Lab7

Yue Zhang

Task1

```
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup$ openssl req -x509 -newkey rsa:4096 -sha25
6 -days 3650 -keyout ca.key -out ca.crt
Generating a RSA private key
...++++
.....................................................................................
.....................................................................................
.....................................++++
writing new private key to 'ca.key'
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]:US
State or Province Name (full name) [Some-State]:AL
Locality Name (eg, city) []:Auburn
Organization Name (eg, company) [Internet Widgits Pty Ltd]:yue
Organizational Unit Name (eg, section) []:yue
Common Name (e.g. server FQDN or YOUR name) []:yue
Email Address []:yzhang8317@tuskegee.edu
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup$ ls
ca.crt  ca.key  docker-compose.yml  image_www  volumes
```

I generate CA's private key file ca.key and public-key certificate file ca.crt.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4d:46:fe:39:5f:53:1f:22:c9:90:af:23:39:e9:6e:7b:86:29:96:f7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = AL, L = Auburn, O = yue, OU = yue, CN = yue, emailAddress = yz
hang8317@tuskegee.edu
```

This part means this is a CA's certificate.

```
            Not After : Nov  8 22:12:28 2031 GMT
        Subject: C = US, ST = AL, L = Auburn, O = yue, OU = yue, CN = yue, emailAddress = y
zhang8317@tuskegee.edu
```

The information equals issuer's information, so this is a self-signed certificate.

```
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:bf:56:f9:f5:89:f1:90:dd:4d:60:cd:54:5c:9d:
    0c:e9:c4:85:60:74:50:43:5e:72:19:e4:41:02:0e:
    aa:d4:21:ba:27:77:a5:2d:97:82:d8:01:f0:88:e5:
    20:a9:d3:b9:f1:17:9b:0c:ad:76:31:01:25:31:c8:
    27:82:19:64:a4:67:c9:6a:77:4c:62:09:8b:6b:af:
    67:13:2d:dc:84:90:16:68:74:45:57:97:ac:e4:7b:
    32:f2:a3:44:67:a4:49:be:8e:7a:2f:ca:6d:1c:fb:
    5d:7c:9e:1e:a8:fb:6e:cd:76:91:61:c2:bd:85:14:
    f1:dc:96:8a:39:cd:ad:98:fe:e4:41:d4:1a:3e:ac:
    a6:3b:85:e3:01:d6:03:c1:02:2e:cf:46:da:dd:cb:
    90:8c:1b:3c:46:b8:2e:7a:63:22:b8:e3:ab:5a:74:
    7e:e3:fb:83:1c:2f:ad:9e:f9:19:fe:fc:18:a4:07:
    6f:0e:0a:aa:8e:d9:9a:ac:98:77:22:64:b1:5c:d2:
    7a:1a:9c:53:da:a9:2e:6c:82:1c:09:d0:c1:61:b8:
    2a:a6:7e:0a:aa:b9:a8:db:47:9a:2c:5c:83:7c:6f:
    de:f8:c7:d4:bf:c2:aa:e5:cd:2e:90:40:80:1a:cf:
    bc:90:94:ba:96:d7:25:68:0a:63:31:30:d4:89:69:
    7f:d7:ac:f3:33:c2:ef:20:f8:fc:e3:aa:59:3b:48:
    02:0e:7a:87:8c:d0:ab:64:03:b5:0c:33:42:66:93:
    e9:ea:3b:52:34:ff:c1:36:36:9d:9d:e3:15:b1:8e:
    78:b7:93:61:f8:a1:ae:ba:99:59:72:29:d4:ea:8f:
    3b:59:04:c8:65:4b:1b:97:9e:ef:ee:29:98:6c:28:
```

This is modulus n.

```
    a8:77:bb
publicExponent: 65537 (0x10001)
```

This is public exponent e.

```
privateExponent:
    48:40:24:94:e6:28:d4:85:ec:51:10:57:b9:bd:08:
    02:41:d6:07:6d:04:5d:dc:0d:03:df:df:f8:51:e7:
    89:c0:ce:95:56:a5:85:c8:bf:7c:a7:86:d7:7a:85:
    d1:fb:04:2c:98:b8:50:9a:33:96:1f:93:96:ef:b8:
    93:74:d9:3f:07:7d:d3:f9:06:5b:c2:b4:e5:cd:cf:
    03:3b:ff:18:03:7c:a2:a6:bd:04:6d:5e:b8:cc:18:
    99:ec:b2:c8:dc:0d:88:aa:2e:53:5b:81:c6:3e:d8:
    b7:54:d1:c9:07:60:78:af:3c:08:89:4b:9d:34:22:
    7c:24:50:3f:b1:7d:ca:d6:fd:04:2a:7e:5a:8a:41:
    1f:1a:d8:74:7a:06:e2:db:db:27:23:df:43:7f:39:
    ae:de:1d:ed:aa:60:ca:90:22:ad:64:32:f1:2e:2a:
    38:16:62:14:c3:a0:30:f6:69:2d:92:ae:0f:4a:4b:
    52:27:0e:ee:70:16:ea:f3:8b:90:ee:2a:d7:1d:17:
    44:73:21:6a:e1:15:89:9d:bb:ce:ad:08:48:c9:0d:
    39:df:40:51:e5:57:70:ad:e1:f6:bc:5c:5e:21:b4:
    35:86:e7:bc:1d:5b:00:f9:70:8a:c2:00:5d:9f:71:
    d9:ba:7f:96:b3:d9:09:27:5a:fb:59:2f:f8:4f:61:
    19:3c:65:cd:a9:85:40:76:6c:01:6c:dd:b2:03:5e:
    95:fa:f1:35:c3:70:2a:76:ea:8e:64:79:02:0d:a7:
    52:6c:5d:8f:e6:d8:7a:dc:a4:65:fa:2d:09:27:02:
    e3:d4:fe:0a:95:fe:9f:ec:21:09:ff:d6:18:06:fd:
    ad:37:0e:56:24:19:18:58:02:f9:de:b0:82:34:05:
    99:ed:07:64:03:88:ab:b9:be:bf:93:f8:e2:fb:26:
    50:31:1d:07:80:92:42:bf:14:bd:99:80:64:db:e9:
    22:4b:c4:97:8b:a9:4d:d1:6e:66:d4:0a:e2:e3:46:
    ce:ce:bc:7b:3e:69:9e:b4:9b:a7:5d:c0:3f:6e:89:
    be:7a:bc:ad:58:1c:3c:ca:60:55:51:e1:a7:81:29:
```

This is private exponent d.

```
prime1:
    00:fa:71:d2:57:b0:b9:39:31:6d:12:15:80:eb:3a:
    06:bd:e8:b1:0d:6a:54:a1:6e:a2:4a:3a:93:b1:f8:
    44:3f:03:1c:7e:a9:eb:b6:63:47:23:b8:d6:46:3e:
    73:34:96:75:47:c2:2f:b3:76:2b:9e:ce:d1:a8:b1:
    27:6f:cb:8b:67:4d:00:33:38:a3:13:ee:ee:f3:4a:
    b3:81:88:a1:85:4d:cd:77:d1:c5:1f:cc:20:17:f0:
    bb:96:15:f2:0d:29:44:8e:b4:3c:72:02:7a:44:55:
    07:60:ed:31:c8:ed:32:a8:42:f3:fe:8e:c7:e9:e4:
    f9:41:46:44:d0:5d:83:6a:f0:fc:e0:15:71:74:71:
    bf:4b:52:19:a6:a4:2c:b3:28:3b:66:ea:65:dd:44:
    1c:48:4f:30:49:71:fb:3f:a8:af:14:c7:ea:20:15:
    1f:df:a9:bd:56:bc:2e:5d:17:1f:de:af:62:2a:8f:
    da:f9:92:5e:56:1f:46:98:0b:f3:6c:bb:ae:8e:3b:
    4f:e6:01:33:1c:a5:71:64:03:6e:f0:44:50:db:60:
    f2:47:ba:08:f8:24:cf:ed:b3:e3:85:99:73:11:3b:
    98:01:8d:bb:89:39:d7:68:7a:7c:f2:ac:3f:48:2d:
    38:29:6c:61:2a:0f:d1:20:90:5d:71:cd:2e:b6:af:
    a6:9f
```

```
prime2:
    00:c3:95:85:62:51:33:a5:79:19:b6:0e:57:1d:64:
    ad:1c:a3:51:ef:08:99:8b:f4:1e:57:8f:35:a8:3c:
    c5:4d:5c:18:a2:70:34:e6:61:05:86:82:18:13:cf:
    85:98:42:d2:9f:4b:15:62:88:06:13:85:61:35:83:
    a4:b3:50:07:de:15:7d:49:fa:88:f5:ac:20:cb:34:
    72:a8:0b:64:8c:57:31:3a:c9:eb:9d:4f:15:47:52:
    64:91:47:0d:05:f0:a3:17:3b:6a:b0:d0:2e:ad:b0:
    27:86:c7:c1:c3:c4:31:f0:ff:e8:f8:0e:89:5c:d1:
    9f:72:15:00:c3:55:5b:db:1d:30:bf:ae:ec:91:80:
    07:f8:6b:b3:1c:b0:52:f7:ed:ff:2b:aa:a8:79:c1:
    80:79:c8:00:aa:ed:40:c3:b6:61:8a:08:87:ff:2a:
    c1:37:ec:33:4e:74:90:80:32:e0:0e:3c:14:1c:71:
    99:73:9c:fc:1e:be:44:2a:f5:f8:91:ef:e6:0e:94:
    3a:82:6c:38:bf:ea:06:5e:d7:fd:5d:93:b1:6e:e1:
    6b:a7:0b:c4:8e:46:b4:cc:4b:fe:09:de:0c:5e:91:
    86:e5:17:71:45:30:92:a3:ed:a9:8d:84:8f:be:89:
    38:58:cd:b9:5c:ec:a9:7e:ac:0c:a4:4e:65:77:01:
    65:65
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup$ vi find.c
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup$ gcc -o find find.c -lcrypto
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup$ ./find
find p q!
```

Prime1 and prime2 are p and q. then I use find.c to verify, if prime1*prime2 = n then print “find p q !”.

Task2

```
seed@ip-172-31-30-228:/home/ubuntu/lab7$ openssl req -newkey rsa:2048 -sha256 -keyout serve
r.key -out server.csr -subj "/CN=www.yue.com/O=Yue Inc./C=US" -passout pass:dees -addext "s
ubjectAltName = DNS:www.yue.com, DNS:www.yue1.com, DNS:www.yue2.com"
Generating a RSA private key
....+++++
.....................................................................................+++++
writing new private key to 'server.key'
-----
seed@ip-172-31-30-228:/home/ubuntu/lab7$
```

I generated a certificate request for my web server.

Task3

```
seed@ip-172-31-30-228:/home/ubuntu/lab7$ openssl ca -config myCA_openssl.cnf -policy policy
_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile
 ca.key
Using configuration from myCA_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: Nov 10 23:44:56 2021 GMT
            Not After : Nov  8 23:44:56 2031 GMT
        Subject:
            countryName               = US
            organizationName          = Yue Inc.
            commonName                = www.yue.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F9:3B:B8:17:A7:B7:EF:97:BC:B3:84:0F:E0:63:2D:2B:A8:FE:5F:53
            X509v3 Authority Key Identifier:
                keyid:18:24:12:23:DE:00:A7:D0:16:C6:CD:10:30:F0:34:7A:EF:C9:76:AE

Certificate is to be certified until Nov  8 23:44:56 2031 GMT (3650 days)
```

I generated a certificate for my server.

Task4

```
seed@ip-172-31-30-228:/home/ubuntu/lab7/Labsetup/volumes$ ls
README.md  ca.crt  server.crt  server.key
```

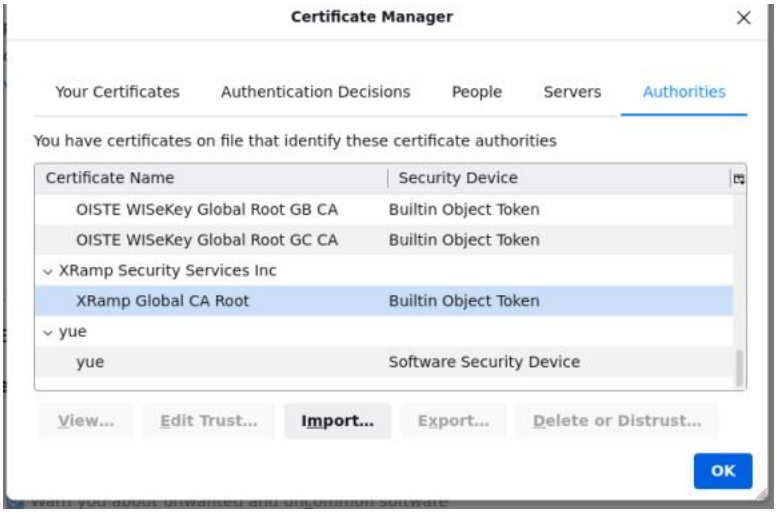
I copied server.crt and server.key to volumes.

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.yue.com
    ServerAlias www.yue1.com
    ServerAlias www.yue2.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /volumes/server.crt
    SSLCertificateKeyFile /volumes/server.key
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.yue.com
    DirectoryIndex index_red.html
</VirtualHost>
```

Then I added these content to bank32_apache_ssl.conf.

```
root@9a778fce7949:/# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.yue.com:443 (RSA):
 *
root@9a778fce7949:/#
```

Start the service.



I added the ca.crt to the firefox.

Then I can browse my website.

Task5

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.seed-server.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /volumes/server.crt
    SSLCertificateKeyFile /volumes/server.key
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.seed-server.com
    DirectoryIndex index_red.html
</VirtualHost>
```

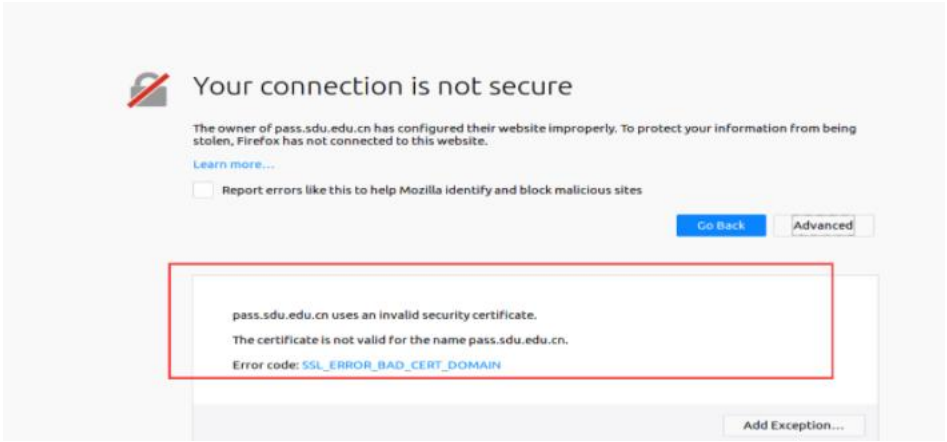
I add this new content to bank32_apache_ssl.conf. , and rest of configuration are the same as task4.

```
10.9.0.80 www.seed-server.com
```

Modify /etc/hosts file to emulate the result of a DNS cache posting attack.

Then I start the service again.

We can see when I try to go to the www.seed-server.com , it point to my server which I already deployed in task4.



But when I try to visit https://www.seed-server.com/ it will failed. This is because the accessed URL domain name does not match the Common Name in the subject domain in the certificate.

Task6

```
seed@ip-172-31-30-228:/home/ubuntu/lab7$ openssl req -newkey rsa:2048 -sha256 -keyout seed.
key -out seed.csr -subj "/CN=www.seed-server.com/O=Seed Inc./C=US" -passout pass:dees
Generating a RSA private key
.....+++++
.............................+++++
writing new private key to 'seed.key'
-----
```

```
seed@ip-172-31-30-228:/home/ubuntu/lab7$ openssl ca -config myCA_openssl.cnf -policy policy
_anything -md sha256 -days 3650 -in seed.csr -out seed.crt -batch -cert ca.crt -keyfile ca.
key
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4099 (0x1003)
        Validity
            Not Before: Nov 11 20:01:12 2021 GMT
            Not After : Nov  9 20:01:12 2031 GMT
        Subject:
            countryName               = US
            organizationName          = Seed Inc.
            commonName                = www.seed-server.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                D8:09:DE:A3:27:53:EA:D4:D2:19:36:4B:3B:47:B3:E2:FC:5F:82:95
```

As an attacker, I already known CA's private key. So I can generate a certificate for my website.

```
</VirtualHost>
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.seed-server.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /volumes/seed.crt
    SSLCertificateKeyFile /volumes/seed.key
</VirtualHost>
<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.seed-server.com
    DirectoryIndex index.html
</VirtualHost>
```

Then I modify the configuration. Restart the service.

I can visit this website.