EAST WEST UNIVERSITY

Mini Project-1

Submitted to

Rashedul Amin Tuhin

Senior Lecturer

Assistant Proctor

Department of Computer Science

and Engineering

Submitted By

Anika Anmol Sara (2019-1-60-210)

Rabeya Islam Dola (2019-1-60-096)

Oshin Nusrat Rahman (2019-1-60-014)

Date: 25/08/2022

Apache install:

```
sudo apt-get install apache2
```

```
sudo apache2ctl configtest   (To check whether the configuration is right in apache server or not.)
```

Make directory:

```
mkdir ca   (To make a directory. We named it ca)
cd ca   (Enter into the directory)
```

Make Certificate Authority:

```
openssl genrsa -des3 -out myCA.key 2048    (To generate a private key for encryption.)
```

```
openssl req -x509 -new -nodes -key myCA.key -sha256 -days 825 -out myCA.pem
```

(To generate a root certificate by using the previous private key to encrypt.)

After generating root certificate:

```
Enter pass phrase for myCA.key:123… (any password)
Country Name (2 letter code) [AU]:bd
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:EWU
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:AcmeCA (as mentioned)
Email Address []:W@gmail.com (any)
```

Create a CA Signed Certificate:

```
NAME=www.verysecureserver
```

(We declared a variable named NAME and use the domain name as mentioned.)

```
openssl genrsa -out $NAME.key 2048
```

(Generate a new private key)

```
openssl req -new -key $NAME.key -out $NAME.csr
```

(For creating a certificate signing request.)

After creating a certificate signing request:

```
Country Name (2 letter code) [AU]:bd
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name :EWU
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:www.verysecureserver.com (use the domain name)
```

```
Email Address []:w@gmail.com (any)

A challenge password []: (can skip)
An optional company name []: (can skip)
```

Create a Config file for Extensions:

```
>$NAME.ext cat <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = $NAME (need to include the domain name here because Common Name is not so commonly honoured by itself)
DNS.2 = bar.$NAME (We have added a subdomain here)
IP.1 = 10.0.2.15
EOF
```

Create the Signed Certificate:

```
openssl x509 -req -in $NAME.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial \
 -out $NAME.crt -days 825 -sha256 -extfile $NAME.ext
```

(To verify the certificate)

```
openssl verify -CAfile myCA.pem -verify_hostname bar.$NAME $NAME.crt
```

(To check the work)

Copy Private Key and Certificates:

```
sudo cp $NAME.key /etc/ssl/private/ (To store the private keys in ssl file)
sudo cp $NAME.crt /etc/ssl/certs/ (To store the certificates in ssl file)
```

Create SSL Apache Config:

```
>default-ssl.conf cat <<-EOF
<IfModule mod_ssl.c>
   <VirtualHost _default_:443>
      DocumentRoot /var/www/html

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

      SSLEngine on
      SSLCertificateFile    /etc/ssl/certs/$NAME.crt
```

```
        SSLCertificateKeyFile /etc/ssl/private/$NAME.key
    </VirtualHost>
</IfModule>
EOF
```

```
Sudo nano /etc/hosts
 (to edit the file)
```

```
sudo cp default-ssl.conf /etc/apache2/sites-available/default-ssl.conf
sudo a2enmod ssl
 (to enable the port)
sudo a2ensite default-ssl
 (to enable default ssl)
sudo systemctl restart apache2
(Restart the apache2)
```

Firewall Configuration:

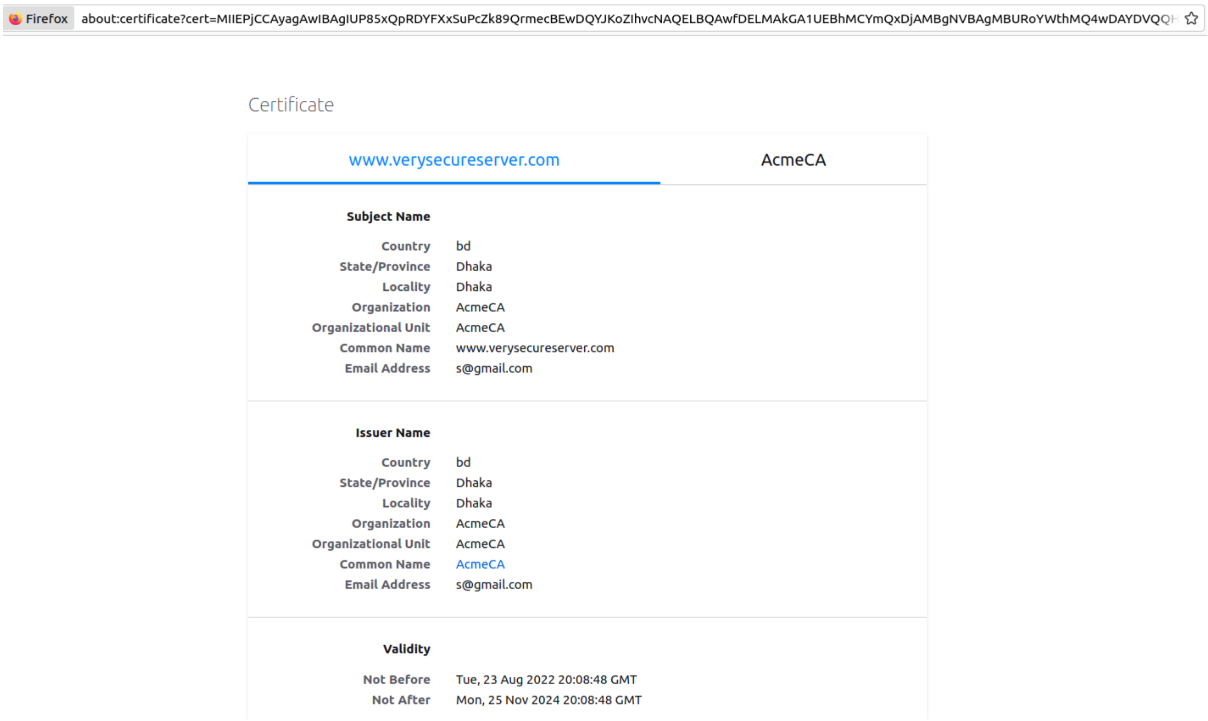
```
sudo ufw allow 53 (for port 53)
sudo ufw allow 80 (for port 80)
sudo ufw allow 443 (for port 443)

sudo ufw status (for checking ports)
```

Upload File:

```
sudo nano /var/www/html/index.html
```

Certificate:



about:certificate?cert=MIIEPjCCAyagAwIBAgIUP85xQpRDYFXxSuPcZk89QrmecBEwDQYJKoZIhvcNAQELBQAwfDELMAkGA1UEBhMCYmQxDjAMBgNVBAgMBURoYWthMQ4wDAYDVQQH

Certificate

Subject Name

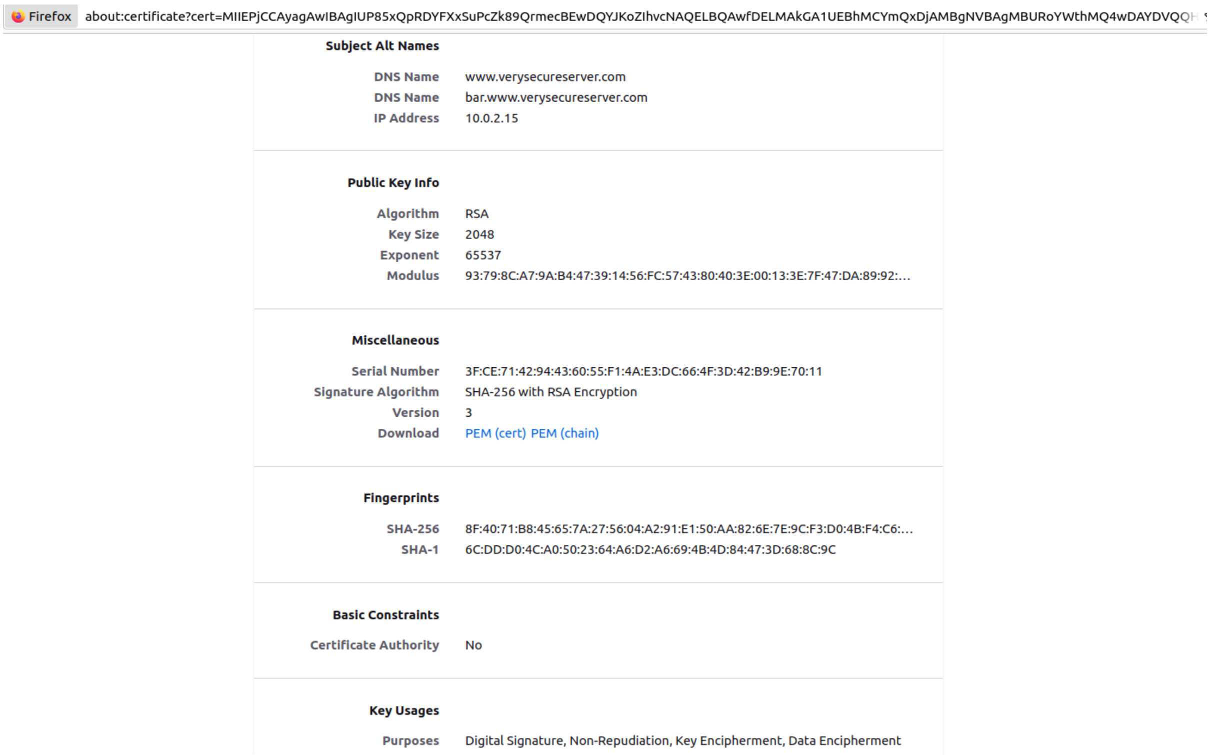
Country	bd
State/Province	Dhaka
Locality	Dhaka
Organization	AcmeCA
Organizational Unit	AcmeCA
Common Name	www.verysecureserver.com
Email Address	s@gmail.com

Issuer Name

Country	bd
State/Province	Dhaka
Locality	Dhaka
Organization	AcmeCA
Organizational Unit	AcmeCA
Common Name	AcmeCA
Email Address	s@gmail.com

Validity

Not Before	Tue, 23 Aug 2022 20:08:48 GMT
Not After	Mon, 25 Nov 2024 20:08:48 GMT



about:certificate?cert=MIIEPjCCAyagAwIBAgIUP85xQpRDYFXxSuPcZk89QrmecBEwDQYJKoZIhvcNAQELBQAwfDELMAkGA1UEBhMCYmQxDjAMBgNVBAgMBURoYWthMQ4wDAYDVQQH

Subject Alt Names

DNS Name	www.verysecureserver.com
DNS Name	bar.www.verysecureserver.com
IP Address	10.0.2.15

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	93:79:8C:A7:9A:B4:47:39:14:56:FC:57:43:80:40:3E:00:13:3E:7F:47:DA:89:92:…

Miscellaneous

Serial Number	3F:CE:71:42:94:43:60:55:F1:4A:E3:DC:66:4F:3D:42:B9:9E:70:11
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	8F:40:71:B8:45:65:7A:27:56:04:A2:91:E1:50:AA:82:6E:7E:9C:F3:D0:4B:F4:C6:…
SHA-1	6C:DD:D0:4C:A0:50:23:64:A6:D2:A6:69:4B:4D:84:47:3D:68:8C:9C

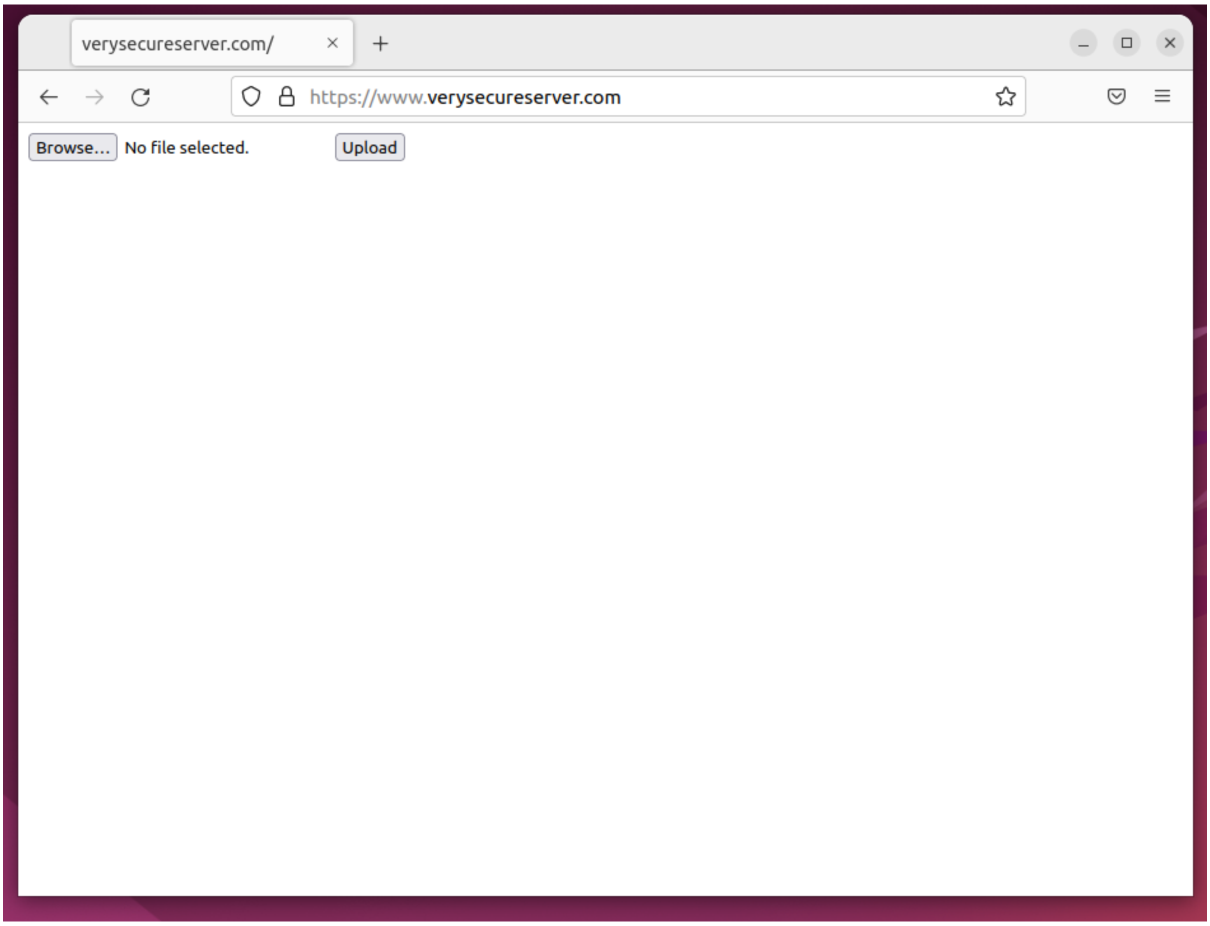
Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment

Lock pad:



https://www.verysecureserver.com

No file selected.