Lab 4 PKI Lab

Name: Guo Yuchen
Student ID: 1004885

Task 1: Becoming a Certificate Authority (CA)

Generate self-signed certificate for ModelCA:

$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 -keyout ca.key -out ca.crt

```
root@8373c99b1c3b:~/PKI/demoCA# openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
> -keyout ca.key -out ca.crt \
> -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" \
> -passout pass:dees
Generating a RSA private key
.....................................++++
.....................................................................................
.....................................................................................
writing new private key to 'ca.key'
-----
```

To see the decoded content:

$ openssl x509 -in ca.crt -text -noout

```
root@8373c99b1c3b:~/PKI/demoCA# openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:b5:f8:1b:d9:54:af:5b:47:aa:ff:0b:18:53:98:b6:b4:54:66:3a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 15 08:59:40 2023 GMT
            Not After : Oct 12 08:59:40 2033 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:b3:c7:0e:92:b7:c2:47:08:46:14:8c:4f:e2:e6:
                    41:90:b7:cc:32:20:49:2e:5c:59:6e:86:2f:e6:a3:
                    40:a6:a1:82:53:c2:dc:97:66:48:b4:e7:44:2b:bc:
                    3e:85:1e:a2:84:24:bf:6b:10:2f:17:5b:4c:e7:98:
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

0d:b5:f8:1b:d9:54:af:5b:47:aa:ff:0b:18:53:98:b6:b4:54:66:3a

Signature Algorithm: sha256WithRSAEncryption

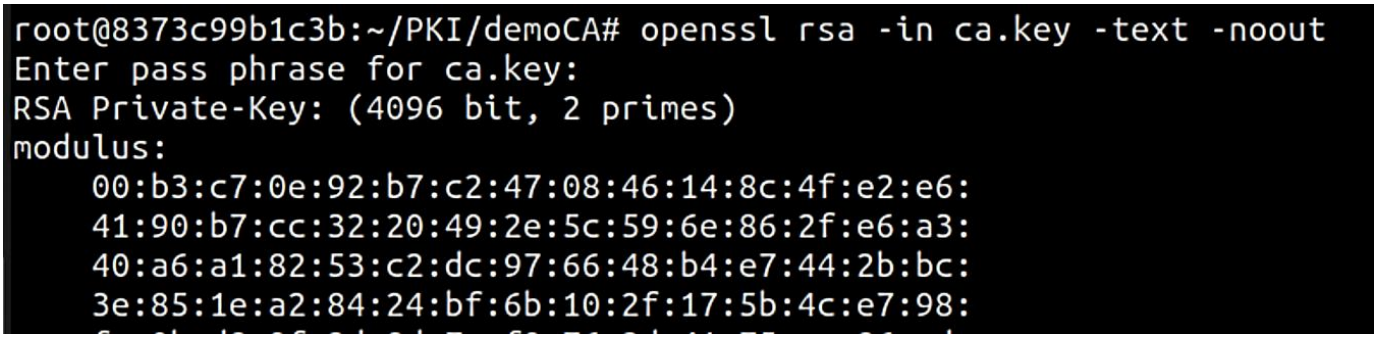
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US

Validity

Not Before: Oct 15 08:59:40 2023 GMT
Not After : Oct 12 08:59:40 2033 GMT
Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (4096 bit)
Modulus:
00:b3:c7:0e:92…
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:FE:25
X509v3 Authority Key Identifier:
keyid:E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:FE:25

X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
68:7c:8e:79… [See Appendix.1 for full content]

$ openssl rsa -in ca.key -text -noout



[The full content is recorded in Appendix.2]

• *What part of the certificate indicates this is a CA's certificate?*

CA:TRUE

• *What part of the certificate indicates this is a self-signed certificate?*

Subject is the same as issuer:

- **Subject: CN = www.modelCA.com, O = Model CA LTD., C = US**
- **Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US**

• *In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that n = pq. Please identify the values for these elements in your certificate and key files.*

- **public exponent *e***: 65537
- **modulus *n*:**

733428481176842462766000476326593751876867725043743136258634360066563305383835655447813112619725042287388288111042933860517457404139144327620689047298726886741735722136381440690666529157048482124542053330739816397111575734718243936476744169258976473603534630627907012122018792769681432469686077863482647584368479291634948209110600502696196777065630154063926493253997722243109323695669354003693567463941862012384674678761160016564620606392875302040972367686069359063907547195022327345688771921769215043533897317060132681819203264641135934828103591414904222793304073567082020168283109392056101040582815757497867462968180758128058796078881325228859950549125441547190684866557429757338233722286458367943369925830960992381775433168592915116811584959641352210676244413208102536933430903457109870075194526420306459878710153837355577190625159540712277422587315543676253962880307653872542210358567876145242118141347659462116014243425325572884260827328170304865595399175078888932192512389486362586015837541680261226859948390661562718545413385011214331

06796055653147434967321823831686128988712546713613320502955149374421122538249139024513277625537478303171608505265809883009795530062811661891346095471007414756915416068329223113085784731905994372

- **private exponent *d*:**

11221275585944122212116341572129874040724098873939320425508226999080565578350733352419582953504101498414090307596361593938398988954793780876531805052511305817110005166335805279163393636964958924367583454761933166018947724021575342098436476776721175978184295499192858401433514556817668986028567530917101038083010729598888605967242918108144658870007894097683737351202885638542589970087853598112570610435242764237272278261040559510037766178344081440354044174723007558072235494033124610975817196483787660774088512440548011658454233691741565861301851947933601846206661802733007943951317176364719967551038182401439060456202458381299667933529181839972069825014391042319129429718201867343883715730843086801092529449463909125672857871081950949905857649764882478818305307169884853205371601827593916295915378339437672001397292366172046525799011410625190807067780360863064710342968371935812870836855982812170476099112926282918061032483974931377762939391680843963439866433012681253063885858559587829294127546274076044588665199551853176090050597898033763977853820385073703552124358041406335798573983020653523315437525263208681057661254089916791710232248453067237327774278078656376013153630782163136140972689486620375502481676282201323402441637813

- **prime 1 p:**

27849742390385662748150600182724267776775469343196145743231011803417159060014379696408644188278998334667783537754961627177182831628832271384518689549670981022494624657310014284801484879860940311761194443108642038780617698079412801054193627526997424554023763384719095475427646651164692462003871583022154398799963311539985256107794057339998221385337752157065286053191750507294688184518690524359106256088986705986842059979994972600291303052187630276603258426460181011789965060290466345779170362313223613519025414633601228315808267425230452042359919298680300043001148083081355416104009500351159066168417208849910161123072

- **prime 2 q:**

26335198038673346519142269796663678408458896767618933797348461186450074892681766289076520742425091781157875621541444680651967012928949671365383133668969063524071967594527874046728190406912257783731950218498574399642469449229727662576519188919293801808052588237802108894170074518704992559689159405039523461067753618209319089477850188219100786550505329850875245265747213895664111816711865063416407184590111338847650656580345288150143321757647271881885770005766718285669259653889823495002135278234842855209989409128710966521029896455274449528456463741724990832615493831093146781316086745141745125804970273029891288118591

By the way, to convert the hex strings copied from terminal to integer, I wrote a python function:

```
def hex_to_int(hex_string):
    splited_hex = hex_string.replace("\n","").replace(" ","").split(":")
    res = ""
    for s in splited_hex:
        res += s
    return int(res, 16)
```

Task 2: Generating a Certificate Request for Your Web Server

Generate a CSR with 2 alias:

```
root@8373c99b1c3b:~/PKI# openssl req -newkey rsa:2048 -sha256 \
> -keyout server.key -out server.csr \
> -subj "/CN=www.yuchen2023.com/O=Yuchen2023 Inc./C=US" \
> -passout pass:dees \
> -addext "subjectAltName = DNS:www.yuchen2023.com, \
> DNS:www.yuchen2023A.com, \
> DNS:www.yuchen2023B.com"
Generating a RSA private key
..............................+++++
..........................+++++
writing new private key to 'server.key'
```

$ openssl req -in server.csr -text -noout

```
root@8373c99b1c3b:~/PKI# openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.yuchen2023.com, O = Yuchen2023 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
                    f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
                    66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
                    94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
                    31:75:47:65:c0:3a:10:43:f5:18:6f:02:5d:09:8e:
                    a4:b8:00:9b:9b:a5:c4:0e:64:89:ce:2f:00:a2:c8:
                    54:9b:8b:68:b3:44:96:67:7e:61:80:c4:58:ad:62:
                    71:24:30:a1:ce:c8:b0:b5:a7:5e:4d:e1:fa:9a:19:
                    fe:46:cd:69:5b:bc:98:74:c4:d5:be:cc:e6:48:e8:
                    13:0e:99:ed:e9:74:59:41:ab:99:fc:19:e2:70:31:
                    83:d1:e5:93:93:6b:c9:ff:f2:07:eb:24:25:3e:f3:
                    9b:2a:ec:51:7a:c1:f3:3f:77:a2:0e:bf:d4:4f:0c:
                    78:99:9b:2e:8c:14:29:25:8f:c2:b3:80:3d:02:b9:
                    20:26:dc:e7:ed:4a:d3:68:4f:01:25:2e:54:26:db:
                    95:98:38:1a:37:ce:8f:15:97:22:94:8d:1d:92:35:
                    17:47:7f:e5:05:30:c5:0b:bf:3f:b5:11:cb:30:af:
                    40:74:7f:87:2b:52:a4:29:5b:31:2c:37:c1:13:12:
                    f0:3f
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.yuchen2023.com, DNS:www.yuchen2023A.com, DNS:www.yuchen2023B.com
    Signature Algorithm: sha256WithRSAEncryption
         ba:9b:7b:4b:fa:9f:cb:85:32:a4:f9:73:2b:49:1b:7f:a7:0e:
```

[The full content is recorded in Appendix.3]

$ openssl rsa -in server.key -text -noout

```
root@8373c99b1c3b:~/PKI# openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
    f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
    66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
    94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
```

[The full content is recorded in Appendix.4]

Task 3: Generating a Certificate for your server

Turn the certificate signing request (server.csr) into an X509 certificate (server.crt), using the CA's ca.crt and ca.key:

```
openssl ca -config /etc/ssl/openssl.cnf -policy policy_anything \
-md sha256 -days 3650 \
-in server.csr -out server.crt -batch \
-cert ca.crt -keyfile ca.key
```

```
root@8373c99b1c3b:~/PKI# openssl ca -config /etc/ssl/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 /etc/ssl/openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4661 (0x1235)
        Validity
            Not Before: Oct 16 08:01:49 2023 GMT
            Not After : Oct 13 08:01:49 2033 GMT
        Subject:
            countryName               = US
            organizationName          = Yuchen2023 Inc.
            commonName                = www.yuchen2023.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                42:02:90:1C:B8:7F:9C:56:6E:0B:13:9B:B6:61:2B:37:93:03:1E:0E
            X509v3 Authority Key Identifier:
                keyid:E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:FE:25

            X509v3 Subject Alternative Name:
                DNS:www.yuchen2023.com, DNS:www.yuchen2023A.com, DNS:www.yuchen2023B.com
Certificate is to be certified until Oct 13 08:01:49 2033 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

$ openssl x509 -in server.crt -text -noout

```
root@8373c99b1c3b:~/PKI# openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4661 (0x1235)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 16 08:01:49 2023 GMT
            Not After : Oct 13 08:01:49 2033 GMT
        Subject: C = US, O = Yuchen2023 Inc., CN = www.yuchen2023.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
                    f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
                    66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
                    94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
                    31:75:47:65:c0:3a:10:43:f5:18:6f:02:5d:09:8e:
                    a4:b8:00:9b:9b:a5:c4:0e:64:89:ce:2f:00:a2:c8:
                    54:9b:8b:68:b3:44:96:67:7e:61:80:c4:58:ad:62:
                    71:24:30:a1:ce:c8:b0:b5:a7:5e:4d:e1:fa:9a:19:
                    fe:46:cd:69:5b:bc:98:74:c4:d5:be:cc:e6:48:e8:
                    13:0e:99:ed:e9:74:59:41:ab:99:fc:19:e2:70:31:
                    83:d1:e5:93:93:6b:c9:ff:f2:07:eb:24:25:3e:f3:
                    9b:2a:ec:51:7a:c1:f3:3f:77:a2:0e:bf:d4:4f:0c:
                    78:99:9b:2e:8c:14:29:25:8f:c2:b3:80:3d:02:b9:
                    20:26:dc:e7:ed:4a:d3:68:4f:01:25:2e:54:26:db:
                    95:98:38:1a:37:ce:8f:15:97:22:94:8d:1d:92:35:
                    17:47:7f:e5:05:30:c5:0b:bf:3f:b5:11:cb:30:af:
                    40:74:7f:87:2b:52:a4:29:5b:31:2c:37:c1:13:12:
                    f0:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

```
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                42:02:90:1C:B8:7F:9C:56:6E:0B:13:9B:B6:61:2B:37:93:03:1E:0E
            X509v3 Authority Key Identifier:
                keyid:E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:FE:25

            X509v3 Subject Alternative Name:
                DNS:www.yuchen2023.com, DNS:www.yuchen2023A.com, DNS:www.yuchen2023B.com
    Signature Algorithm: sha256WithRSAEncryption
         12:53:69:c2:69:7b:95:82:e2:b2:73:61:67:01:65:c2:c8:84:
         51:70:27:39:73:40:59:70:53:73:bd:db:84:4a:8e:32:30:98:
         bf:3a:3a:11:59:42:ca:e6:30:cc:3c:af:15:90:9f:7e:0d:c2:
         4e:da:60:15:2e:dd:27:31:44:c5:8c:f9:96:55:68:6f:17:3d:
         0d:7d:9c:8b:f2:8a:1e:0c:53:44:70:a7:13:77:75:52:8c:f3:
```

[The full content is recorded in Appendix.5]

In X509v3 Subject Alternative Name, we see that 3 names are recorded:

- DNS:www.yuchen2023.com,
- DNS:www.yuchen2023A.com,
- DNS:www.yuchen2023B.com

Thus, alternative names are included.

Task 4: Deploying Certificate in an Apache-Based HTTPS Website

Create yuchen2023_apache_ssl.conf inside /etc/apache2/sites-available:

```
<VirtualHost *:443>
    DocumentRoot /var/www/yuchen2023
    ServerName www.yuchen2023.com
    ServerAlias www.yuchen2023A.com
    ServerAlias www.yuchen2023B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/yuchen2023.crt
    SSLCertificateKeyFile /certs/yuchen2023.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/yuchen2023
    ServerName www.yuchen2023.com
    ServerAlias www.yuchen2023A.com
    ServerAlias www.yuchen2023B.com
    DirectoryIndex index_http.html
</VirtualHost>
```

Copy generated server certificates to /certs and rename according to the config file defined above:

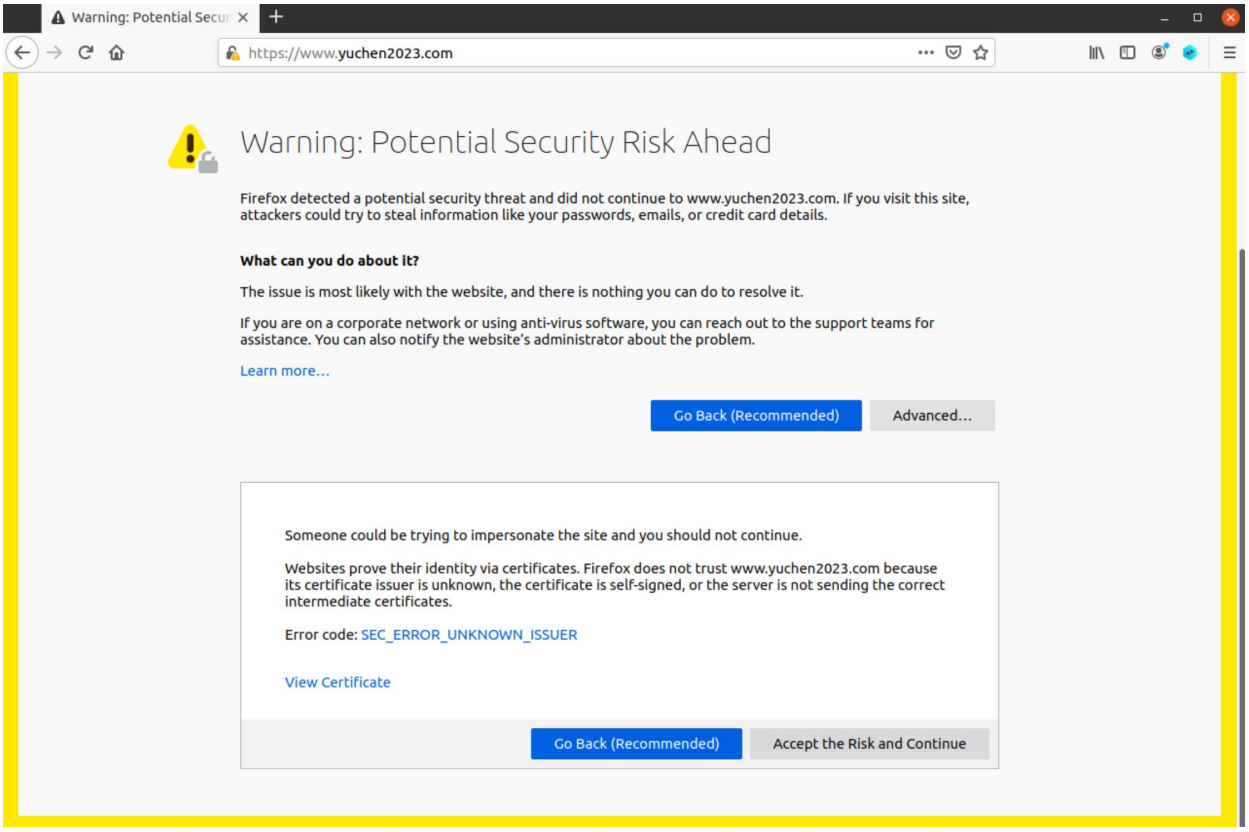
```
root@8373c99b1c3b:~/PKI# ls
ca.crt  ca.key  demoCA  server.crt  server.csr  server.key
root@8373c99b1c3b:~/PKI# cp server.crt /certs/yuchen2023.crt
root@8373c99b1c3b:~/PKI# cp server.key /certs/yuchen2023.key
```

Enable the site by :

```
$ a2ensite yuchen2023_apache_ssl.conf
$ service apache2 restart
```

After setting up the apache server, browse the web, and it shows the expected content for port 80 request:

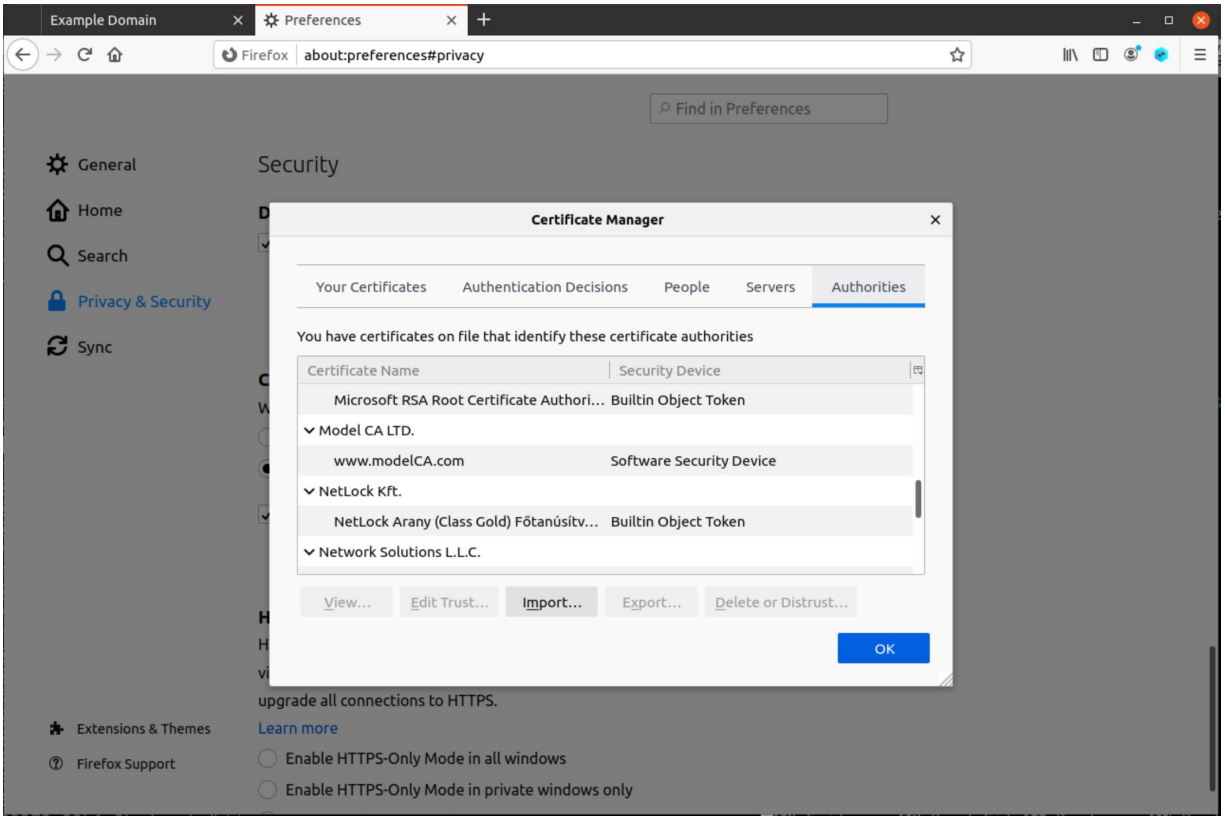
However, when visiting https site, it shows a warning with the error code: SEC_ERRO_UNKNOWN_ISSUER.



After clicking “Accept the Risk and Continue” , the intended page for port 443 is shown:

This is because the server’s certificate is signed by our root CA, which is not trusted by the browser. Thus we need to upload the self-signed certificate of our CA to tell the browser that this CA is trusted, and the websites who use certificates signed by this CA is also trusted.

So we import ca.crt in the Certificate Manager in Firefox:



After importing ca.crt from PKI, the web is considered to be safe.

Task 5: Launching a Man-In-The-Middle Attack

Similar to task 4, set up the configuration of www.example.com.

1. Create example_apache.conf file inside /etc/apache2/sites-available.

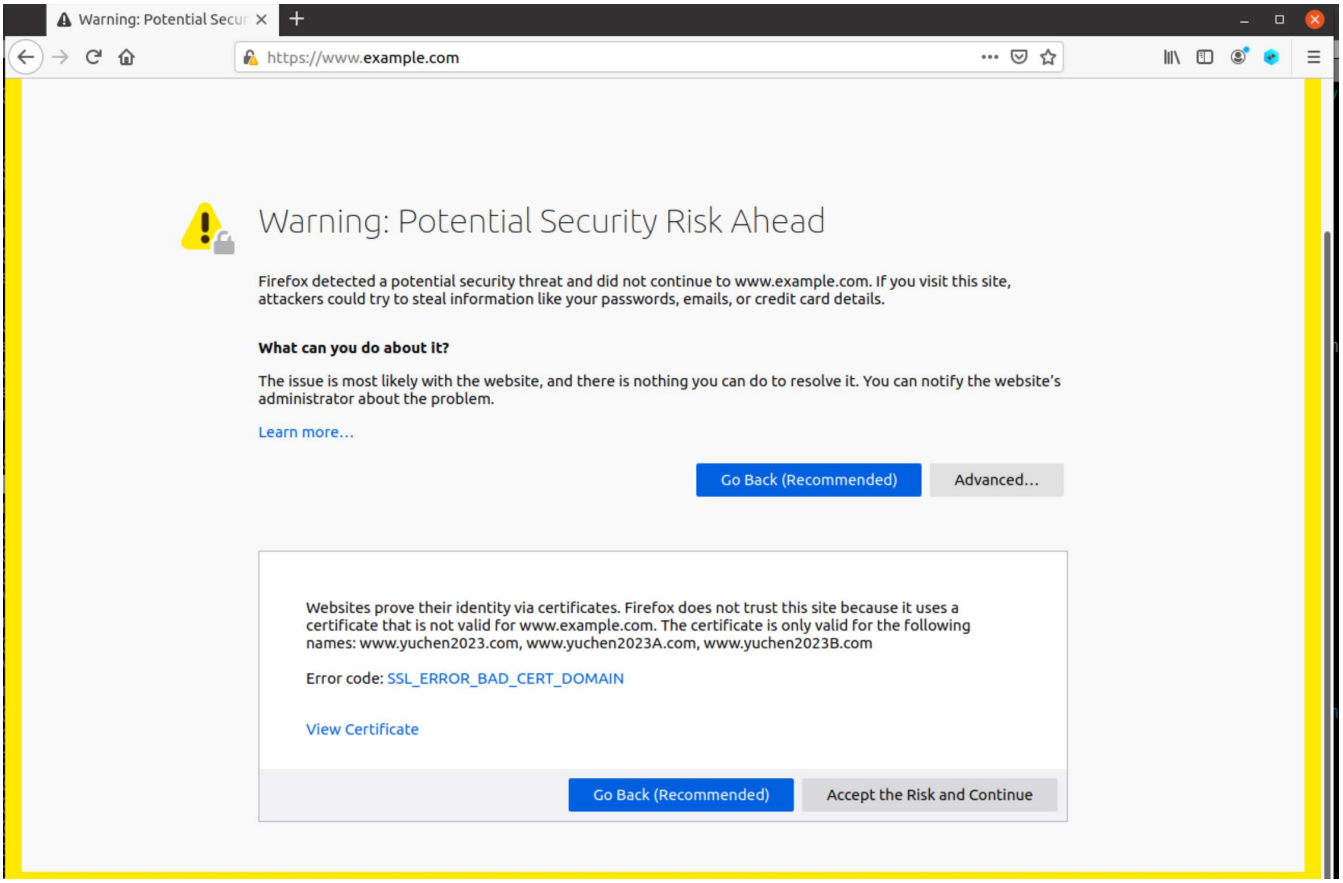
```
root@8373c99b1c3b: /etc/apache2/sites-available 63x37
  GNU nano 4.8              example_apache.conf
<VirtualHost *:443>
    DocumentRoot /var/www/example
    ServerName www.example.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/example.crt
    SSLCertificateKeyFile /certs/example.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/example
    ServerName www.example.com
    DirectoryIndex index_http.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warnin>
ServerName localhost
```

2. Directly copy yuchen2023.crt and yuchen2023.key to be example.crt and example.key.
3. Add DNS entry to the /etc/hosts in the victim machine.

```
seed@VM: /etc 63x37
  GNU nano 4.8                    hosts
# 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

# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com

# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com

# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
#10.9.0.80       www.seedlab-shellshock.com
10.9.0.80       www.bank32.com
10.9.0.80       www.yuchen2023.com
10.9.0.80       www.example.com
```

4. After setting everything up, visit http://www.example.com

Visit https://www.example.com



The error is caused by an invalid security certificate being used, with the specific error code of SSL_ERROR_BAD_CERT_DOMAIN. This is because the certificate used is for www.yuchen2023.com, instead of www.example.com that we are visiting.

Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA

Since the attacker gets CA's private key, i.e. ca.key, they can sign certificate for their fake servers without contacting the real CA:

```
# generate csr
$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj
"<SERVER_DOMAIN_INFO>"

# sign certificate
$ openssl ca -config openssl.cnf -policy policy_anything -md sha256 -days 3650 -in
server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
```

Take www.example.com as an example:
Generate server.csr and sign it:

```
root@8373c99b1c3b:~/PKI# openssl ca -config /etc/ssl/openssl.cnf -policy pol
icy_anything -md sha256 -days 3650 -in server.csr -out server.crt -batch -ce
rt ca.crt -keyfile ca.key
Using configuration from /etc/ssl/openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4662 (0x1236)
        Validity
            Not Before: Oct 16 09:19:05 2023 GMT
            Not After : Oct 13 09:19:05 2033 GMT
        Subject:
            countryName               = US
            organizationName          =  Example Domain Inc.
            commonName                = www.example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                AF:08:6C:8D:3A:95:1B:AD:83:A9:1B:56:96:93:F3:49:D8:78:C0:C7
            X509v3 Authority Key Identifier:
                keyid:E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:
FE:25

Certificate is to be certified until Oct 13 09:19:05 2033 GMT (3650 days)
```

Use this crt and key as example.crt and example.key, which are defined in the virtual host

No error pops out since the domain name matches.

Appendix

1. ca.crt

Signature Algorithm: sha256WithRSAEncryption

68:7c:8e:79:a5:11:ab:af:63:ee:05:c8:5f:b3:c1:d3:bd:bc:
fb:a4:82:b7:a4:6f:35:1e:09:6a:c2:07:b1:c2:1e:3c:36:a2:
f2:1e:34:1e:90:45:0d:52:9e:c6:21:0a:dd:76:9b:41:e1:2f:
9a:9c:72:8a:ee:2d:af:71:b7:48:bb:f1:97:f5:5d:58:e4:37:
18:61:a1:7f:0b:12:a6:a0:00:9c:c7:74:d4:2e:e7:83:74:93:
a1:c0:ab:fc:bd:ec:64:88:92:c1:9d:d8:41:eb:6a:63:15:4e:
1e:ec:f9:18:60:75:b5:2e:e0:43:97:5f:b1:ca:9a:e8:1b:d2:
ed:5d:94:7c:25:6a:97:67:0c:24:e6:d0:7d:c2:6d:fe:22:e3:
86:a5:f9:07:89:c1:18:d6:5a:bb:ac:c8:5a:a9:d0:37:2e:90:
c3:14:ea:dc:15:3c:9a:f4:80:a3:e3:be:30:25:92:34:39:aa:
51:ff:b1:3b:e0:03:05:e8:b5:76:1a:d0:db:78:96:2a:28:d1:
66:d9:f3:77:ff:0b:d7:62:e9:3e:7b:13:f6:0e:b9:3a:21:de:
e1:c0:b7:5b:7d:b3:48:94:2c:ed:53:4c:e0:50:c8:d3:8b:ce:
a5:c6:8c:4e:ed:0e:c0:69:aa:d6:b8:2b:ad:f9:b1:6b:7e:f0:
66:3d:db:7b:e1:a4:8d:77:1c:64:31:53:31:90:fc:49:43:13:
1e:94:43:e7:c2:52:ac:74:fa:29:4c:9c:23:06:71:70:13:61:
1a:4f:00:0a:2d:ed:10:3d:4d:54:37:d1:30:1c:db:e1:55:74:
16:7a:f2:9c:4d:16:c7:14:6e:e7:d7:8d:68:40:05:ff:2e:c2:
49:31:f2:d1:ea:5b:a9:28:9b:79:df:6c:d6:87:01:c2:80:4f:
a1:3a:09:02:c1:12:9f:1e:19:b6:08:73:ed:8e:c9:4e:a6:a1:
96:ef:df:3f:57:84:8a:dc:20:20:9b:9e:1a:c4:cf:4c:04:22:
c4:ab:c2:81:82:6b:aa:d8:ee:c7:ea:12:03:39:50:e5:7d:ad:
4a:b9:6b:71:b0:46:37:4b:56:6c:2a:ac:6d:7f:1c:7e:8e:d9:
3c:e4:c4:c5:75:73:56:1c:d0:03:f6:ae:9d:09:8a:76:0b:1e:
b6:2c:a3:d9:ca:2f:7f:33:58:45:34:cb:b7:3f:ab:ad:d6:52:
3c:2b:36:77:4c:f9:ea:22:3e:4e:02:af:04:31:e0:de:30:c3:

d9:11:ad:5a:92:0e:0c:7a:e7:21:f4:e4:1a:c5:5d:b5:30:7a:
a8:c2:c3:21:53:05:ff:32:71:77:aa:e6:34:83:ec:59:29:87:
17:b4:b6:15:73:3d:2c:d3

2. ca.key

RSA Private-Key: (4096 bit, 2 primes)

modulus:

00:b3:c7:0e:92:b7:c2:47:08:46:14:8c:4f:e2:e6:
41:90:b7:cc:32:20:49:2e:5c:59:6e:86:2f:e6:a3:
40:a6:a1:82:53:c2:dc:97:66:48:b4:e7:44:2b:bc:
3e:85:1e:a2:84:24:bf:6b:10:2f:17:5b:4c:e7:98:
fa:0b:d8:9f:2d:8d:7e:f9:76:2d:41:75:ac:86:ed:
81:28:95:c9:8b:90:a0:95:c6:a7:8a:ce:d9:78:b8:
f2:b3:d4:30:d8:84:5e:9e:68:6e:28:07:a8:c4:66:
8d:8e:a1:02:91:17:b0:30:98:6d:6d:d4:64:30:16:
f3:27:d8:28:57:09:dd:d6:32:91:b2:3b:b5:6f:0b:
15:88:d0:a2:4f:89:63:e1:33:51:6c:0f:62:03:83:
8f:2c:d3:b3:8f:bc:99:81:66:a2:b8:c6:28:4e:2d:
cc:f3:3a:42:12:4f:ee:12:03:d2:f0:44:46:b1:cb:
01:ae:36:57:9c:23:8e:54:4f:62:e7:c5:1a:25:d2:
2e:cb:d2:b6:36:82:50:7c:55:64:90:cb:b3:ea:b0:
b8:a4:af:65:36:0e:b9:c0:05:39:12:53:03:89:00:
b2:40:2b:36:0f:b8:30:cc:95:2f:37:f0:ca:30:79:
c8:66:40:6c:b5:43:7c:cc:29:5c:a9:9d:63:9e:9b:
c3:23:21:d2:02:89:ea:17:33:c0:b0:cc:53:08:95:
5f:bf:ea:9a:65:9c:a6:96:cc:8a:b0:69:6c:2c:9b:
02:b0:fc:dc:3a:a9:53:2f:ec:0f:d7:70:af:67:fc:
37:b4:88:ec:00:12:92:4b:2d:d1:81:a8:ed:46:a2:
86:56:cd:08:03:5c:38:3b:30:09:43:23:09:8b:79:
4a:99:44:69:91:f5:d0:75:72:5a:31:09:37:9a:23:
28:33:3c:95:38:97:1c:12:66:1d:ba:71:68:38:20:
52:d8:75:d7:b6:09:39:f8:d2:37:ab:45:9c:b2:89:
3c:cf:40:ed:39:16:9b:c3:67:97:93:c0:37:16:69:
c3:51:ce:a9:7f:26:46:24:1c:49:9d:ee:e1:71:ac:
c9:f0:94:3c:f2:24:78:5b:cc:00:fc:e8:c9:f2:25:
dd:74:b9:15:51:24:ec:db:f2:34:eb:f8:58:85:51:
c5:bb:a7:55:c7:80:19:66:c5:99:06:24:4b:56:28:
66:66:63:9f:98:08:71:d7:62:44:be:2e:81:8f:02:
d2:9d:d3:4d:bd:52:b8:79:af:2f:0e:e1:c9:eb:b2:
e6:43:c2:83:29:fc:6b:23:1a:24:8d:3f:4f:f8:a9:
20:fa:a0:01:58:65:11:a8:99:c5:af:5c:a5:10:5e:
97:ab:0d

publicExponent: 65537 (0x10001)

privateExponent:

1b:81:6a:26:62:7d:13:f7:1d:19:c9:b9:f3:42:3d:
67:d1:e7:29:08:2d:8a:2d:50:f5:8b:0c:4b:22:51:
22:ed:75:0e:31:b3:24:6a:de:d6:e6:c7:54:55:b1:
cf:16:37:d1:35:fa:1f:7c:53:68:24:6c:e8:c6:4c:
03:81:fa:20:b3:14:69:40:7e:7e:14:6d:f8:1a:e0:
77:00:2b:dc:f1:9c:d0:2d:9b:b6:ae:1d:31:ce:42:

3b:e7:4c:2d:e4:5a:c1:ab:c2:a6:d7:3d:28:07:74:
c3:0c:b9:62:cf:98:02:67:5f:de:bc:ef:33:38:5f:
ad:89:f1:ea:17:35:5c:af:52:01:4e:07:5d:5c:f9:
c7:7b:fc:49:65:00:e6:14:be:f1:64:8d:1f:72:82:
76:5e:51:8b:bd:54:53:2b:0b:dc:6f:5c:fd:51:1e:
99:5c:21:7d:c1:c2:ef:f8:ab:ce:5c:f3:e0:01:ea:
58:e8:31:91:4f:13:58:ac:e8:ba:03:3b:13:ec:4b:
82:9d:d3:89:15:79:10:fc:d3:ad:1f:ad:80:4b:d7:
84:42:dd:9e:5e:b4:66:bf:a5:d2:ba:e6:c0:90:5d:
b5:59:a7:24:d2:8e:8c:ce:8a:71:e9:a2:55:b6:5c:
45:e0:b7:81:28:39:30:d7:67:39:00:3e:9c:a6:c2:
3d:1d:24:98:4c:8e:1d:cf:f1:bb:55:f7:28:06:40:
78:f0:cc:d6:57:f3:06:1c:6b:4c:8d:38:7a:68:48:
c4:a0:a7:cb:c5:ba:4b:62:39:45:cb:b7:6e:93:3b:
c6:cb:f7:bf:19:22:6a:36:a8:52:b8:60:2b:5e:01:
5d:27:d5:6b:d2:ab:86:0e:3c:38:d4:54:d8:c9:e8:
6c:38:95:1a:c6:f7:7a:ad:d4:20:5d:ea:18:0b:f2:
07:8e:ad:35:db:9c:81:b5:56:be:86:79:35:d3:c2:
00:ee:92:fd:b5:6c:94:72:82:af:18:35:48:ef:49:
43:8a:e2:b1:9a:e8:1e:8e:5c:b0:74:46:7d:49:c4:
bd:63:aa:08:b6:3a:27:78:93:83:ed:9a:06:f5:01:
17:8c:34:45:e8:c4:6f:34:f5:c0:5d:95:ce:4a:a2:
5c:dc:53:01:92:67:ed:6a:f8:87:ae:ed:9b:7c:02:
69:7b:48:33:31:59:ba:b9:08:64:0d:6f:8c:b4:3a:
87:c4:bb:89:7c:8e:e1:00:ff:b7:cc:3b:02:17:d4:
a5:92:27:6e:79:38:c3:39:b8:b0:e9:49:11:79:38:
67:6c:26:25:c0:6e:85:35:87:b7:fd:89:74:67:ac:
cb:b5:6b:19:ed:8a:d9:5d:8d:71:29:d6:1d:d3:29:
bf:b5
prime1:
00:dc:9c:c9:dc:0e:55:c7:23:9d:96:ca:57:d0:f7:
92:27:b5:e6:dc:4f:e7:5f:7f:40:76:d2:83:fe:a0:
9a:20:49:26:41:81:e7:71:c5:6b:c4:2e:28:c3:e6:
79:22:d6:30:72:88:49:b5:14:1f:68:c3:ae:38:de:
69:4e:59:60:a6:67:b9:21:3e:40:ef:bb:f2:9b:39:
f1:2d:89:2a:58:30:af:b9:49:90:bf:fc:76:e4:18:
aa:70:ed:f6:6e:5a:ca:4d:d1:b4:f8:ad:b4:b3:c1:
7e:bf:6d:ca:53:bb:9f:01:be:f9:19:8f:6e:10:37:
ba:01:8c:dc:95:19:09:6f:39:58:0a:d8:bc:c7:b8:
4b:fd:93:6e:a9:38:57:ba:d1:27:e9:ef:43:f2:f0:
49:a1:c2:cd:5e:aa:b0:48:32:d2:c0:f1:e5:32:b9:
ee:6f:d4:3e:10:17:71:92:ce:a1:8d:93:93:71:75:
63:41:cf:43:25:49:25:7e:0c:a2:e3:d2:b4:02:bc:
7f:94:68:5d:8f:35:03:2e:20:6b:da:be:5b:e7:17:
d5:4d:f9:11:7d:3e:60:d5:a9:1b:e0:8b:c9:ed:9b:
4a:7f:fc:71:2a:48:6e:a0:d2:be:ff:52:ee:5e:c2:
bb:49:60:8c:1e:0c:45:29:56:71:e0:85:df:cf:f1:
10:b3
prime2:

00:d0:9d:6d:8c:d6:0d:81:5b:3f:b1:24:8e:d3:75:
24:c4:74:a3:cd:66:b1:12:fc:73:88:c5:f0:62:7f:
ef:f7:8c:d0:4d:02:18:7d:d9:2a:0f:2d:37:7e:1c:
3a:90:11:e7:31:80:83:17:4c:ae:15:e9:50:90:57:
a7:68:33:3a:28:7d:be:4a:ae:8a:30:b5:0b:c3:74:
cf:ca:3f:e1:ba:9e:f0:5a:18:27:1d:54:d2:ab:56:
03:46:8a:51:6e:6b:83:bd:4a:ed:50:4b:4a:d9:1a:
ca:c6:5f:65:0c:2a:06:66:ec:35:67:8e:17:f5:1f:
0d:6e:66:0a:d1:12:8e:81:07:95:e2:95:e4:2e:f9:
4c:d5:77:7b:3a:2a:7a:3a:89:38:d8:09:ba:c2:3f:
a9:01:f4:1a:47:43:3d:bf:2a:87:1b:0c:6a:fe:b6:
92:23:fb:74:37:70:e7:7a:3b:ea:fe:eb:2e:09:86:
0c:d5:1a:b6:75:4a:8c:03:d6:4c:47:3f:42:f2:8b:
64:5d:50:58:6b:49:cf:54:92:cc:b9:75:2b:1f:07:
9f:1d:51:2e:d7:b7:b7:b7:98:36:9c:99:8a:0e:c6:
3f:2c:e3:0b:79:c3:fe:6f:a5:26:bb:ee:2e:be:dc:
7d:1e:3c:1e:c0:7a:5f:c7:2b:21:6b:4a:2a:c7:b2:
b5:3f
exponent1:
52:dc:f1:55:1e:6d:49:a7:2f:01:fc:6e:8f:a6:ed:
d6:cc:94:32:1c:31:23:c5:80:49:21:39:42:e2:c0:
01:70:78:56:12:9d:04:36:cb:0b:9c:ea:e2:ea:26:
85:d7:3d:cb:47:35:a8:36:2e:b6:03:09:e5:82:64:
bb:71:06:c4:7a:21:27:43:62:d0:a9:1f:ae:fe:4c:
80:76:0c:d9:a3:2f:dd:c0:ac:05:f0:a6:17:76:cc:
4e:2e:93:69:4f:e0:bc:ea:0f:b7:78:47:6f:5d:36:
66:60:ae:a6:54:ca:9c:b5:46:8b:3b:3c:74:0a:fa:
6a:aa:a6:0f:ba:9f:b8:8f:29:6a:a9:8d:fe:d6:52:
74:a4:73:e4:4b:ad:68:16:37:8f:be:b7:1f:00:f2:
27:38:2c:3b:6a:91:5c:0c:fa:ec:4d:ef:70:e6:35:
90:fb:7f:74:3b:da:04:f2:67:eb:ed:8a:6c:0b:53:
84:dc:7c:b3:fc:8d:80:92:ee:7b:f4:20:79:06:a4:
44:f2:0e:72:43:cf:35:fc:27:86:ba:09:7a:fb:90:
bb:00:da:78:d8:7d:36:c3:96:1c:f9:64:97:42:c4:
f0:dd:b9:03:d0:c0:fc:d7:2b:b6:6b:47:ed:7f:e7:
28:e0:82:c0:a6:8b:33:c3:ac:72:50:d6:88:1c:5b:
d1
exponent2:
34:7f:f9:ea:e0:8f:a3:87:40:3f:27:51:1e:5c:33:
b5:91:19:0b:ff:14:ff:0f:33:50:2f:68:30:91:bb:
e5:53:b5:b4:3b:9b:c8:48:17:b2:9c:11:84:16:3c:
92:b7:3e:b4:91:7f:ec:24:2b:07:6e:a1:0c:c2:52:
6a:01:c2:58:20:54:fc:5c:72:80:91:7f:75:5f:f7:
4f:11:c6:8f:fd:a1:c5:3a:a0:d5:5b:dc:6c:ac:07:
c4:ff:d8:40:6e:a4:47:c6:0c:75:11:8d:b3:97:6f:
82:7e:cd:62:43:4d:3b:27:a4:c4:fb:d8:81:a2:9f:
f1:b1:92:75:4d:33:39:bb:9b:f7:da:fb:02:eb:50:
6f:c4:52:e9:af:78:f5:34:45:6e:f0:fb:e4:18:bb:
42:b7:98:c9:68:5d:a8:b7:5e:2a:eb:74:1d:c7:fa:

7d:3d:b1:e0:a5:f4:4b:29:bb:19:0e:3c:96:be:fa:
89:c2:e0:3a:22:59:9c:39:99:16:b1:0f:fb:14:23:
5c:ec:74:64:03:be:3e:ad:77:02:11:3f:99:de:84:
27:8f:9f:b7:40:0f:e7:0f:52:67:14:a8:ce:d1:0b:
63:13:7c:76:d7:61:37:dd:9b:22:de:6d:3b:31:27:
f7:ac:ef:9c:46:ef:c5:a2:d0:15:3d:24:08:ff:ab:
67
coefficient:
00:bd:5d:58:a8:75:3a:79:8d:01:06:90:80:de:57:
6d:9e:69:fc:46:62:ca:24:85:a1:0a:9c:6a:2f:b6:
65:40:f5:e9:15:30:41:1d:5f:41:e4:c2:7a:73:1c:
53:52:4e:8a:ad:0d:0f:f9:66:49:14:d7:fd:32:9e:
8e:1e:ed:56:2c:88:ac:9f:97:4b:ca:a0:c4:f6:e8:
7f:99:a4:94:1f:3f:75:ca:7f:1b:6b:69:bd:c5:ee:
50:01:76:9d:ab:5d:a3:36:7c:0a:01:14:71:06:7b:
0b:4a:80:66:24:36:56:36:dc:33:a8:2d:b4:ea:d0:
f1:58:05:da:dd:b8:8b:fe:e3:b7:ae:dc:18:2d:1c:
24:73:dd:40:19:14:11:c7:aa:01:9e:2d:ec:2a:cc:
77:09:48:c6:fa:b9:55:f6:76:0c:a6:a4:d3:a1:ea:
04:3f:ac:10:ad:69:9d:0d:7b:6d:ed:43:b5:c9:bf:
0f:62:78:62:18:87:f4:60:1e:9b:6e:cc:ab:0a:9d:
6d:98:75:59:e3:9a:64:aa:b5:5d:b9:80:c3:e5:e7:
20:ee:45:9f:d5:d9:db:34:97:16:96:ec:8e:39:08:
9e:89:b4:4d:bf:14:2f:ba:c4:ec:ff:90:58:62:4d:
20:80:04:16:9c:6f:d8:02:a6:59:45:41:85:69:ca:
2c:4a

3. server.csr

Certificate Request:
Data:
Version: 1 (0x0)
Subject: CN = www.yuchen2023.com, O = Yuchen2023 Inc., C = US
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
31:75:47:65:c0:3a:10:43:f5:18:6f:02:5d:09:8e:
a4:b8:00:9b:9b:a5:c4:0e:64:89:ce:2f:00:a2:c8:
54:9b:8b:68:b3:44:96:67:7e:61:80:c4:58:ad:62:
71:24:30:a1:ce:c8:b0:b5:a7:5e:4d:e1:fa:9a:19:
fe:46:cd:69:5b:bc:98:74:c4:d5:be:cc:e6:48:e8:
13:0e:99:ed:e9:74:59:41:ab:99:fc:19:e2:70:31:
83:d1:e5:93:93:6b:c9:ff:f2:07:eb:24:25:3e:f3:
9b:2a:ec:51:7a:c1:f3:3f:77:a2:0e:bf:d4:4f:0c:
78:99:9b:2e:8c:14:29:25:8f:c2:b3:80:3d:02:b9:
20:26:dc:e7:ed:4a:d3:68:4f:01:25:2e:54:26:db:

95:98:38:1a:37:ce:8f:15:97:22:94:8d:1d:92:35:
17:47:7f:e5:05:30:c5:0b:bf:3f:b5:11:cb:30:af:
40:74:7f:87:2b:52:a4:29:5b:31:2c:37:c1:13:12:
f0:3f
Exponent: 65537 (0x10001)
Attributes:
Requested Extensions:
X509v3 Subject Alternative Name:
DNS:www.yuchen2023.com, DNS:www.yuchen2023A.com, DNS:www.yuchen2023B.com
Signature Algorithm: sha256WithRSAEncryption
ba:9b:7b:4b:fa:9f:cb:85:32:a4:f9:73:2b:49:1b:7f:a7:0e:
ef:bd:6f:6f:a0:f9:e8:24:65:f9:ee:79:24:ca:ce:f1:0a:12:
19:1d:91:d6:2d:07:88:d0:c6:85:b5:a1:54:80:8e:6e:05:83:
8a:80:df:fd:fa:99:5f:f8:6d:19:f0:42:a7:d3:e9:75:38:a1:
ad:3a:c8:0f:82:32:f3:e6:74:ee:84:73:cb:44:21:1e:40:e1:
9c:7f:1f:45:94:7f:b8:a8:61:bb:ec:75:17:a1:9f:68:ab:44:
2a:ea:f8:ad:9f:8e:63:4b:27:74:a3:90:b0:d3:c3:75:24:a5:
fe:72:51:35:ad:f6:a4:d0:46:60:32:52:ef:f5:f7:63:6d:61:
59:61:ed:56:ab:ca:0b:a7:90:36:ca:91:27:24:00:d7:36:be:
98:c8:56:9f:70:1b:ba:42:2a:77:92:60:cf:d0:59:62:35:e8:
95:ac:fa:fe:92:84:3b:3c:dd:6f:19:2a:c6:eb:8b:cb:e8:19:
35:3d:64:b0:61:27:7f:7d:d0:80:48:b2:1c:f1:c0:34:57:ab:
08:ad:cb:9b:b5:40:c4:44:e2:83:4f:79:27:44:34:85:6b:77:
29:18:72:6d:22:6a:02:86:ee:01:81:96:a1:cf:1a:26:fc:14:
0f:64:75:3a

4. server.key

RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
31:75:47:65:c0:3a:10:43:f5:18:6f:02:5d:09:8e:
a4:b8:00:9b:9b:a5:c4:0e:64:89:ce:2f:00:a2:c8:
54:9b:8b:68:b3:44:96:67:7e:61:80:c4:58:ad:62:
71:24:30:a1:ce:c8:b0:b5:a7:5e:4d:e1:fa:9a:19:
fe:46:cd:69:5b:bc:98:74:c4:d5:be:cc:e6:48:e8:
13:0e:99:ed:e9:74:59:41:ab:99:fc:19:e2:70:31:
83:d1:e5:93:93:6b:c9:ff:f2:07:eb:24:25:3e:f3:
9b:2a:ec:51:7a:c1:f3:3f:77:a2:0e:bf:d4:4f:0c:
78:99:9b:2e:8c:14:29:25:8f:c2:b3:80:3d:02:b9:
20:26:dc:e7:ed:4a:d3:68:4f:01:25:2e:54:26:db:
95:98:38:1a:37:ce:8f:15:97:22:94:8d:1d:92:35:
17:47:7f:e5:05:30:c5:0b:bf:3f:b5:11:cb:30:af:
40:74:7f:87:2b:52:a4:29:5b:31:2c:37:c1:13:12:
f0:3f
publicExponent: 65537 (0x10001)
privateExponent:
12:b4:85:64:42:15:e5:67:cc:fc:39:1b:04:8f:0f:

37:fd:2f:c2:80:2e:7a:24:1f:36:34:54:eb:61:c6:
06:f6:a9:a9:ca:d2:02:01:d1:0c:39:81:f6:41:44:
6f:97:6f:32:67:15:0a:00:50:22:b0:67:95:be:72:
8b:9c:06:f5:3f:90:e0:81:1d:e5:e4:11:46:63:05:
e4:3a:43:3f:0e:13:d9:ee:8b:79:92:58:f8:d6:fc:
fa:de:b9:11:a2:8f:66:49:3d:fe:e5:07:80:6e:5a:
9b:e3:ae:23:76:f7:83:88:da:2a:da:7e:e6:16:11:
a0:0e:cb:1c:51:3b:c3:d8:a6:f5:45:4d:bd:c6:46:
2a:16:5a:58:c8:e5:f2:e0:c4:48:02:2e:ce:07:42:
2f:ed:fe:2e:63:e8:a0:35:79:87:04:39:ac:41:ab:
11:23:45:1f:b1:8e:7a:1f:a1:63:be:7b:65:50:ef:
d1:29:bc:40:e8:80:75:bf:0c:fa:62:36:fb:fc:64:
f2:63:af:38:52:89:11:34:3d:c2:e4:68:f8:de:10:
d5:f2:0f:fb:d9:ec:de:ce:21:62:b7:1a:7c:ff:47:
35:bf:99:e7:27:a8:4f:b3:8e:a2:16:7b:bd:6c:82:
80:43:1a:ed:32:a3:b7:2f:f0:19:7d:fd:40:c2:45:
d9
prime1:
00:fa:9d:4f:d2:6a:6d:b0:50:80:bf:bb:aa:77:62:
53:5d:c2:9f:9a:06:2e:04:34:73:7b:bd:05:d9:e6:
96:91:bc:00:be:05:6a:9a:73:b7:39:fe:83:ec:90:
c1:da:c4:47:5c:1a:4a:5c:0d:d6:67:a9:41:17:02:
8d:1b:46:19:bf:47:88:70:bf:f3:e6:f0:4c:0c:d5:
c7:16:a9:ce:1e:3b:9a:06:62:d6:54:4a:12:db:9f:
b5:f4:f7:ea:7d:c0:08:cc:b9:8d:12:bb:f9:bd:17:
ea:86:43:ae:fe:8e:53:d6:6c:86:1e:84:f4:74:51:
cc:62:b3:99:cd:40:b5:1b:ad
prime2:
00:c0:25:ae:74:57:9f:6e:51:08:13:62:1a:39:66:
b8:a0:71:01:06:ec:45:17:3c:55:73:c8:04:7a:9a:
32:a8:7c:23:f7:22:76:9b:2d:fb:88:94:4b:9c:65:
f4:b0:19:91:d7:14:6a:8c:06:26:38:08:26:e2:48:
1c:97:43:f3:4d:5e:09:b8:5d:e3:cb:72:61:0b:2b:
35:1c:71:78:55:c4:03:12:d7:76:84:4a:c1:9a:af:
27:0d:9a:6a:8f:a2:05:c9:6f:14:94:08:a7:1f:8b:
f9:8e:c1:e8:c1:df:e6:e8:36:a8:16:7f:e3:83:52:
a4:3e:40:20:4c:b9:fd:b9:1b
exponent1:
42:8e:96:cd:5e:00:85:8b:cb:b5:9f:e4:74:d2:43:
2b:aa:6d:72:9d:63:89:30:58:df:2a:e3:2b:ec:86:
5e:6b:dc:92:9a:a3:a6:23:47:2c:fa:c0:14:8a:99:
41:3d:51:6a:4f:7d:22:17:76:b2:8f:0b:bf:4d:a9:
25:ee:27:16:5a:ac:0c:ad:9d:db:de:43:84:41:1e:
1f:91:b7:30:e6:49:50:9a:dd:2b:03:85:20:98:b8:
dd:37:1e:2a:89:5e:8c:e8:56:63:fc:52:25:fa:fd:
08:ed:5e:c3:32:0f:67:e9:e8:70:a0:84:bf:83:9d:
d1:34:bb:8a:fc:3d:5c:fd
exponent2:
00:80:20:60:5d:3a:14:98:e6:35:c1:5f:18:67:90:

64:aa:af:cf:e4:82:e6:6b:61:13:06:3a:a9:29:eb:
ea:bd:c8:d1:de:b8:bf:68:28:d8:62:b1:a8:5d:a8:
ea:ea:06:92:e6:5d:b9:d2:97:43:22:f7:e4:9d:dd:
42:1b:67:f7:34:6e:f1:82:5c:31:4a:f7:81:58:86:
3e:4b:32:2a:f0:dd:dc:c2:d2:a4:38:00:f5:6a:a5:
43:20:62:08:8e:b0:96:b5:44:79:ef:60:79:b8:a2:
89:0d:b5:a5:f4:a9:cd:fa:a8:7f:9b:49:3a:37:d6:
82:a8:f3:ef:d5:d9:ec:23:63
coefficient:
50:99:74:4d:b5:8b:05:4b:36:c2:15:ff:09:74:26:
df:d1:5c:21:43:8c:00:72:ef:15:39:b4:24:5f:01:
a2:9b:f6:b4:21:60:ab:6b:03:29:3c:64:5b:89:bd:
4a:e6:0d:b8:1e:4e:d7:67:62:de:0a:b3:ac:ed:5e:
01:00:62:d5:46:4a:a7:8b:ff:87:88:65:a8:0b:61:
98:95:a3:ee:ed:2f:cf:e1:de:18:33:e0:c0:99:78:
a8:1d:bf:99:5f:f2:19:f7:b5:42:49:27:e5:bd:38:
8f:ba:89:77:68:bc:a5:5b:bb:53:87:c5:0b:9a:f3:
d9:7a:02:3c:89:9d:cc:89

5. server.crt
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4661 (0x1235)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
Validity
Not Before: Oct 16 08:01:49 2023 GMT
Not After : Oct 13 08:01:49 2033 GMT
Subject: C = US, O = Yuchen2023 Inc., CN = www.yuchen2023.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:bc:1a:df:63:2a:8c:5f:99:a5:92:f5:02:b2:7f:
f8:bc:18:f9:31:23:aa:c5:60:2d:07:a4:5c:38:fc:
66:f2:8d:ac:d1:a0:89:84:e2:39:fb:4e:d8:97:48:
94:ad:26:40:92:b0:82:c5:cc:4f:77:a2:70:fb:03:
31:75:47:65:c0:3a:10:43:f5:18:6f:02:5d:09:8e:
a4:b8:00:9b:9b:a5:c4:0e:64:89:ce:2f:00:a2:c8:
54:9b:8b:68:b3:44:96:67:7e:61:80:c4:58:ad:62:
71:24:30:a1:ce:c8:b0:b5:a7:5e:4d:e1:fa:9a:19:
fe:46:cd:69:5b:bc:98:74:c4:d5:be:cc:e6:48:e8:
13:0e:99:ed:e9:74:59:41:ab:99:fc:19:e2:70:31:
83:d1:e5:93:93:6b:c9:ff:f2:07:eb:24:25:3e:f3:
9b:2a:ec:51:7a:c1:f3:3f:77:a2:0e:bf:d4:4f:0c:
78:99:9b:2e:8c:14:29:25:8f:c2:b3:80:3d:02:b9:
20:26:dc:e7:ed:4a:d3:68:4f:01:25:2e:54:26:db:
95:98:38:1a:37:ce:8f:15:97:22:94:8d:1d:92:35:
17:47:7f:e5:05:30:c5:0b:bf:3f:b5:11:cb:30:af:

```
                40:74:7f:87:2b:52:a4:29:5b:31:2c:37:c1:13:12:
                f0:3f
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            42:02:90:1C:B8:7F:9C:56:6E:0B:13:9B:B6:61:2B:37:93:03:1E:0E
        X509v3 Authority Key Identifier:
            keyid:E0:A5:4A:9E:10:1C:97:09:A2:D4:F1:83:B0:89:C1:ED:AE:4B:FE:25

        X509v3 Subject Alternative Name:
            DNS:www.yuchen2023.com, DNS:www.yuchen2023A.com, DNS:www.yuchen2023B.com
Signature Algorithm: sha256WithRSAEncryption
    12:53:69:c2:69:7b:95:82:e2:b2:73:61:67:01:65:c2:c8:84:
    51:70:27:39:73:40:59:70:53:73:bd:db:84:4a:8e:32:30:98:
    bf:3a:3a:11:59:42:ca:e6:30:cc:3c:af:15:90:9f:7e:0d:c2:
    4e:da:60:15:2e:dd:27:31:44:c5:8c:f9:96:55:68:6f:17:3d:
    0d:7d:9c:8b:f2:8a:1e:0c:53:44:70:a7:13:77:75:52:8c:f3:
    8f:f1:d3:eb:7e:c3:af:d3:c6:b2:ab:9a:4b:3e:d4:0f:be:e3:
    69:14:50:67:0e:4a:07:66:b4:dd:e4:59:ce:0d:2d:3d:af:42:
    c7:2f:44:3c:a4:15:de:16:e0:49:59:b5:02:ae:5c:51:da:f8:
    a6:e1:f6:38:ec:e7:62:db:dc:09:e0:a6:b5:30:56:90:8e:62:
    6f:a5:a2:ec:ea:99:86:75:d2:66:77:0f:a1:a7:42:ca:59:4b:
    fb:2e:ff:6f:10:34:22:5a:a6:ac:dd:ec:88:7f:a7:37:61:06:
    a3:5d:73:db:b4:0b:a0:db:7e:4d:5e:96:bb:32:71:51:12:f7:
    e9:9f:1b:1a:59:2f:9d:da:3d:7f:cb:55:9e:a2:4e:b9:74:db:
    df:61:82:28:0b:97:30:cb:e7:c6:90:8e:8a:6b:92:c3:cf:72:
    7e:24:00:bd:49:56:55:33:a8:91:ca:bc:b8:08:6c:ba:f4:dc:
    3b:f8:04:d2:20:a7:82:26:44:07:cd:02:61:57:04:57:0c:e4:
    c9:6e:d8:8a:55:e4:41:5c:ea:74:f8:58:5c:8f:e9:0c:a8:03:
    2f:b0:8f:84:99:2d:8b:7f:6f:fd:56:7a:57:3c:80:f9:89:74:
    a0:b5:13:40:ca:66:e4:76:54:19:66:82:d1:51:29:ce:c5:4b:
    db:95:a6:25:29:26:44:2c:d3:11:be:08:37:06:bf:17:ea:86:
    2f:75:93:6a:31:02:72:b8:48:53:bc:46:b5:4b:d2:c0:d5:4e:
    a6:62:a6:fd:aa:2f:d3:e0:0d:1a:20:62:b5:3d:b4:f7:fc:a7:
    ca:7a:47:a4:f0:fd:a9:fc:2c:84:37:23:9f:18:50:80:e1:4b:
    d5:e7:32:27:88:c5:99:6a:f6:f4:74:ed:05:f4:78:02:d8:88:
    e7:87:d6:85:f8:57:fd:b3:ee:25:f7:4b:a3:ff:c0:77:3e:06:
    6f:ef:ab:2d:47:f0:1f:d6:60:c0:49:8c:4b:33:67:bd:23:dd:
    79:69:44:44:6d:0d:94:b0:a8:8d:6b:cd:04:31:50:11:d3:83:
    91:b0:b3:d2:8e:2d:9e:97:71:e5:7b:04:a7:b1:eb:68:8b:91:
    3d:74:c3:b1:f5:c5:80:53
```