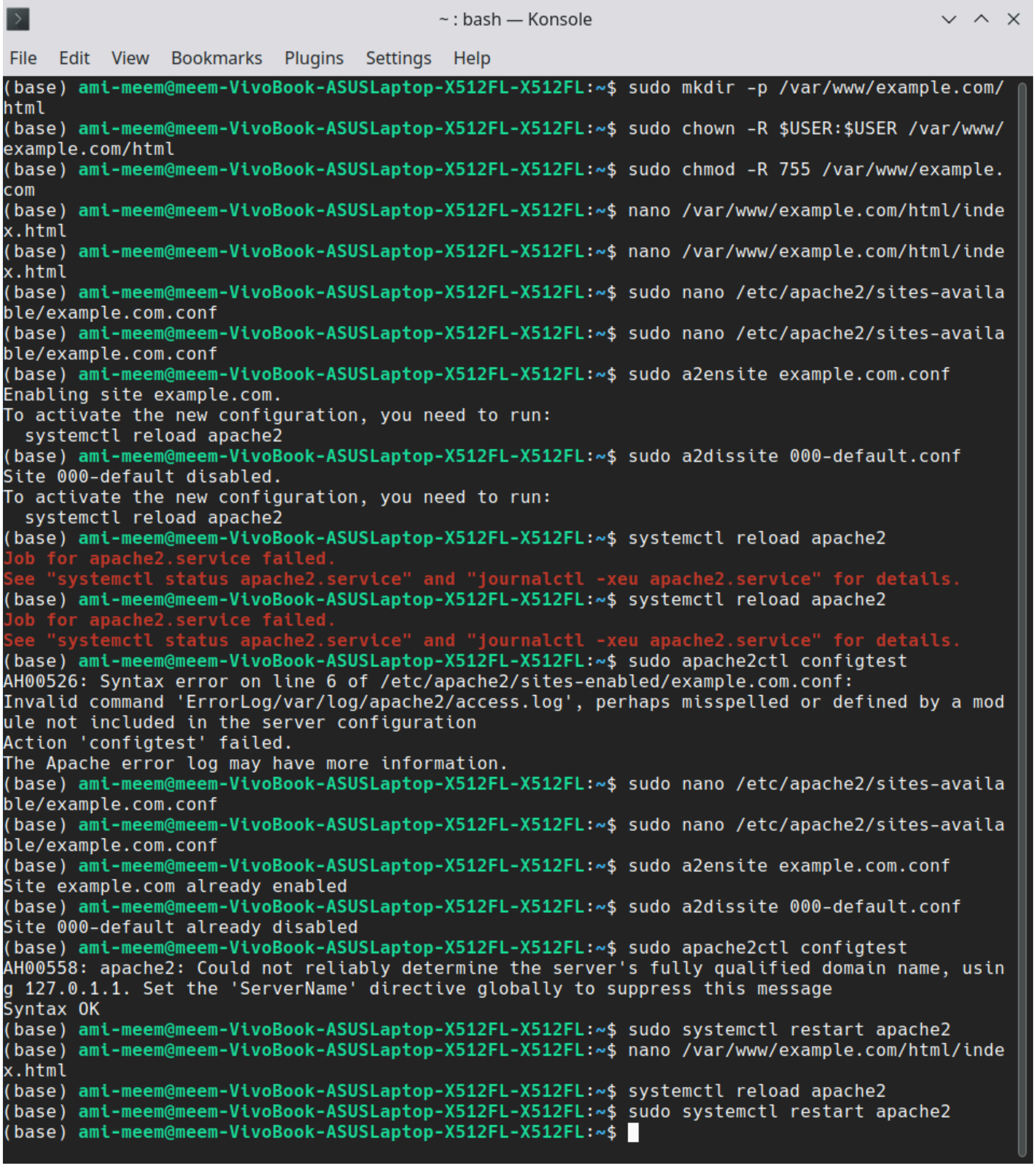
Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server itself.

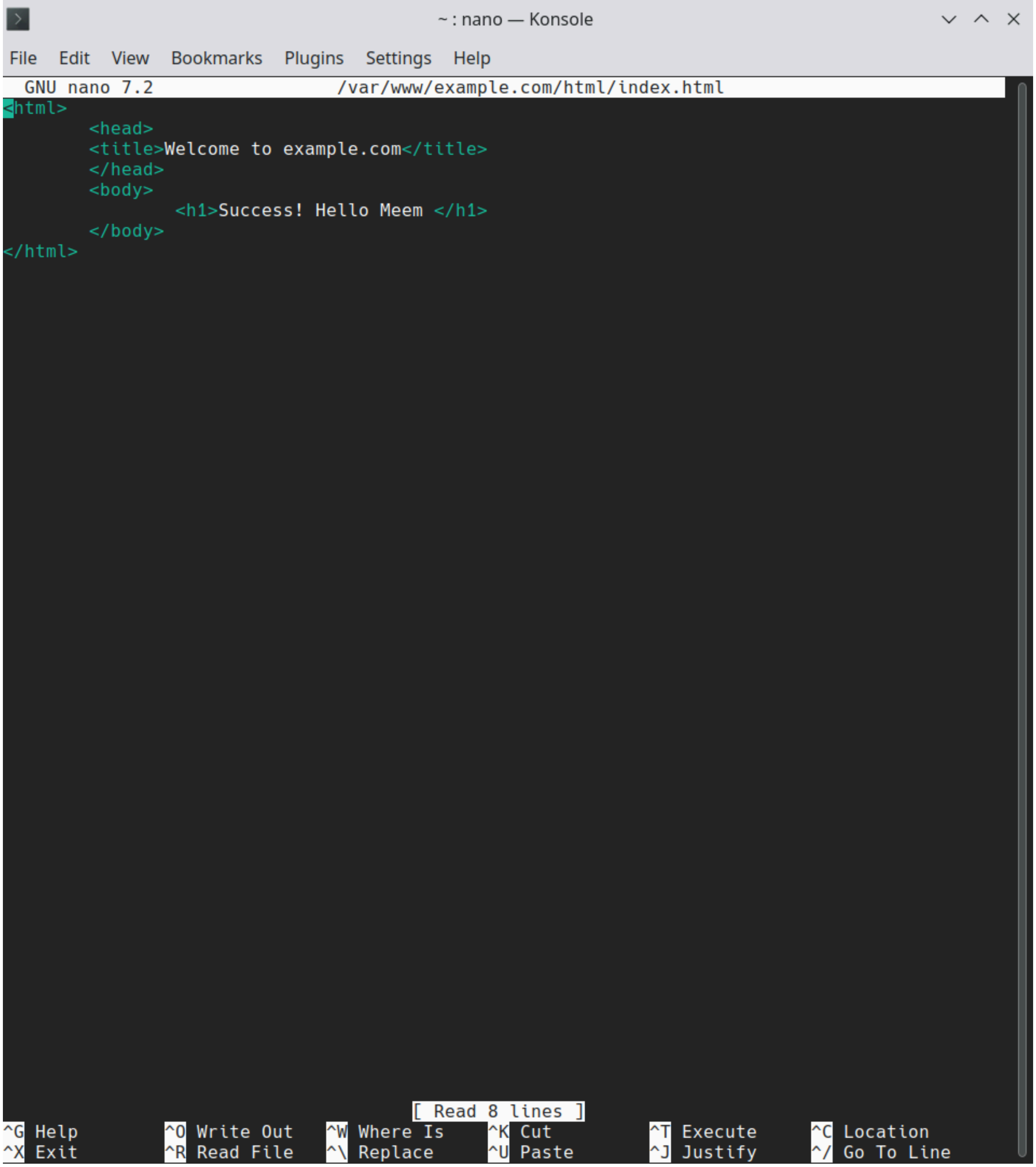


```
Email Address []:abc@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:challenge
An optional company name []:option
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$  openssl ca -in server.csr -out server.crt -cert ca.crt -
keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jul  9 22:47:41 2024 GMT
            Not After : Jul  9 22:47:41 2025 GMT
        Subject:
            countryName               = BN
            stateOrProvinceName       = Dhaka
            organizationName          = option
            organizationalUnitName    = option
            commonName                = example.com
            emailAddress              = abc@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                A9:B1:46:1B:0D:23:B7:13:F5:3E:DB:A1:74:B6:28:BF:94:64:B2:A3
            X509v3 Authority Key Identifier:
                43:05:8B:8C:2E:52:1B:A7:A5:E9:9C:58:ED:19:D7:0D:A3:4F:E6:6B
Certificate is to be certified until Jul  9 22:47:41 2025 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ 
```

6. Setting up host

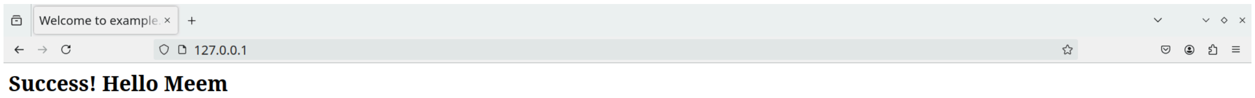


```
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo mkdir -p /var/www/example.com/
html
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo chown -R $USER:$USER /var/www/
example.com/html
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo chmod -R 755 /var/www/example.
com
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nano /var/www/example.com/html/inde
x.html
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nano /var/www/example.com/html/inde
x.html
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo nano /etc/apache2/sites-availa
ble/example.com.conf
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo nano /etc/apache2/sites-availa
ble/example.com.conf
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo a2ensite example.com.conf
Enabling site example.com.
To activate the new configuration, you need to run:
  systemctl reload apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ systemctl reload apache2
Job for apache2.service failed.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ systemctl reload apache2
Job for apache2.service failed.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo apache2ctl configtest
AH00526: Syntax error on line 6 of /etc/apache2/sites-enabled/example.com.conf:
Invalid command 'ErrorLog/var/log/apache2/access.log', perhaps misspelled or defined by a mod
ule not included in the server configuration
Action 'configtest' failed.
The Apache error log may have more information.
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo nano /etc/apache2/sites-availa
ble/example.com.conf
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo nano /etc/apache2/sites-availa
ble/example.com.conf
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo a2ensite example.com.conf
Site example.com already enabled
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo a2dissite 000-default.conf
Site 000-default already disabled
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, usin
g 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo systemctl restart apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nano /var/www/example.com/html/inde
x.html
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ systemctl reload apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo systemctl restart apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ 
```



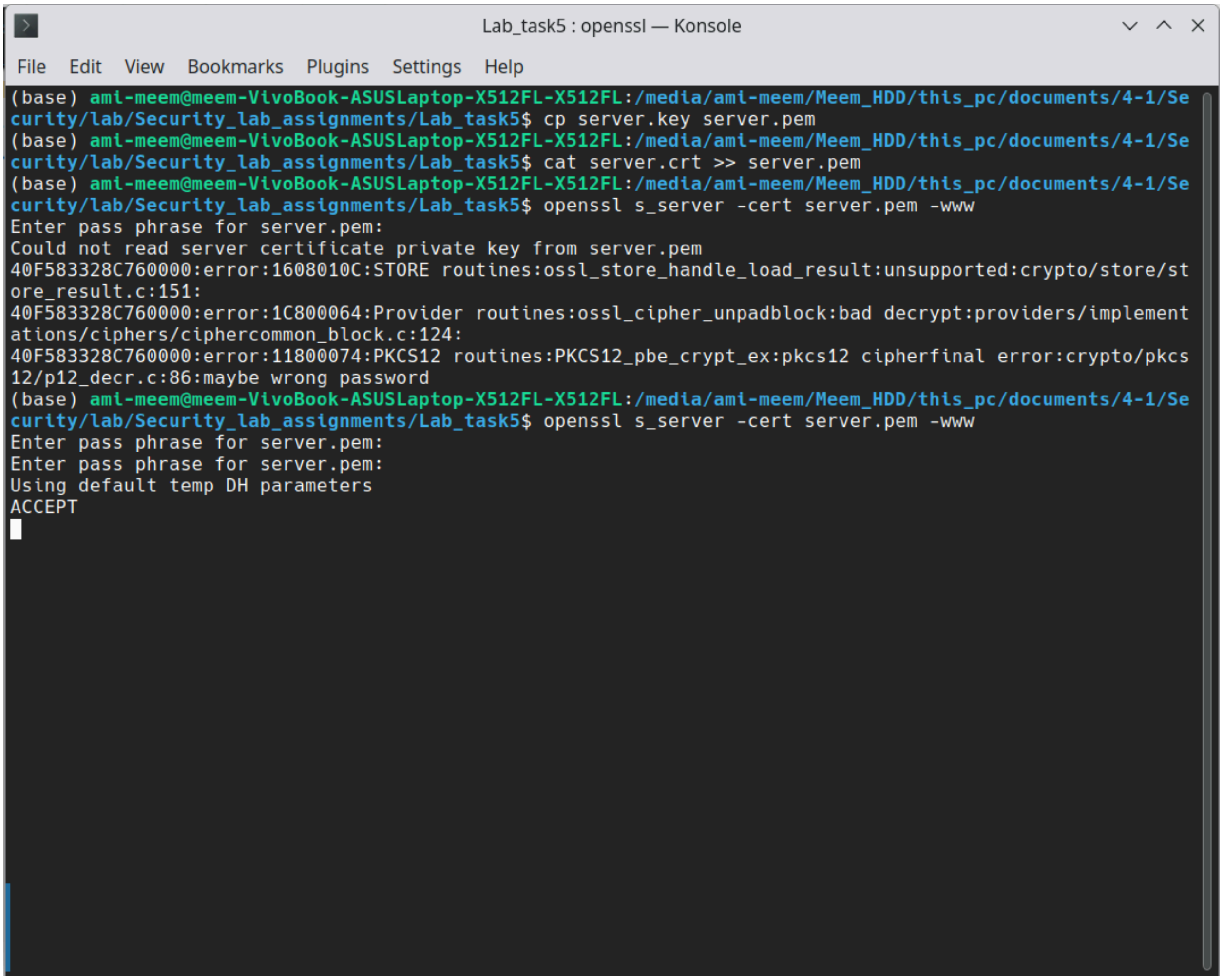
```
  GNU nano 7.2                 /var/www/example.com/html/index.html
<html>
        <head>
        <title>Welcome to example.com</title>
        </head>
        <body>
                <h1>Success! Hello Meem </h1>
        </body>
</html>
```

```
                                      [ Read 8 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line
```



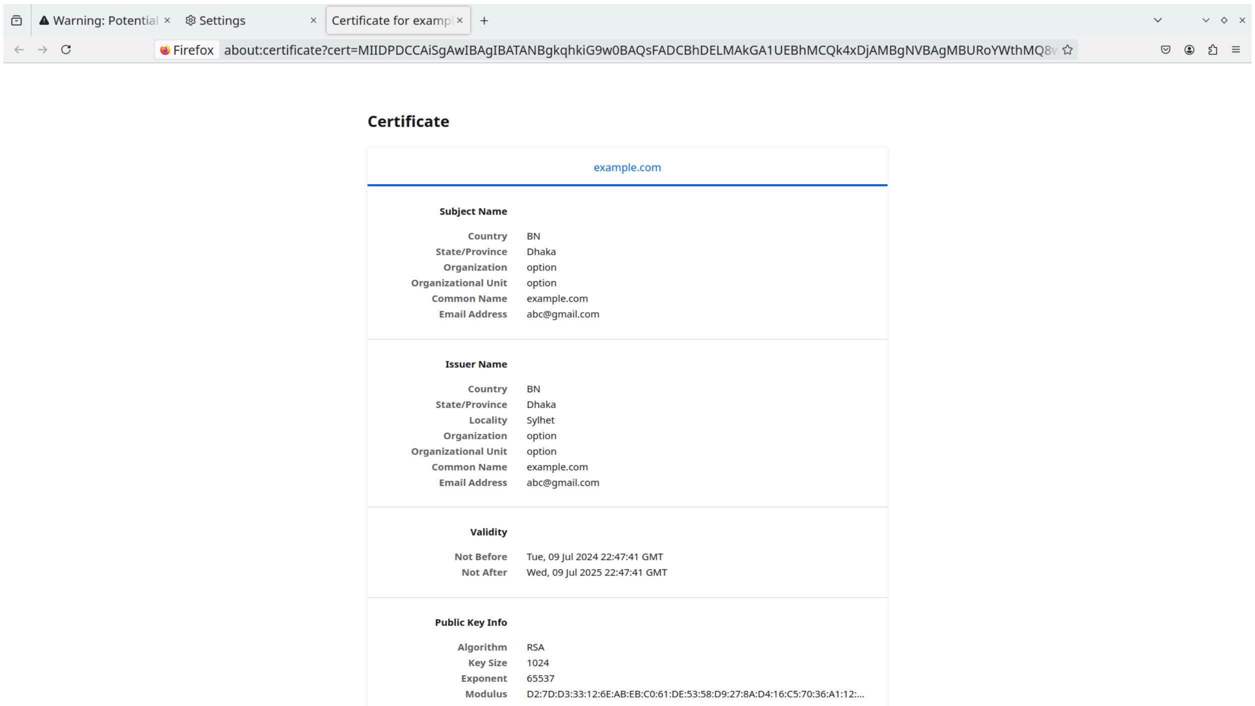
Success! Hello Meem

7. Lauch a server


Lab_task5 : openssl — Konsole
File Edit View Bookmarks Plugins Settings Help

```
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ cp server.key server.pem
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ cat server.crt >> server.pem
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40F583328C760000:error:1608010C:STORE routines:ossl_store_handle_load_result:unsupported:crypto/store/st
ore_result.c:151:
40F583328C760000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:providers/implement
ations/ciphers/ciphercommon_block.c:124:
40F583328C760000:error:11800074:PKCS12 routines:PKCS12_pbe_crypt_ex:pkcs12 cipherfinal error:crypto/pkcs
12/p12_decr.c:86:maybe wrong password
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:/media/ami-meem/Meem_HDD/this_pc/documents/4-1/Se
curity/lab/Security_lab_assignments/Lab_task5$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

7. Certificate in firefox browser


Warning: Potential
Settings
Certificate for exampl
Firefox
about:certificate?cert=MIIDPDCCAiSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UEBhMCQk4xDjAMBgNVBAgMBURoYWthMQ8v

Certificate

example.com

Subject Name

Country	BN
State/Province	Dhaka
Organization	option
Organizational Unit	option
Common Name	example.com
Email Address	abc@gmail.com

Issuer Name

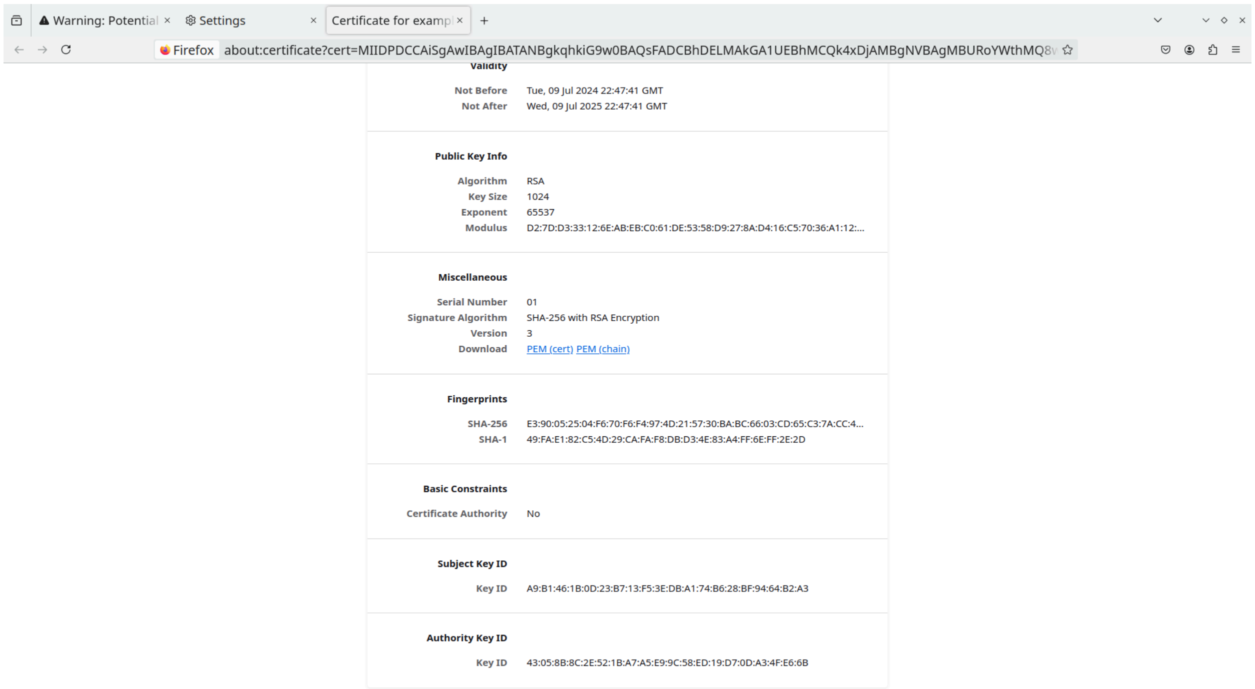
Country	BN
State/Province	Dhaka
Locality	Sylhet
Organization	option
Organizational Unit	option
Common Name	example.com
Email Address	abc@gmail.com

Validity

Not Before	Tue, 09 Jul 2024 22:47:41 GMT
Not After	Wed, 09 Jul 2025 22:47:41 GMT

Public Key Info

Algorithm	RSA
Key Size	1024
Exponent	65537
Modulus	D2:7D:D3:33:12:6E:AB:EB:C0:61:DE:53:58:D9:27:8A:D4:16:C5:70:36:A1:12:...


Warning: Potential
Settings
Certificate for exampl
Firefox
about:certificate?cert=MIIDPDCCAiSgAwIBAgIBATANBgkqhkiG9w0BAQsFADCBhDELMAkGA1UEBhMCQk4xDjAMBgNVBAgMBURoYWthMQ8v

Validity

Not Before	Tue, 09 Jul 2024 22:47:41 GMT
Not After	Wed, 09 Jul 2025 22:47:41 GMT

Public Key Info

Algorithm	RSA
Key Size	1024
Exponent	65537
Modulus	D2:7D:D3:33:12:6E:AB:EB:C0:61:DE:53:58:D9:27:8A:D4:16:C5:70:36:A1:12:...

Miscellaneous

Serial Number	01
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	E3:90:05:25:04:F6:70:F6:F4:97:4D:21:57:30:BA:BC:66:03:CD:65:C3:7A:CC:4...
SHA-1	49:FA:E1:82:C5:4D:29:CA:FA:F8:DB:D3:4E:83:A4:FF:6E:FF:2E:2D

Basic Constraints

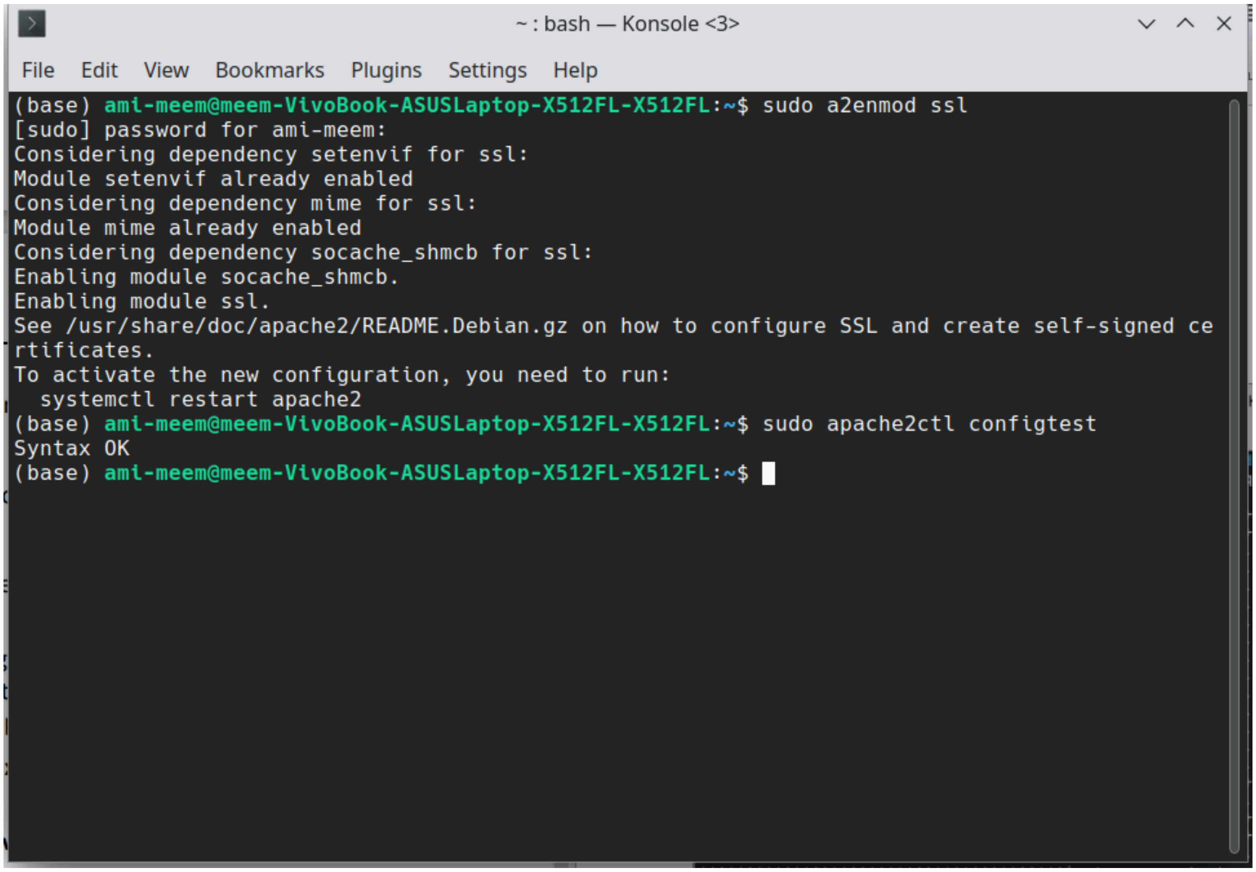
Certificate Authority	No

Subject Key ID

Key ID	A9:B1:46:1B:0D:23:B7:13:F5:3E:DB:A1:74:B6:28:BF:94:64:B2:A3

Authority Key ID

Key ID	43:05:8B:8C:2E:52:1B:A7:A5:E9:9C:58:ED:19:D7:0D:A3:4F:E6:6B



```
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo a2enmod ssl
[sudo] password for ami-meem:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed ce
rtificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo apache2ctl configtest
Syntax OK
(base) ami-meem@meem-VivoBook-ASUSLaptop-X512FL-X512FL:~$ 
```