

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

```
+      bijon@cyborg: /etc
GNU nano 6.2      hosts
127.0.0.1      localhost
127.0.0.1      example.com
127.0.0.1      webserverlab.com
127.0.1.1      cyborg

# 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
# Added by Docker Desktop
# To allow the same kube context to work on the host and the container:
127.0.0.1      kubernetes.docker.internal
# End of section

[ Read 17 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

bijon@cyborg: /var/www/example.com

GNU nano 6.2html/index.html

<html>
<head></head>
<body>
 <p>Hi Sir, it's Bijon! </p>
</body>
</html>

[Read 6 lines]

^G Help

^X Exit

^O Write Out

^R Read File

^W Where Is

^_ Replace

^K Cut

^U Paste

^T Execute

^J Justify

^C Location

^_ Go To Line

M-U Undo

M-E Redo


```
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 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 15:26:43 2024 GMT
    Not After : Jul  7 15:26:43 2025 GMT
  Subject:
    countryName           = BD
    stateOrProvinceName   = Mymensingh
    organizationName       = SUST
    organizationalUnitName = SWE
    commonName             = example.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      6D:5C:56:CF:76:39:FC:73:F8:D5:88:02:B9:11:FA:A6:C3:A2:9C:35
    X509v3 Authority Key Identifier:
      25:09:5A:09:D9:50:C0:52:64:86:17:64:E8:9C:B0:31:5C:05:E6:52
Certificate is to be certified until Jul  7 15:26:43 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
bijon@cyborg:~/lab5$ _
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
bizon@cyborg:~/lab5$ cp server.key server.pem
bizon@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/implementations/encode_decode/decode_epki2pki.c:96:
bizon@cyborg:~/lab5$ cat server.crt >> server.pem
bizon@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
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_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

```



```
bijon@cyborg: ~/certs
bijon@cyborg:~$ ls
Desktop  Documents  Downloads  lab5  Music  Pictures  Postman  pt  Public  snap  Templates  Videos
bijon@cyborg:~$ cd lab5
bijon@cyborg:~/lab5$ mkdir ~/certs
bijon@cyborg:~/lab5$ cd ~/certs
bijon@cyborg:~/certs$ pwd
/home/bijon/certs
bijon@cyborg:~/certs$
openssl genrsa -des3 -out myCA.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
bijon@cyborg:~/certs$
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]: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:~/certs$ _
```

```
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$ _
```

```
+      bijon@cyborg: /etc/apache2/sites-available
GNU nano 6.2                                example.com.conf *
<VirtualHost *:80>
ServerAdmin admin@example.com
ServerName example.com
ServerAlias www.example.com
DocumentRoot /var/www/example.com/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost _default_:443>
ServerAdmin admin@example.com
ServerName example.com

DocumentRoot /var/www/example.com/html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
    SSLOptions +StdEnvVars
</Directory>

</VirtualHost>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

[illegible]