Markus Afonso, Devin Kandola
Group 41, Set C
February 13, 2024

(Q1) What part of the certificate indicates this is a CA's certificate?

X509v3 Basic Constraints extension tells us that it is a CA certificate.

```
        86:21:CD:49:C9:31:7F:52:B2:60:3D:72:41:F3:32:A6:09:F2:DA:01
    X509v3 Authority Key Identifier:
        keyid:86:21:CD:49:C9:31:7F:52:B2:60:3D:72:41:F3:32:A6:09:F2:DA:01

    X509v3 Basic Constraints: critical
        CA:TRUE
ature Algorithm: sha256WithRSAEncryption
 87:14:b7:f2:94:9a:0b:fa:56:b2:f5:4c:45:b1:62:bf:c6:b4:
 4f:5d:3e:14:16:b6:21:9c:a6:60:d8:f2:06:f9:52:d1:84:3e:
 e0:64:6b:c6:a3:4e:14:50:60:ec:77:a6:d0:7a:36:a5:18:99:
 6e:7e:7e:71:c5:13:26:8b:f8:d8:0f:be:ad:47:1d:a6:a5:3b:
```

(Q2) What part of the certificate indicates this is a self-signed certificate?

We can tell this is a self-signed certificate by seeing who the issuer and subject are. Since they are the same 'www.modelCA.com', it is self-signed

```
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = CA
Validity
    Not Before: Feb 13 17:07:12 2024 GMT
    Not After : Feb 10 17:07:12 2034 GMT
Subject: CN = www.modelCA.com, O = Model CA LTD., C = CA
Subject Public Key Info:
```

(Q3) What is your web server name? What other alternative names did you add to your certificate signing request?

```
[02/13/24]seed@VM:~/lab6$ openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.c
sr -subj "/CN=www.markusdevin2024.com/O=BCIT/C=CA" -passout pass:dees -addext "subjectAltName =
 DNS:www.markusdevin2024.com, DNS: www.markusdevin2024.ca, DNS:www.markusdevin2024.io"
```

The web server name is "www.markusdevin2024.com". The alternative names added to the certificate signing request are "www. markusdevin2024.ca" and "www. markusdevin2024.io".

(Q4) If this were a real-world scenario, how would you submit the CSR to a Certificate Authority (CA)?

Choose a CA

Prepare the CSR in a command line tool like OpenSSl, where you would include details regarding your information about the organization and your public key

Create an account on the CA platform and submit a request.

CA will send an email that they are validating the CSR. Once the Validation is complete you can download and install the certificate for your web server.

Markus Afonso, Devin Kandola
Group 41, Set C
February 13, 2024

(Q5) List the steps for a web server to get a public-key certificate from a CA?

Generate a key pair: The web server must generate a public and private key pair. The public key will be included in the certificate, while the private key will be kept secure.

Create a CSR (Certificate Signing Request): The CA will perform a validation process to verify the information in the CSR. This may include confirming the domain ownership by checking DNS records

Submit CSR to a CA: In the CRS it will include the public key and identifying information about the website (like domain name and company details).

CA Validation: The CSR is submitted to a Certificate Authority. The CA will validate the identity of the requester and the domain ownership before issuing a certificate.

(Q6) Who is the issuer of this certificate? What part of the certificate indicates this?

The issuer of this certificate is 'www.modelCA.com' this is indicated by the 'Issuer' parameter of the certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = CA
        Validity
            Not Before: Feb 13 17:22:33 2024 GMT
            Not After : Feb 10 17:22:33 2034 GMT
        Subject: C = CA, O = BCIT, CN = www.markusdevin2024.com
        Subject Public Key Info:
```

(Q7) Can the certificate generated in this step be used to sign other certificates. What part of the certificate indicates this?

No, since the basic constraint is CA:FALSE. If a certificate has the Basic Constraints extension set to CA:TRUE, it indicates that the certificate is a CA certificate and can be used to sign other certificates

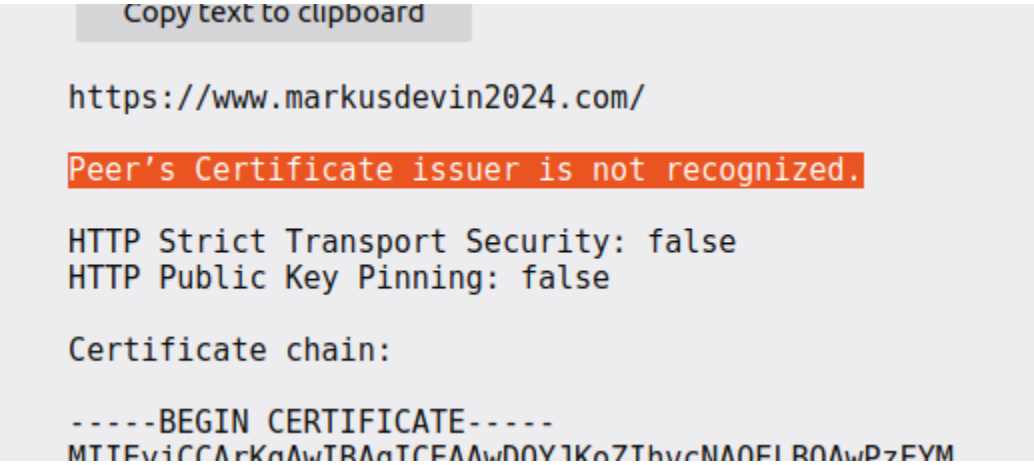
```
                b9:1f
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            8C:9A:F0:89:33:3C:70:E8:9E:6C:67:
```

(Q8) How long is this certificate valid for? Where in the OpenSSL command did we indicate this?

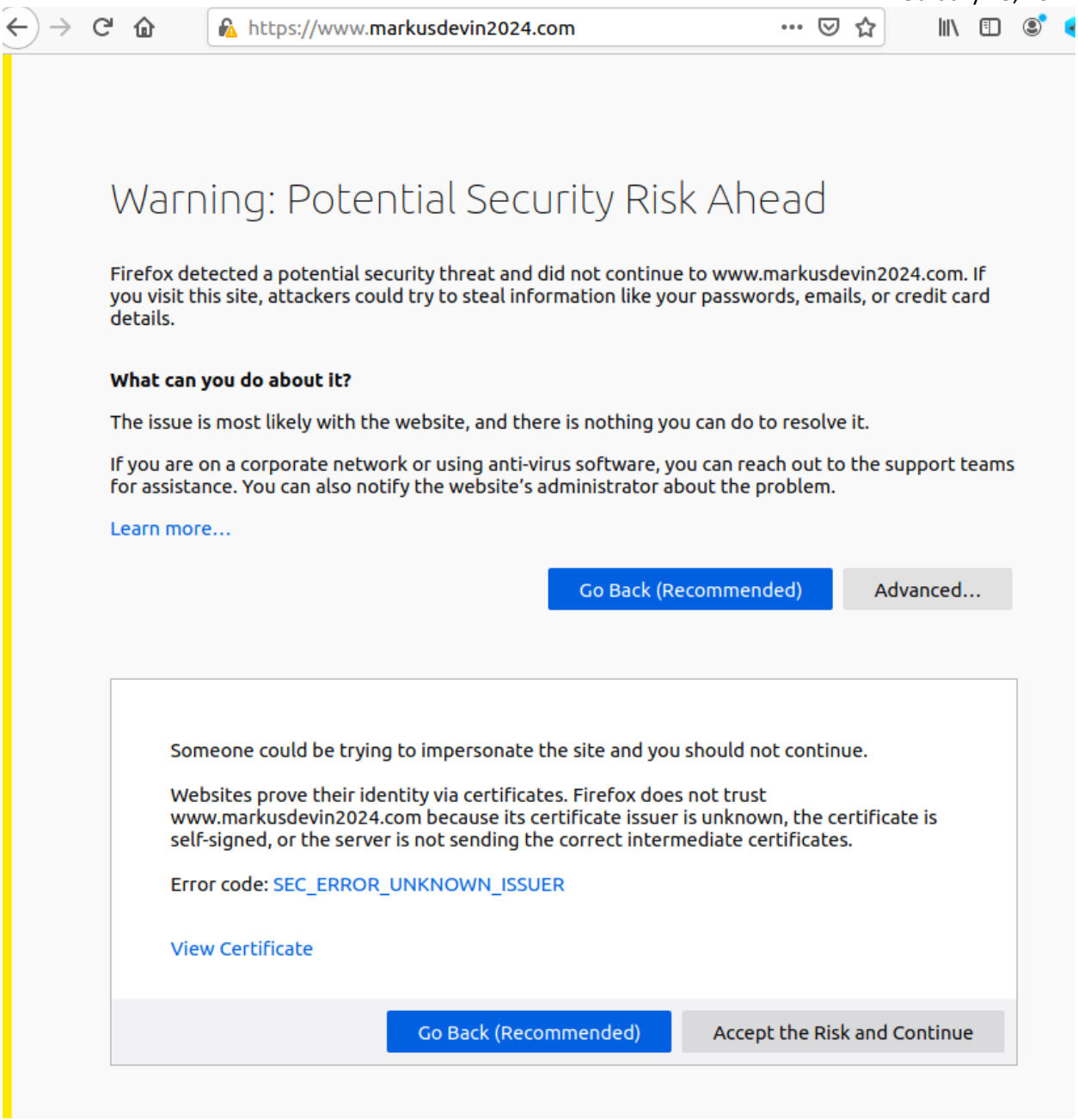
Its valid for 3650 days, we indicated this by passing '3650' with the '-days' option.

(Q9) You should see a warning if you navigate to your HTTPS website. Click on Advanced and explain what you see and why.

The certificate is from an unrecognized issuer:



Markus Afonso, Devin Kandola
Group 41, Set C
February 13, 2024



(Q10) Explain how you can fix this error and provide a screenshot that you can successfully browse the HTTPS website without getting a warning (for the main domain and the alternative domains)

We fixed this warning by adding the ca.crt that we created to sign the key. By doing this, Firefox now sees the certificate was signed by an authorized issuer.

Markus Afonso, Devin Kandola
Group 41, Set C
February 13, 2024

(Q11) On the container, navigate to /etc/apache2/sites-available and add the following entry to the field for the HTTP connection in mywebsite_apache_ssl.conf file that was copied there when you ran the container. Restart the server and provide a screenshot to show that all coming traffic will be directed to the HTTPS version.

```
[02/13/24]seed@VM:~/lab6$ curl http:/www.markusdevin2024.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.markusdevin2024.com">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.markusdevin2024.com Port 80</address>
</body></html>
[02/13/24]seed@VM:~/lab6$
```

(Q12) Explain what warning you will see when navigating to this website (https://www.example.com/) on the VM (via HTTPS).

> The warning indicates that the url www.example.com does not match the certificate. This happened because we specified our domain (www.markusdevin2024.com) when we created the certificate.