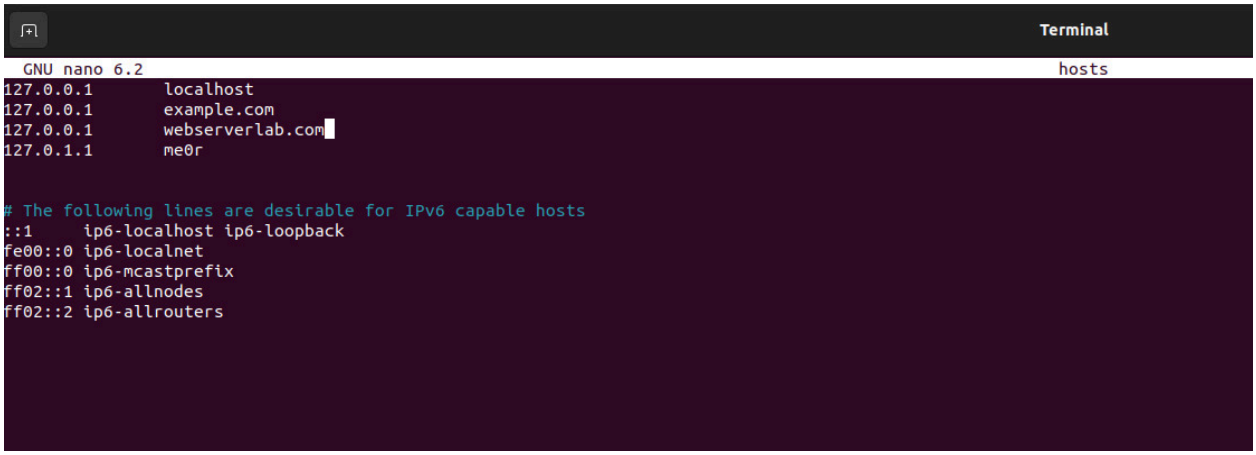
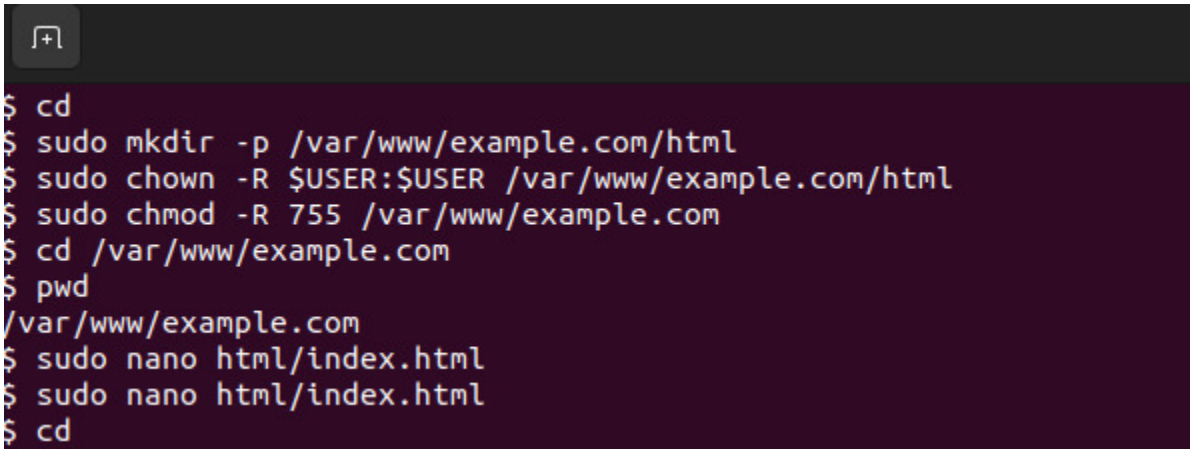
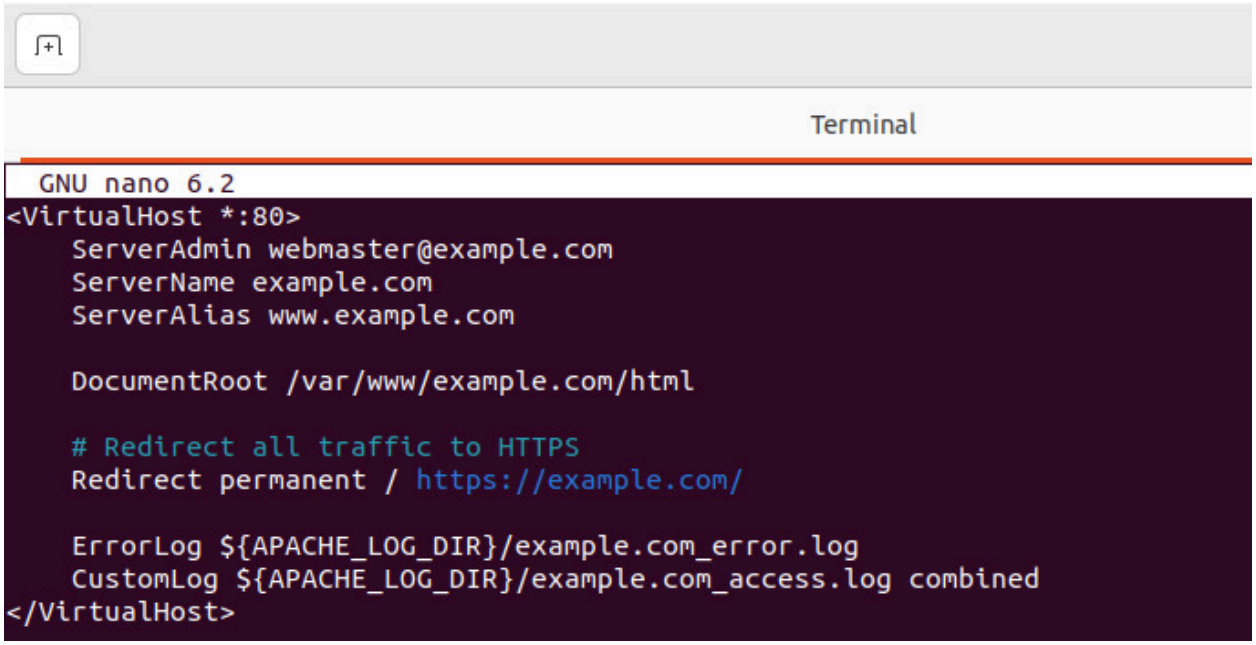
Checkpoint - 1





Checkpoint 2



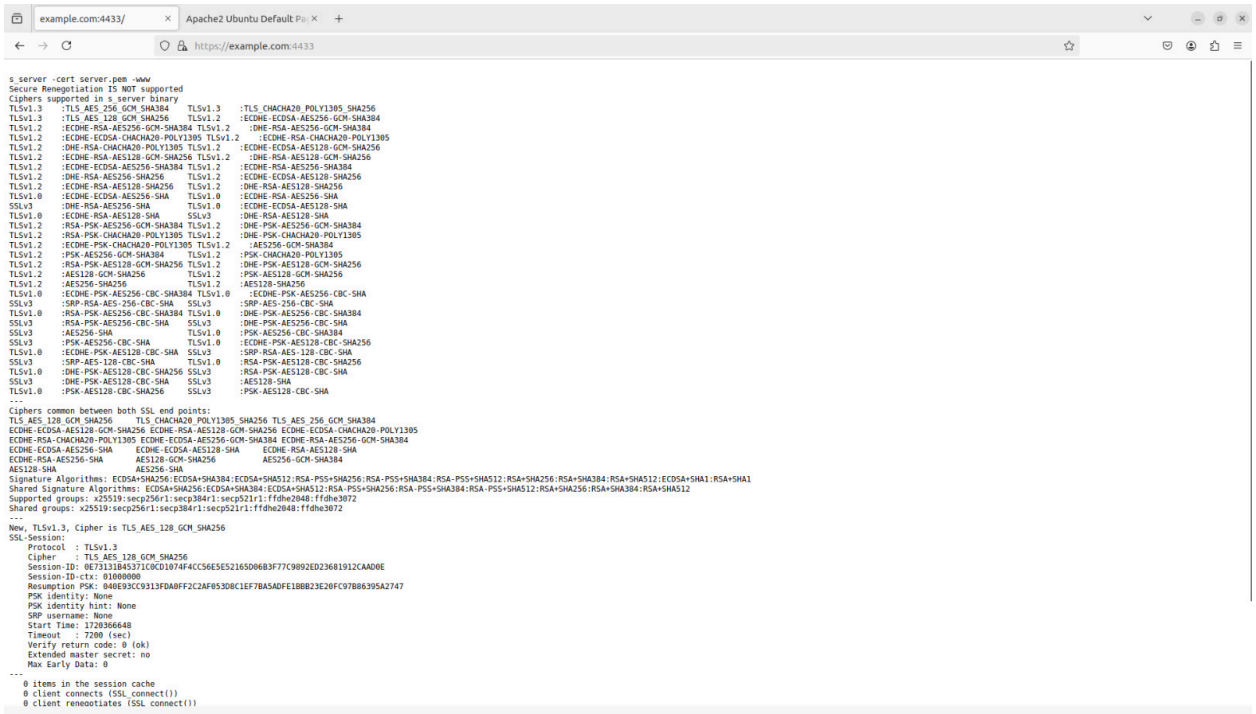
```
Terminal

$ sudo nano /etc/apache2/sites-available/000-default.conf
$ sudo nano /etc/apache2/sites-available/example.com.conf
$ sudo systemctl reload apache2
$
```

```
Terminal

 GNU nano 6.2                                  /etc/apache2/sites-available/example.com.conf
<VirtualHost *:80>
    ServerAdmin webmaster@example.com
    ServerName example.com
    ServerAlias www.example.com

    DocumentRoot /var/www/example.com/html

    # Redirect all traffic to HTTPS
    # Redirect permanent / https://example.com/

    ErrorLog ${APACHE_LOG_DIR}/example.com_error.log
    CustomLog ${APACHE_LOG_DIR}/example.com_access.log combined
</VirtualHost>
```

```
#####################################################################
[ ca ]
default_ca      = CA_default            # The default ca section

#####################################################################
[ CA_default ]

dir             = ./demoCA              # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/private/cakey.pem# The private key

x509_extensions = usr_cert              # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default            # Subject Name options
cert_opt        = ca_default            # Certificate field options
```

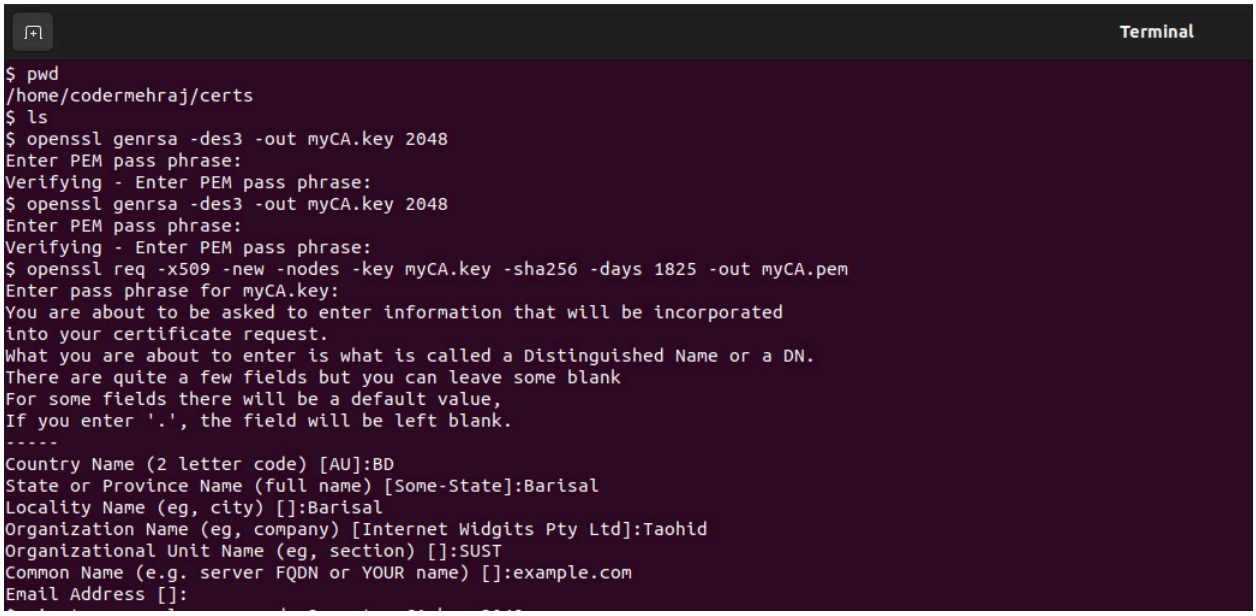
```
$ ls
demoCA  openssl.cnf
$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
....+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+
.........+...........+..+...........+........+....+.....+............+.+++++
......+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+....
..+......+.........+...........+..+.............+.+..+....+...+...+..+...+.....
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]:BD
State or Province Name (full name) [Some-State]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:
$ openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ 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]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
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 []:hello
An optional company name []:
$
```

```
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]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
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 []:hello
An optional company name []:
$ 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: 4096 (0x1000)
        Validity
            Not Before: Jul  7 15:26:34 2024 GMT
            Not After : Jul  7 15:26:34 2025 GMT
        Subject:
            countryName               = BD
            stateOrProvinceName       = Barisal
            organizationName          = Taohid
            organizationalUnitName    = SUST
            commonName                = example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                C5:5B:0B:D7:EB:01:E7:20:AF:F9:41:E5:CE:B0:35:F3:EB:9C:1C:80
            X509v3 Authority Key Identifier:
                51:15:6D:FE:C0:0C:25:F7:85:A8:6B:EF:53:F8:75:F4:EB:41:C8:A4
Certificate is to be certified until Jul  7 15:26:34 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
Data Base Updated
$ cp server.key server.pem
$ cat server.crt >> server.pem
$
```

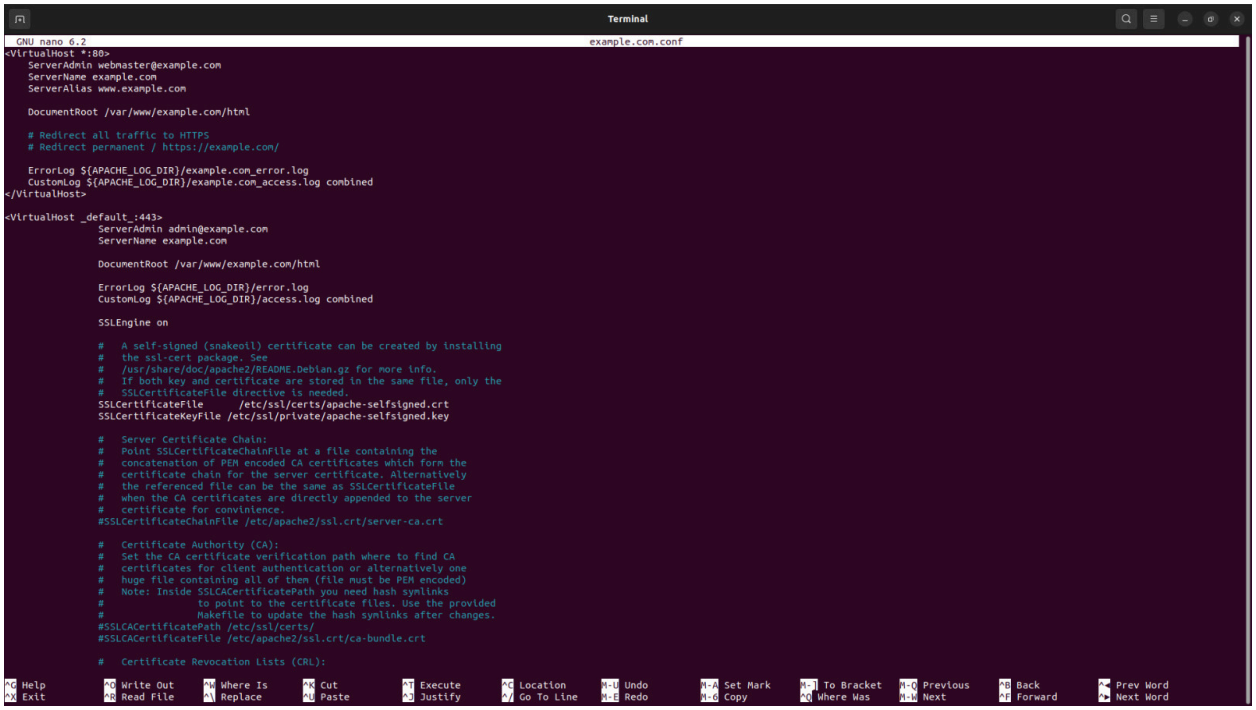

example.com:4433/
Apache2 Ubuntu Default Pa
https://example.com:4433
s_server -cert server.pem -www
Secure Renegotiation IS NOT supported
Ciphers supported in s_server binary
TLSv1.3 :TLS_AES_256_GCM_SHA384 TLSv1.3 :TLS_CHACHA20_POLY1305_SHA256
TLSv1.3 :TLS_AES_128_GCM_SHA256 TLSv1.2 :ECDHE-ECDSA-AES256-GCM-SHA384
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
TLSv1.2 :ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 :DHE-RSA-AES128-GCM-SHA256
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 :ECDHE-RSA-AES128-SHA256 TLSv1.2 :DHE-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 SSLv3 :DHE-RSA-AES128-SHA
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 :ECDHE-PSK-CHACHA20-POLY1305 TLSv1.2 :AES256-GCM-SHA384
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
TLSv1.2 :AES128-GCM-SHA256 TLSv1.2 :PSK-AES128-GCM-SHA256
TLSv1.2 :AES256-SHA256 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
SSLv3 :RSA-PSK-AES256-CBC-SHA SSLv3 :DHE-PSK-AES256-CBC-SHA
SSLv3 :AES256-SHA TLSv1.0 :PSK-AES256-CBC-SHA384
SSLv3 :PSK-AES256-CBC-SHA TLSv1.0 :ECDHE-PSK-AES128-CBC-SHA256
TLSv1.0 :ECDHE-PSK-AES128-CBC-SHA SSLv3 :SRP-RSA-AES-128-CBC-SHA
SSLv3 :SRP-AES-128-CBC-SHA TLSv1.0 :RSA-PSK-AES128-CBC-SHA256
TLSv1.0 :DHE-PSK-AES128-CBC-SHA256 SSLv3 :RSA-PSK-AES128-CBC-SHA
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_CHACHA20_POLY1305_SHA256 TLS_AES_256_GCM_SHA384
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA AES128-GCM-SHA256 AES256-GCM-SHA384
AES128-SHA AES256-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512
Supported groups: x25519:secp256r1:secp384r1:secp521r1:ffdhe2048:ffdhe3072
Shared groups: x25519:secp256r1:secp384r1:secp521r1:ffdhe2048:ffdhe3072

New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_128_GCM_SHA256
Session-ID: 0E73131B45371C0CD1074F4CC56E5E52165D06B3F77C9092ED23681912CAAD0E
Session-ID-ctx: 01000000
Resumption PSK: 040E93CC9313FDA0FF2C2AF053D8C1EF7BA5ADFE1BBB23E20FC97BB6395A2747
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1720366648
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
Max Early Data: 0
---
0 items in the session cache
0 client connects (SSL_connect())
0 client renegotiates (SSL_connect())


Terminal
$ pwd
/home/codermehraj/certs
$ ls
$ openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
$ openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem
Enter pass phrase for myCA.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]:Barisal
Locality Name (eg, city) []:Barisal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Taohid
Organizational Unit Name (eg, section) []:SUST
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:



Checkpoint 3

Checkpoint 4