Lab 4

Student ID: 1005288

For this lab, all openssl commands will be run in the seed@VM, and the container will be the victim / user

1

Preparation:

run the install.sh script given, which will create the demoCA folder with the required files
configure the /usr/lib/ssl/openssl.cnf file: uncomment the line on unique_subject

Run the commands to create ca.crt and ca.key, can press enter for all prompts
Running openssl x509 -in ca.crt -text -noout opens the certificate file that we want to check, we can look at the subject and issuer field

The subject is Model CA LTD, and the CA flag is set to True. Implying that this is a CA's certificate.

```
[10/17/23]seed@VM:~/.../Labsetup$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:7f:df:1d:ce:bf:dc:e9:10:93:05:1f:ed:f9:1b:de:36:a5:75:0a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 17 06:01:13 2023 GMT
            Not After : Oct 14 06:01:13 2033 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
        Subject Public Key Info:
```

```
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                67:BA:F3:C9:5B:2D:8A:F9:A2:15:80:0D:2B:AE:B2:5D:FA:F1:59:53
            X509v3 Authority Key Identifier:
                keyid:67:BA:F3:C9:5B:2D:8A:F9:A2:15:80:0D:2B:AE:B2:5D:FA:F1:59:53

            X509v3 Basic Constraints: critical
                CA:TRUE
```

This cert has the same subject and authority key identifiers, showing that the subject was the one that signed this certificate. Thus this certificate was self-signed.

Running openssl rsa -in ca.key -text -noout opens the key file, the privateExponent, publicExponent and modulus are explicitly stated in the opened file.
Hence, e = publicExponent, d = privateExponent, n = modulus; p and q are widely known as large prime numbers, hence they are prime1 and prime2.

```
privateExponent:
    24:0b:a3:5f:09:c7:bf:b5:33:9a:83:c8:01:cb:6b:
    19:cb:3d:23:9c:90:09:43:f8:ac:54:ec:12:49:10:
    9d:e9:74:2c:8d:b4:92:09:58:99:db:a6:96:9e:d0:
    09:1f:cc:d9:04:52:4d:3f:b7:fa:6b:9e:9c:5c:ad:
    15:35:f2:e1:ff:4f:4f:5a:7f:74:5b:0b:1a:9d:0c:
    1b:ad:19:3f:fe:fd:a7:68:bd:9e:42:cb:26:4a:70:
    13:16:a0:ba:61:8a:f4:b4:19:cd:94:ca:ec:08:20:
    89:a9:ff:30:b0:1d:6c:09:4d:b7:72:65:26:a1:3f:
    d7:af:e1:4d:e5:77:53:09:93:f1:18:0a:d9:52:35:
    af:be:0f:81:63:e3:c3:7b:43:dc:2c:53:77:d3:82:
    3a:6e:ec:04:9e:18:aa:a0:59:dc:84:45:d1:78:82:
    f3:31:00:69:ab:ce:de:1c:01:a2:99:3a:f9:a0:5e:
    ca:68:49:fa:38:62:dd:67:f9:32:8e:03:d4:53:05:
    b2:d6:a6:ce:1a:55:d3:3d:bf:fe:7f:c7:ea:44:b1:
    02:b5:f5:d3:7e:3c:45:4f:84:fd:f3:09:ab:a9:0b:
    7f:13:bc:c6:49:e2:81:9a:c0:e3:97:ff:d5:87:9a:
    ab:57:2d:82:7d:60:5a:1e:f2:01:3c:da:3b:8e:45:
    a2:68:10:21:76:8b:59:50:66:25:e0:f7:da:aa:ef:
    96:47:aa:e8:68:82:ae:a6:6a:61:e2:91:6a:ca:76:
    c4:26:64:86:df:49:73:0d:7e:d8:5a:be:e5:42:90:
    96:59:e0:3a:a3:42:62:f5:82:85:af:9b:9f:5b:d6:
    b6:32:14:73:62:48:61:05:16:28:b4:99:2e:a3:da:
    89:59:42:d9:b8:5b:58:83:17:92:00:42:63:eb:3f:
    22:97:6b:20:cd:58:86:7b:32:d0:74:24:1f:00:52:
    27:10:02:19:c1:7d:3d:b0:61:a7:22:57:5d:2c:4c:
    95:fc:e4:44:20:0d:eb:a4:32:14:87:56:a6:19:aa:
    ee:f4:74:46:c8:2c:0f:29:01:a3:b8:76:22:68:68:
    75:ce:96:7c:1b:99:b2:74:30:53:d5:8e:df:5f:00:
    68:6e:e3:b0:f4:d2:8b:2b:79:f4:f1:45:d3:02:de:
    de:e9:66:19:0f:68:81:9a:d4:6b:a8:f7:b4:d7:c8:
    da:43:91:d5:d3:a8:2d:b2:f0:cd:e4:b7:b8:c9:88:
    14:45:2b:1c:3b:ca:15:a8:44:fc:bf:77:3b:b0:21:
    b1:25:9e:3a:06:f5:f0:0d:5c:09:49:6b:69:cb:82:
    f6:5c:12:9e:2f:27:92:86:ed:52:a1:ca:2a:0e:c8:
    51:09

modulus:
    00:c0:f7:bf:a5:ef:d4:b3:c6:b0:11:e3:31:d8:2c:
    19:b4:6e:b9:c1:37:93:61:a8:4b:9f:6b:f4:45:de:
    59:e6:07:7c:f7:cc:d4:f5:60:0a:1a:c5:aa:7a:27:
    33:bb:e8:89:5d:55:03:2b:69:b6:84:fd:4d:94:ea:
    e8:d3:db:32:90:2b:30:5c:8d:00:c5:4a:64:69:10:
    28:aa:d4:d0:e3:5b:2a:d5:d9:b6:1e:8a:21:3a:f6:
    4d:fd:8c:0f:e9:f6:fe:7f:e0:2e:e0:8f:b7:13:d8:
    9d:4a:f5:5a:5a:3d:70:cc:e8:3d:3e:b2:03:1d:c9:
    58:cf:6f:fb:44:f0:d7:fc:56:a2:ea:60:86:dd:da:
    41:33:90:10:b7:c2:35:9a:af:0e:eb:4d:28:07:2c:
    15:34:02:a4:f0:f2:2e:f0:d6:e5:e0:ed:9a:d3:01:
    4e:29:52:01:cf:fd:d6:22:1a:ad:89:88:6b:20:91:
    0d:3b:7e:c6:36:00:5b:76:8b:68:d1:ef:a7:b7:df:
    6b:91:02:2a:d7:bf:81:cf:79:e6:13:26:7c:6c:d6:
    34:19:68:31:61:bd:ff:7d:16:c2:17:2b:b2:84:22:
    71:d8:6b:50:b8:29:56:85:86:ae:5e:49:c3:a3:a4:
    7e:b3:cb:7c:e0:91:45:0a:25:fa:66:46:96:27:68:
    75:20:45:12:7d:c0:a4:e5:66:cc:1d:e1:6e:b6:3e:
    93:af:7b:cc:17:e5:67:e6:3f:99:38:2e:62:70:75:
    d3:96:c5:43:e8:01:b3:13:92:cf:e6:57:79:21:fd:
    1d:91:8e:81:1c:84:9f:ab:be:15:b8:a0:bf:c2:88:
    2a:e1:23:5d:7e:b4:58:a2:94:9d:41:c1:09:76:7c:
    c4:f1:b6:f5:95:a8:62:76:6b:ca:91:af:9e:6f:91:
    7d:72:fd:86:8d:f8:9e:2b:f5:0f:49:c2:08:3e:c7:
    2d:d4:ac:ba:0e:8c:33:86:0d:f2:b0:63:32:00:c7:
    e3:3e:72:86:b0:d9:04:39:06:0d:85:79:82:66:84:
    bc:ff:ce:66:fd:ef:92:99:ba:be:41:63:6d:0e:e8:
    be:2d:82:2a:70:42:cd:bd:5d:7d:ec:db:10:70:3e:
    dd:f7:1c:06:82:b6:dc:1b:77:e5:ef:cc:4b:f4:8d:
    bd:13:0a:45:f8:93:c1:a8:2f:4f:bc:5a:ed:10:5f:
    aa:f3:f2:24:06:3e:fa:9a:26:95:58:92:b8:d0:4c:
    11:bf:9c:42:48:0b:61:5f:03:8d:71:8d:a3:f5:3e:
    dc:53:3a:c8:44:40:48:03:23:21:22:9a:58:cd:4e:
    5e:d8:be:9a:7c:3d:5d:0e:94:e6:0c:08:61:44:94:
    4d:15:91
publicExponent: 65537 (0x10001)

prime1:
    00:f5:c0:76:c7:4c:26:71:1c:38:d4:83:8c:4b:2f:
    a8:49:4d:c0:4d:77:3d:91:fd:d9:26:e3:3b:21:45:
    10:35:af:1c:f2:7e:e4:be:b6:26:e4:8e:72:eb:5e:
    35:4b:2c:99:37:f1:b2:dc:80:27:1e:2d:87:b4:28:
    b3:01:be:40:4b:15:33:e2:0f:9e:9c:15:a3:99:35:
    c6:3d:1f:8c:2d:7b:0b:cf:57:47:f0:2e:8c:ea:f3:
    4e:ab:e1:e5:d1:36:d7:0b:1b:50:68:7f:92:67:2b:
    31:bf:6b:20:c4:17:01:10:c4:5b:40:0a:2e:ee:8d:
    ea:77:0e:e0:71:f3:45:1f:b9:8f:b3:e0:c9:dd:91:
    e1:7d:08:d3:c2:c9:6d:f8:62:a6:03:df:19:77:fb:
    86:e1:e4:fc:e2:26:c9:76:ae:e4:e3:8c:5a:a8:1f:
    dd:24:0b:64:2b:8b:a1:b4:2b:14:0c:b7:de:16:f3:
    5e:4d:f0:9f:29:f0:da:92:2f:c3:c6:cd:31:3b:70:
    81:a1:88:8f:4f:5f:86:e0:f1:ba:20:4a:dc:57:03:
    32:87:f8:e9:45:a8:e3:b7:46:36:81:64:00:5c:1d:
    f3:4b:10:ab:24:69:8f:b9:88:d7:c4:f9:91:1b:4b:
    80:04:b8:53:52:36:c4:5d:00:13:9f:e2:44:fc:a7:
    f7:67
prime2:
    00:c9:03:c9:2f:dd:ff:6a:22:5b:ee:39:d7:4a:a0:
    f0:6b:4e:73:f6:3a:89:49:ab:6c:cf:a2:ba:ca:6c:
    82:b0:5b:42:82:ab:ca:4e:ba:7a:48:25:b2:42:59:
    6b:04:55:0b:bc:d3:fc:25:43:dc:d4:b9:fb:c5:1e:
    33:77:d9:18:b6:8e:c5:48:61:9a:0d:88:a5:92:9b:
    50:b3:ec:a4:93:c4:39:95:cc:79:63:55:88:72:07:
    88:03:90:a9:25:d4:13:61:f5:67:3d:c0:50:f0:b1:
    ce:15:cf:8a:4a:f4:98:71:d6:f9:55:e0:70:08:0e:
    0e:25:ff:37:68:11:ab:8b:08:9f:0a:f3:18:66:bd:
    31:a7:29:d1:6a:aa:a7:68:81:3b:8d:db:1a:bc:46:
    63:ba:92:6e:c6:74:38:53:a8:82:ed:f7:29:95:3d:
    d7:66:99:cc:c4:df:a3:00:79:bb:19:bb:ba:f0:b4:
    81:94:89:d3:ec:85:b5:94:4c:b6:2d:15:d6:89:5c:
    fd:d4:0e:3d:7b:40:e0:44:1f:7b:5e:07:1e:b7:59:
    75:ec:c6:cf:82:4b:80:7a:04:f6:1d:1a:e0:87:f5:
    58:76:e7:28:94:5c:c7:12:da:06:61:56:f8:77:e6:
    99:32:25:88:1c:ec:9f:51:74:98:c6:ea:92:29:b9:
    c8:47
```

2

After running the openssl command

```
openssl req -newkey rsa:2048
            -sha256 -keyout melvin.key
            -out melvin.csr
            -subj "/CN=www.melvin2023.com/O=Melvin Inc./C=US"
            -passout pass:dees
            -addext "subjectAltName = DNS:www.melvin2023.com, DNS:www.melvin2023A.com,
DNS:www.bank32.com"
```

The melvin.csr and melvin.key files were created, with several hostnames, www.melvin2023.com, www.melvin2023A.com and www.bank32.com as shown in the -addext flag.
We can see that these files were indeed present after running the ls command.

```
[10/17/23]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout melvin.key -o
ut melvin.csr -subj "/CN=www.melvin2023.com/O=Melvin Inc./C=US" -passout pass:dees -addext "
subjectAltName = DNS:www.melvin2023.com, DNS:www.melvin2023A.com, DNS:www.bank32.com"
Generating a RSA private key
..............................+++++
.....................................................................+++++
writing new private key to 'melvin.key'
-----
[10/17/23]seed@VM:~/.../Labsetup$ ls
ca.crt  demoCA              image_www   melvin.csr  volumes
ca.key  docker-compose.yml  install.sh  melvin.key
```

3

Preparation:

change openssl.cnf file: uncomment copy_extension = copy

ensure that demoCA directory is in the same directory as all the ca and server files

the shell script was unable to create a symbolic link, hence the path of the openssl config file (usr/lib/ssl/openssl.cnf) was used in the openssl command instead

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

```
[10/17/23]seed@VM:~/.../Labsetup$ openssl ca -config /usr/lib/ssl/openssl.cnf -policy policy_anything
 -md sha256 -days 3560 -in melvin.csr -out melvin.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4660 (0x1234)
        Validity
            Not Before: Oct 17 06:14:31 2023 GMT
            Not After : Jul 16 06:14:31 2033 GMT
        Subject:
            countryName               = US
            organizationName          = Melvin Inc.
            commonName                = www.melvin2023.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                83:EC:E7:F9:B5:65:1F:F7:5B:34:D6:8A:0E:6E:66:F0:E3:5D:59:23
            X509v3 Authority Key Identifier:
                keyid:67:BA:F3:C9:5B:2D:8A:F9:A2:15:80:0D:2B:AE:B2:5D:FA:F1:59:53

            X509v3 Subject Alternative Name:
                DNS:www.melvin2023.com, DNS:www.melvin2023A.com, DNS:www.bank32.com
Certificate is to be certified until Jul 16 06:14:31 2033 GMT (3560 days)

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

We can see that the authority key is the same as the identifier of Model CA, hence CA signed this certificate. Also, we can check that the Alternative Name field matches the -addext flag value in task2.

4

This was done in the user container

Preparation:

add melvin.crt and melvin.key into the /cert/ of the container

This is not necessary but it makes it more convenient when editing the apache_ssl.conf file when we want to change the certificates

```
root@63e8f7f74164:/etc/apache2/sites-available# cd /certs
root@63e8f7f74164:/certs# ls
bank32.crt  bank32.key  server.crt  server.key
```

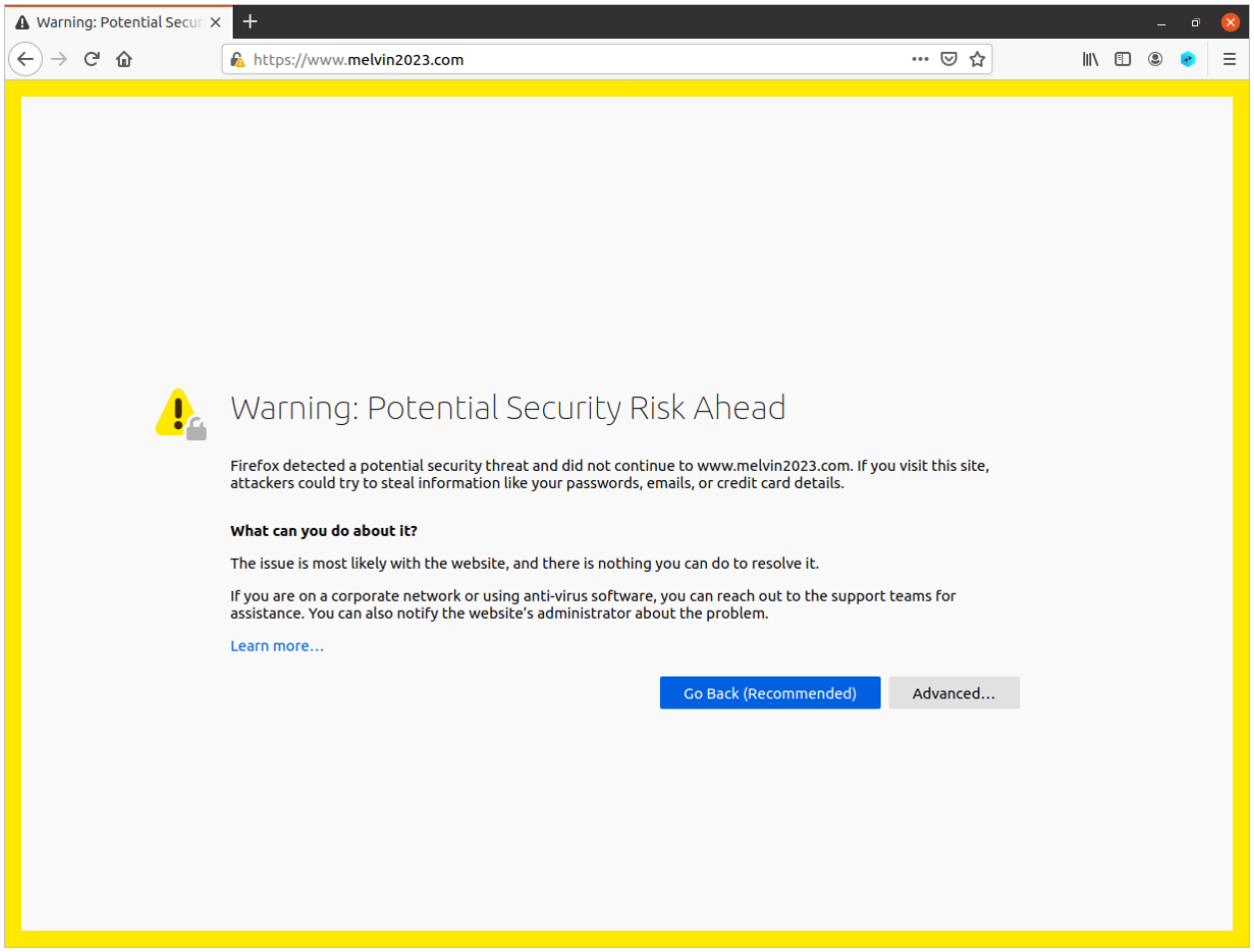
We have to edit the apache32_conf files to use our melvin.crt, melvin.key, and add an alias for www.melvin2023.com

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    #ServerName www.bank32.com
    #ServerAlias www.bank32A.com
    #ServerAlias www.bank32B.com
    #ServerAlias www.bank32W.com
    ServerAlias www.melvin2023.com
    DirectoryIndex index.html
    SSLEngine On
    #SSLCertificateFile /certs/bank32.crt
    #SSLCertificateKeyFile /certs/bank32.key
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>
```

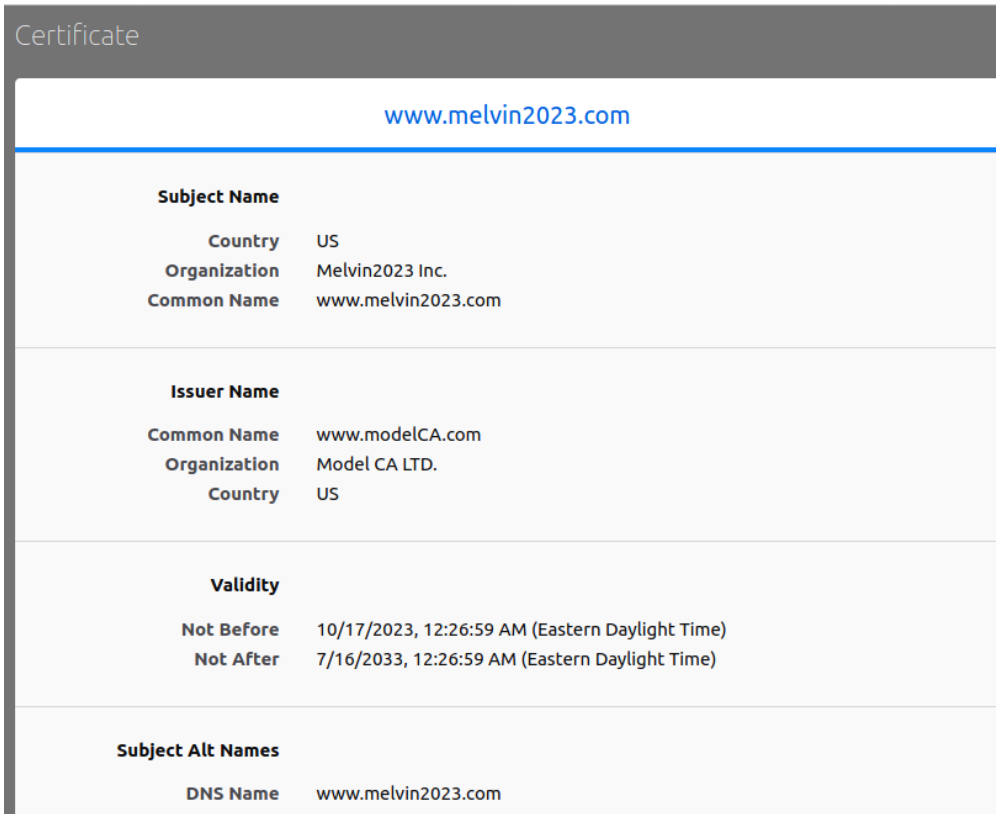
We need to run commands to enable the ssl module and site

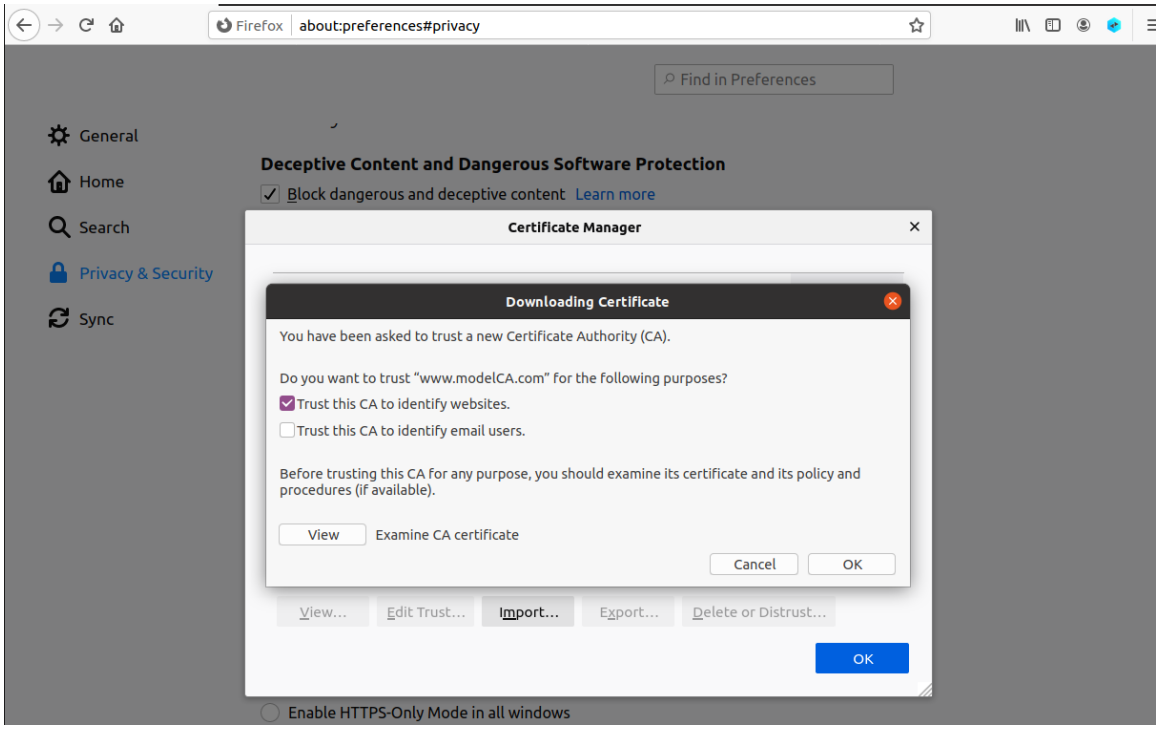
```
root@63e8f7f74164:/etc/apache2/sites-available# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
root@63e8f7f74164:/etc/apache2/sites-available# a2ensite bank32_apache_ssl
Site bank32_apache_ssl already enabled
```

When we first enter the website, we will be prompted that there is a security risk since the certificate was not added to the browser yet.



We need to add the modelCA certificate in firefox using the url about:preferences#privacy, to utilize the chain of trust so that Firefox will accept www.melvin2023.com as a trusted website. We can also view the certificate of this website.





After these, we need to run service apache2 restart, and we can see that the connection with www.melvin2023.com is now secure

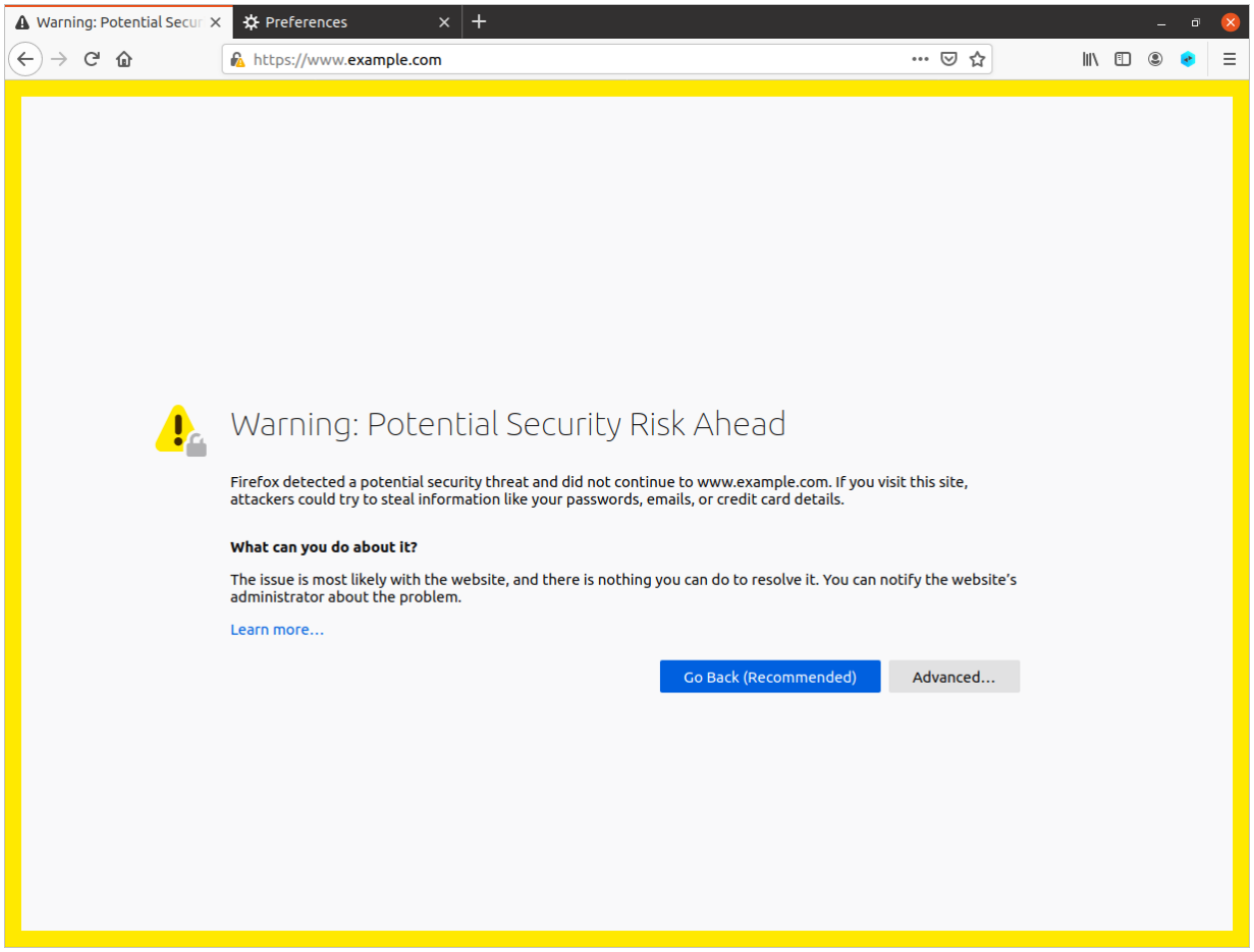
5

Even after adding the domain into /etc/hosts file, firefox will still prompt a warning since www.example.com was not in the alternative domain names given, which means that an attack can only go through if they manage to replace the original csr with the newly added domains
Step 1: edit apache_ssl.conf file, servername = www.example.com, the rest can leave it as it is

```
  GNU nano 4.8                  bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.example.com
    #ServerName www.bank32.com
    #ServerAlias www.bank32A.com
    #ServerAlias www.bank32B.com
    #ServerAlias www.bank32W.com
    #ServerAlias www.melvin2023.com
    DirectoryIndex index.html
    SSLEngine On
    #SSLCertificateFile /certs/bank32.crt
    #SSLCertificateKeyFile /certs/bank32.key
    SSLCertificateFile /certs/melvin.crt
    SSLCertificateKeyFile /certs/melvin.key
</VirtualHost>
```

Step 2: add www.example.com into /etc/hosts file

```
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.9.0.80       5d0c2c73dd14
10.9.0.80       www.bank32.com
10.9.0.80       www.melvin2023.com
10.9.0.80       www.example.com
```



6

For this part, we impersonated an authority CA to sign a similar csr and post it as a trusted site. Basically going over the same workflow, generate a csr with the target domain and a key, get the ca to sign it

Generate csr:

```
openssl req -newkey rsa:2048
            -sha256 -keyout melvin.key
            -out melvin.csr
            -subj "/CN=www.melvin2023.com/O=Melvin Inc./C=US"
            -passout pass:dees
            -addext "subjectAltName = DNS:www.melvin2023.com, DNS:www.melvin2023A.com, DNS:www.bank32.com, DNS:www.instagram.com "

openssl ca -config /usr/lib/ssl/openssl.cnf
                -policy policy_anything
                -md sha256 -days 3650
```

```
                -in server.csr -out server.crt -batch
                -cert ca.crt -keyfile ca.key
```

For this task, I chose www.instagram.com as my target.
This is an output from after we get the CA to sign it, we can see that the Alternative Name www.instagram.com was added

```
        Subject:
            countryName               = US
            organizationName          = Melvin Inc.
            commonName                = www.melvin2023.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                DF:75:BD:40:95:02:C6:FF:33:2A:5F:E8:8A:83:72:78:98:EC:61:7B
            X509v3 Authority Key Identifier:
                keyid:67:BA:F3:C9:5B:2D:8A:F9:A2:15:80:0D:2B:AE:B2:5D:FA:F1:59:5
3

            X509v3 Subject Alternative Name:
                DNS:www.melvin2023.com, DNS:www.melvin2023A.com, DNS:www.bank32.
com, DNS:www.instagram.com
Certificate is to be certified until Oct 14 07:34:38 2033 GMT (3650 days)

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

```
 GNU nano 4.8                 bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    #ServerName www.example.com
    ServerName www.bank32.com
    #ServerAlias www.bank32A.com
    #ServerAlias www.bank32B.com
    #ServerAlias www.bank32W.com
    #ServerAlias www.melvin2023.com
    ServerAlias www.instagram.com
    DirectoryIndex index.html
    SSLEngine On
    #SSLCertificateFile /certs/bank32.crt
    #SSLCertificateKeyFile /certs/bank32.key
    SSLCertificateFile /certs/melvin.crt
    SSLCertificateKeyFile /certs/melvin.key
</VirtualHost>
```

After which, when the user goes into www.instagram.com, the user will see this shown on the browser instead of the real instagram page.


Hello World
Preferences
https://www.melvin2023.com
Hello, world!