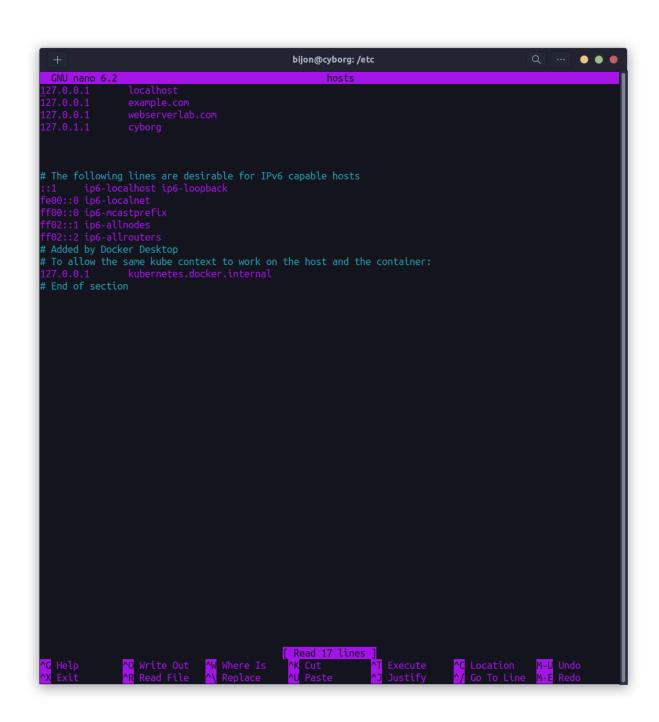
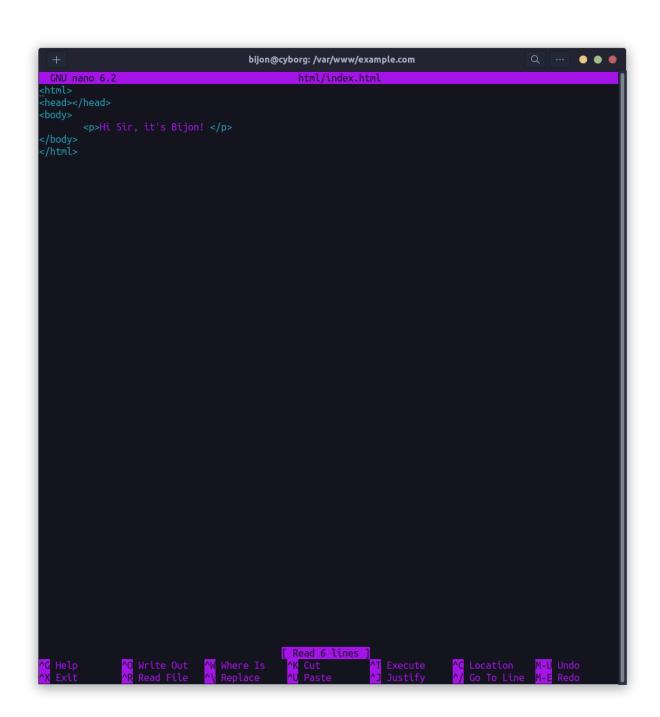
Lab 5- : Setting up an Apache web server
Bijon Saha
2019831007





```
Enter PEM pass phrase:
/erifying - 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]:BD
State or Province Name (full name) [Some-State]:Mymensingh
Locality Name (eg, city) []:Muktagacha
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUST
Organizational Unit Name (eg, section) []:SWE
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
bijon@cyborg:~/lab5$
```

```
Verifying - Enter PEM pass phrase:

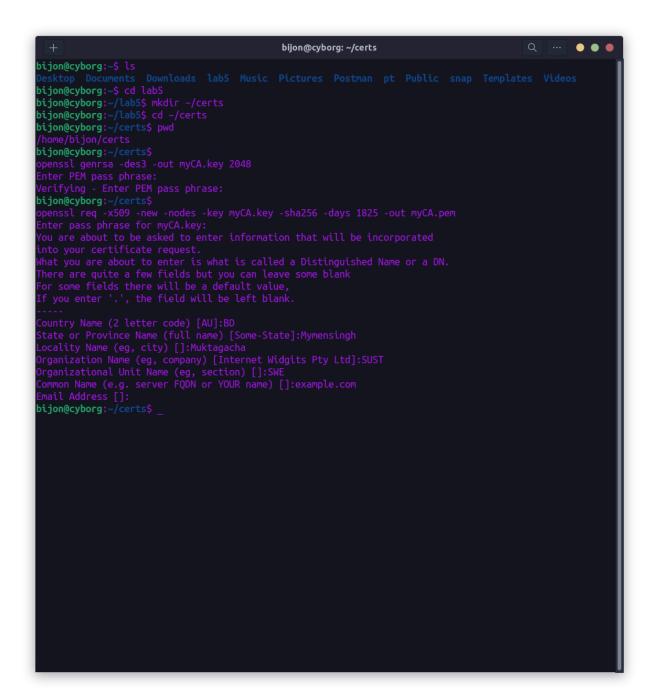
bijon@cyborg:~/lab5$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
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]:BD
State or Province Name (full name) [Some-State]:Mymensingh
Locality Name (eg, city) []:Muktagacha
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUST
Organizational Unit Name (eg, section) []:SWE
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bijon
An optional company name []:
bijon@cyborg:~/lab5$ _
```

```
bijon@cyborg: ~/lab5
bijon@cyborg:~/lab5$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config opens
bijon@cyborg:~/lab5$ _
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
bijon@cyborg:~/lab5$ cp server.key server.pem
bijon@cyborg:~/lab5$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Enter pass phrase for server.pem:
Could not read server certificate private key from server.pem
40079F2837790000:error:1608010C:STORE routines:ossl_store_handle_load_result:unsupported:../crypto/store/store_result.c:151:
40079F2837790000:error:07880109:common libcrypto routines:do_ui_passphrase:interrupted or cancelled:../crypto/passphrase.c:184:
40079F2837790000:error:1C80009F:Provider routines:epki2pki_decode:unable to get passphrase:../providers/mplementations/encode_decode/decode_epki2pki.c:96:
bijon@cyborg:~/lab5$ cat server.crt >> server.pem
bijon@cyborg:~/lab5$ 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
```

```
s server -cert server.pem -www
Secure Renegotiation IS NOT supported
Ciphers supported in s server binary
TLSv1.3
            :TLS AES 256 GCM SHA384
                                        TLSv1.3
                                                    :TLS CHACHA20 POLY1305 SHA256
            :TLS AES 128 GCM SHA256
TLSv1.3
                                         TLSv1.2
                                                    : ECDHE - ECDSA - AES256 - GCM - SHA384
TLSv1.2
            :ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2
                                                       : DHE - RSA - AES256 - GCM - SHA384
TLSv1.2
            :ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2
                                                         : ECDHE - RSA - CHACHA20 - POLY1305
TLSv1.2
            :DHE-RSA-CHACHA20-POLY1305 TLSv1.2
                                                     : ECDHE - ECDSA - AES128 - GCM - SHA256
                                                       :DHE-RSA-AES128-GCM-SHA256
TLSv1.2
            :ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
TLSv1.2
            :ECDHE-ECDSA-AES256-SHA384 TLSv1.2
                                                     : ECDHE-RSA-AES256-SHA384
TLSv1.2
            :DHE-RSA-AES256-SHA256
                                         TLSv1.2
                                                     : ECDHE - ECDSA - AES128 - SHA256
                                         TLSv1.2
                                                     :DHE-RSA-AES128-SHA256
TLSv1.2
            : ECDHE-RSA-AES128-SHA256
TLSv1.0
            : ECDHE - ECDSA - AES256 - SHA
                                         TLSv1.0
                                                     : ECDHE - RSA - AES256 - SHA
SSLv3
            : DHE - RSA - AES256 - SHA
                                         TLSv1.0
                                                     : ECDHE - ECDSA - AES128 - SHA
TLSv1.0
            : ECDHE - RSA - AES128 - SHA
                                                    :DHE-RSA-AES128-SHA
                                         SSLv3
TLSv1.2
            :RSA-PSK-AES256-GCM-SHA384 TLSv1.2
                                                     :DHE-PSK-AES256-GCM-SHA384
TLSv1.2
            :RSA-PSK-CHACHA20-POLY1305 TLSv1.2
                                                     : DHE - PSK - CHACHA20 - POLY1305
TLSv1.2
                                                       : AES256-GCM-SHA384
            :ECDHE-PSK-CHACHA20-POLY1305 TLSv1.2
TLSv1.2
            :PSK-AES256-GCM-SHA384
                                        TLSv1.2
                                                    : PSK-CHACHA20-POLY1305
TLSv1.2
            :RSA-PSK-AES128-GCM-SHA256 TLSv1.2
                                                    :DHE-PSK-AES128-GCM-SHA256
            :AES128-GCM-SHA256
                                                     :PSK-AES128-GCM-SHA256
TLSv1.2
                                         TLSv1.2
            :AES256-SHA256
TLSv1.2
                                         TLSv1.2
                                                     : AES128 - SHA256
TLSv1.0
            :ECDHE-PSK-AES256-CBC-SHA384 TLSv1.0
                                                       : ECDHE-PSK-AES256-CBC-SHA
SSLv3
            :SRP-RSA-AES-256-CBC-SHA
                                        SSLv3
                                                     :SRP-AES-256-CBC-SHA
TLSv1.0
            :RSA-PSK-AES256-CBC-SHA384 TLSv1.0
                                                     :DHE-PSK-AES256-CBC-SHA384
                                                     :DHE-PSK-AES256-CBC-SHA
            :RSA-PSK-AES256-CBC-SHA
SSLv3
                                         SSLv3
                                         TLSv1.0
SSLv3
            : AES256 - SHA
                                                     :PSK-AES256-CBC-SHA384
SSLv3
            : PSK - AES256 - CBC - SHA
                                         TLSv1.0
                                                    : ECDHE - PSK - AES128 - CBC - SHA256
                                                     :SRP-RSA-AES-128-CBC-SHA
TLSv1.0
            : ECDHE-PSK-AES128-CBC-SHA
                                        SSLv3
            :SRP-AES-128-CBC-SHA
                                         TLSv1.0
                                                     :RSA-PSK-AES128-CBC-SHA256
SSLv3
TLSv1.0
                                                    :RSA-PSK-AES128-CBC-SHA
            :DHE-PSK-AES128-CBC-SHA256 SSLv3
SSLv3
            : DHE - PSK - AES128 - CBC - SHA
                                         SSLv3
                                                    : AES128 - SHA
TLSv1.0
           :PSK-AES128-CBC-SHA256
                                         SSLv3
                                                    :PSK-AES128-CBC-SHA
Ciphers common between both SSL end points:
TLS AES 128 GCM SHA256
                            TLS_AES_256_GCM_SHA384
                                                          TLS CHACHA20 POLY1305 SHA256
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-CHACHA20-POLY1305
ECDHE-RSA-AES128-SHA
                            ECDHE-RSA-AES256-SHA
                                                          AES128-GCM-SHA256
AES256-GCM-SHA384
                            AES128-SHA
                                                          AES256-SHA
Signature Algorithms: ECDSA+SHA256:RSA-PSS+SHA256:RSA+SHA256:ECDSA+SHA384:RSA-PSS+SHA384:RS
Shared Signature Algorithms: ECDSA+SHA256:RSA-PSS+SHA256:RSA+SHA256:ECDSA+SHA384:RSA-PSS+SH
Supported groups: ::x25519:secp256r1:secp384r1
Shared groups: x25519:secp256r1:secp384r1
```



```
Use 'sudo apt autoremove' to remove it.

0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

bijon@cyborg:~/certs$ sudo cp ~/certs/myCA.pem /usr/local/share/ca-certificates/myCA.crt

bijon@cyborg:~/certs$ sudo update-ca-certificates

Updating certificates in /etc/ssl/certs...

rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL

1 added, 0 removed; done.

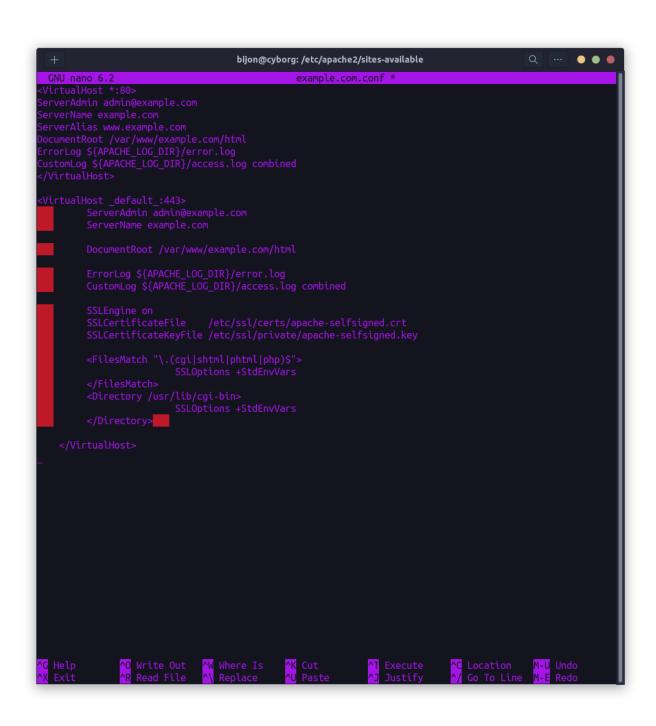
Running hooks in /etc/ca-certificates/update.d...

Adding debian:myCA.pem

done.

done.

bijon@cyborg:~/certs$ _
```



```
Hi Sir, it's Dijonal

bi_jonic/paper; inter_jonation_jonic_jonic_partiallaties_sudo rhod1 = p_inter_jonic_jonic_partiallaties_sudo rhod2 = p_inter_jonic_jonic_partiallaties_sudo chod2 = p_inter_jonic_jonic_partiallaties_sudo chod2 = p_inter_jonic_jonic_partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo chod2 = p_inter_jonic_partiallaties_sudo partiallaties_sudo partiallaties_sudo
```

