Colin Quinn

CS 455 Lab 3

After making the directory:

```
[02/05/20]seed@VM:~/quinn3$ ls
certs  crl  index.txt  newcerts  openssl.cnf  pkilab2020  serial
```

After generating the CA:

```
[02/05/20]seed@VM:~/quinn3$ openssl req -new -x509 -keyout ca.key -out ca.crt -c
onfig openssl.cnf
Generating a 2048 bit 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]:Michigan
Locality Name (eg, city) []:Flint
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kettering
Organizational Unit Name (eg, section) []:Network Security Lab
Common Name (e.g. server FQDN or YOUR name) []:Colin
Email Address []:quin1211@kettering.edu
```

This has the PEM pass phrase set as : hello

After getting the server's key:

```
[02/07/20]seed@VM:~/quinn31$ openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:d0:d6:4e:19:70:21:3a:9e:62:79:af:e5:3b:6f:
    4d:df:93:09:78:c4:6b:c4:34:86:29:39:eb:36:57:
    44:db:b2:1f:2e:31:49:04:ad:c5:9d:ab:1f:5d:4f:
    ed:ed:99:2c:60:8f:ef:33:96:49:56:be:ab:1b:5c:
    5e:ae:55:03:3e:40:ea:e0:1b:e9:85:12:dc:ee:55:
    2e:0b:34:f1:91:d9:2a:0d:26:05:cb:d4:a3:34:12:
    2e:fd:94:0d:f7:f0:06:23:ae:be:c8:63:39:11:40:
    f9:47:b4:eb:15:a5:72:37:81:4e:42:e5:60:ae:63:
    04:e7:a1:73:b9:0e:2a:f9:b5
publicExponent: 65537 (0x10001)
privateExponent:
    0a:cd:6b:10:c9:ca:0e:3c:2f:1f:d8:47:65:41:a6:
    a7:8f:f5:87:77:b1:93:5e:9c:29:f9:c2:fe:f6:98:
    ab:3c:95:7c:50:34:54:b7:a0:67:3d:78:cb:dc:dc:
    93:d3:be:85:e8:2c:19:61:06:be:23:f2:b9:e1:97:
    4c:31:3d:8f:9c:cc:83:b1:28:33:d7:79:38:c1:b0:
    c4:11:65:7d:e3:38:3e:bd:6d:c6:75:ab:a3:6f:e5:
    c0:69:38:12:83:35:18:8c:37:8b:a5:3d:ba:0e:a4:
    57:e3:12:88:e1:2d:22:b3:ee:bb:57:53:6b:88:f3:
    15:26:d2:6b:e0:61:1f:29
prime1:
    00:fc:89:2c:72:44:d2:e3:b8:06:67:57:f5:c4:02:
    bd:a5:9e:57:37:c3:43:01:ee:03:aa:19:e7:6d:91:
    94:e6:3e:b1:39:40:23:4d:8e:3d:62:b9:d9:c7:96:
    2c:26:a5:de:bb:d4:69:cc:d6:4f:12:dd:d5:d6:07:
    fe:2f:a9:b1:9f
prime2:
    00:d3:b3:ac:e4:19:d2:60:e7:91:c5:8b:f1:ef:ae:
    b1:b6:54:6f:92:ff:55:5c:e5:22:3e:9c:16:13:b8:
    ab:49:3e:06:ac:76:a6:89:1a:7e:5b:1f:11:8a:12:
    4f:76:ca:d8:76:d4:ac:62:ca:7f:00:83:0a:66:b6:
    e4:31:0b:5c:2b
exponent1:
    00:89:f3:04:ec:86:dc:0c:b9:02:06:81:ee:26:dc:
    b8:6c:38:4a:bc:93:55:8f:40:4d:90:26:06:5d:bc:
    20:f2:85:5c:9a:41:87:07:5e:a3:f9:c2:3c:4c:e2:
    a3:cb:98:e0:4b:0a:85:a0:f7:90:ca:65:93:e2:0f:
    0b:b3:4d:a7:51
exponent2:
    6e:67:6b:a8:e1:96:87:96:fc:bc:ab:49:17:18:61:
    f1:96:83:41:84:0b:7e:90:b8:95:32:4d:89:27:6b:
    9c:9c:ce:5a:2e:de:96:ed:cc:2b:b5:3e:2e:65:72:
    2f:9f:85:d8:22:fd:6b:df:f2:ef:cf:67:23:3e:0a:
    2f:51:9f:55
coefficient:
    0c:24:2f:a6:21:88:e7:df:a8:02:7a:49:c8:1d:95:
    4f:53:72:70:8f:01:ea:83:0e:61:73:32:af:59:a9:
    27:13:76:f4:1a:bb:0f:cb:f6:a6:dc:51:d0:3c:db:
    10:cc:55:92:65:17:7a:8a:36:99:22:b4:9e:c6:7b:
    ad:a5:d6:a3
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDQ1k4ZcCE6nmJ5r+U7b03fkwl4xGvENIYpOes2V0Tbsh8uMUkE
rcWdqx9dT+3tmSxgj+8zlklWvqsbXF6uVQM+QOrgG+mFEtzuVS4LNPGR2SoNJgXL
1KM0Ei79lA338AYjrr7IYzkRQPlHtOsVpXI3gU5C5WCuYwTnoXO5Dir5tQIDAQAB
AoGACs1rEMnKDjwvH9hHZUGmp4/1h3exk16cKfnC/vaYqzyVfFA0VLegZz14y9zc
k9O+hegsGWEGviPyueGXTDE9j5zMg7EoM9d5OMGwxBFlfeM4Pr1txnWro2/lwGk4
EoM1GIw3i6U9ug6kV+MSiOEtIrPuu1dTa4jzFSbSa+BhHykCQQD8iSxyRNLjuAZn
V/XEAr2lnlc3w0MB7gOqGedtkZTmPrE5QCNNjj1iudnHliwmpd671GnM1k8S3dXW
B/4vqbGfAkEA07Os5BnSYOeRxYvx766xtlRvkv9VXOUiPpwWE7irST4GrHamiRp+
Wx8RihJPdsrYdtSsYsp/AIMKZrbkMQtcKwJBAInzBOyG3Ay5AgaB7ibcuGw4SryT
VY9ATZAmBl28IPKFXJpBhwdeo/nCPEzio8uY4EsKhaD3kMplk+IPC7NNp1ECQG5n
a6jhloeW/LyrSRcYYfGWg0GEC36QuJUyTYkna5yczlou3pbtzCu1Pi5lci+fhdgi
/Wvf8u/PZyM+Ci9Rn1UCQAwkL6YhiOffqAJ6ScgdlU9TcnCPAeqDDmFzMq9ZqScT
dvQauw/L9qbcUdA82xDMVZJlF3qKNpkitJ7Ge62l1qM=
-----END RSA PRIVATE KEY-----
```

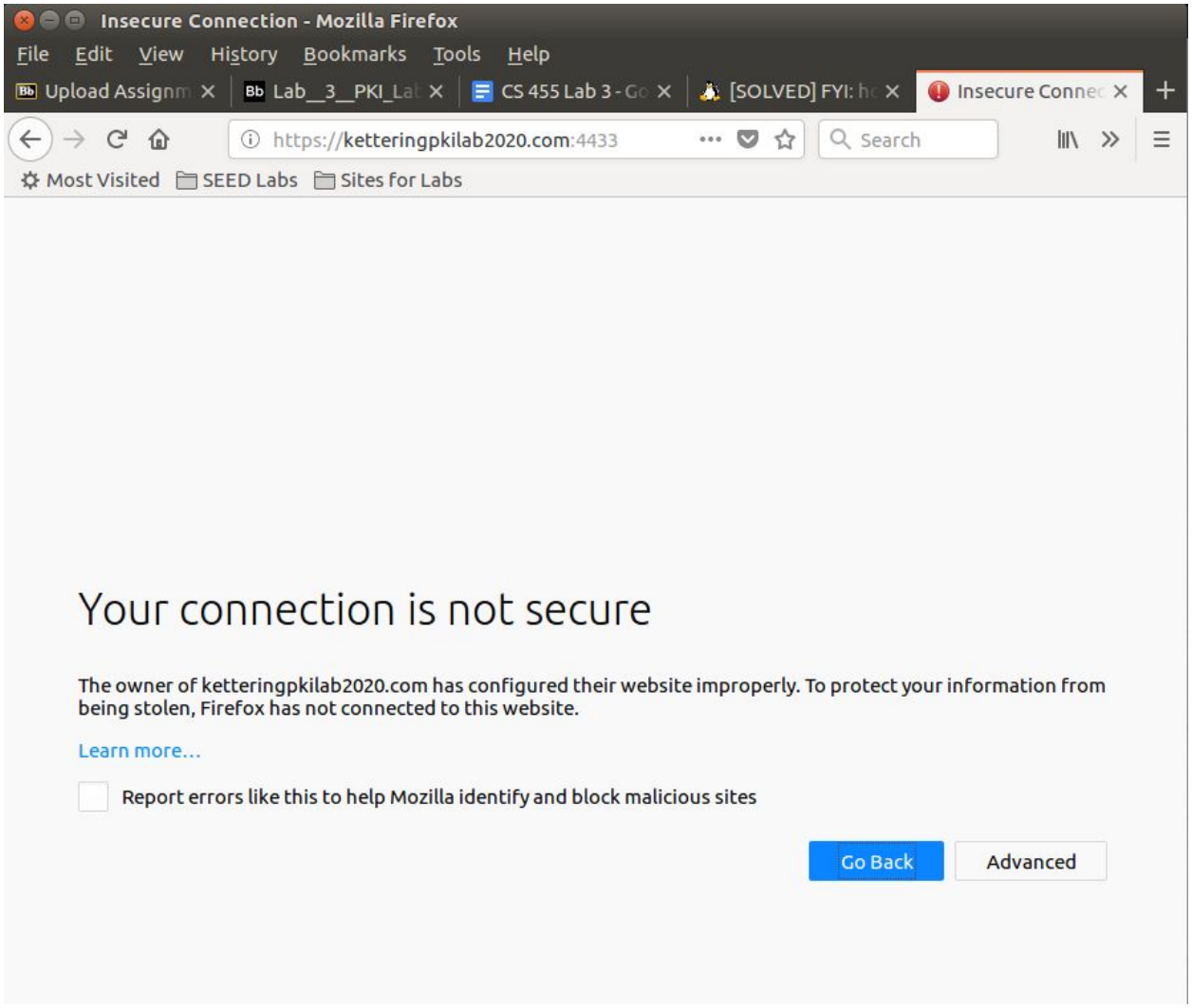
After configuring some information for the website:

```
[02/05/20]seed@VM:~/quinn3$ openssl req -new -key server.key -out server.csr -co
nfig openssl.cnf
Enter pass phrase for server.key:
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]:Michigan
Locality Name (eg, city) []:Flint
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kettering
Organizational Unit Name (eg, section) []:Security Lab
Common Name (e.g. server FQDN or YOUR name) []:KetteringPKILab2020.com
Email Address []:quin1211@kettering.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:helloButHarder
An optional company name []:.
```

Creating the first CA:

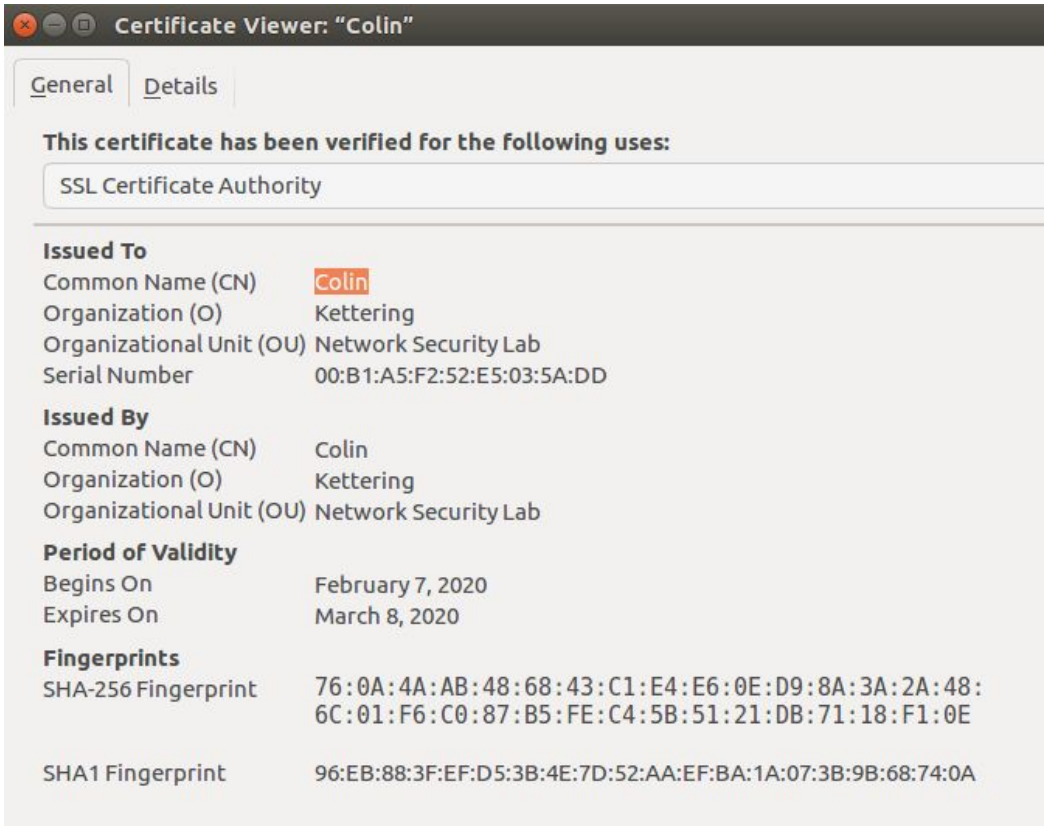
```
[02/07/20]seed@VM:~/quinn31$ openssl ca -in server.csr -out server.crt -cert ca.
crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Feb  7 21:59:53 2020 GMT
            Not After : Feb  6 21:59:53 2021 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Michigan
            organizationName          = Kettering
            organizationalUnitName    = Security Lab
            commonName                = KetteringPKILab2020.com
            emailAddress              = quin1211@kettering.edu
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                82:45:31:B3:C7:65:76:95:5E:70:B2:1A:A9:20:C4:38:34:70:13:DA
            X509v3 Authority Key Identifier:
                keyid:3A:7B:AE:09:63:1C:05:BD:7B:3B:76:2F:07:12:08:20:D9:5A:8C:6
E

Certificate is to be certified until Feb  6 21:59:53 2021 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Task 3:

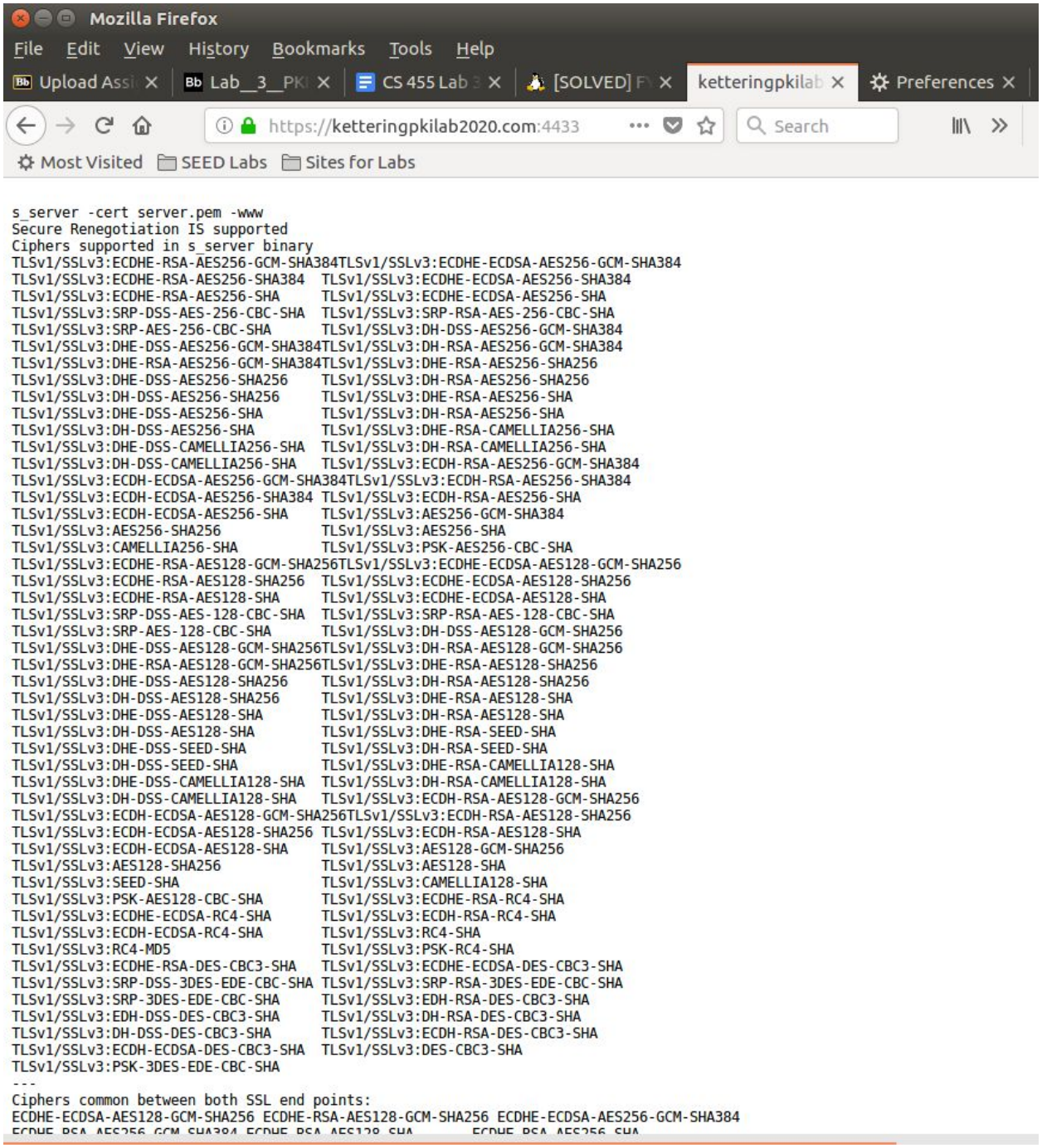


The connection is not accepted because Firefox does not accept our CA key

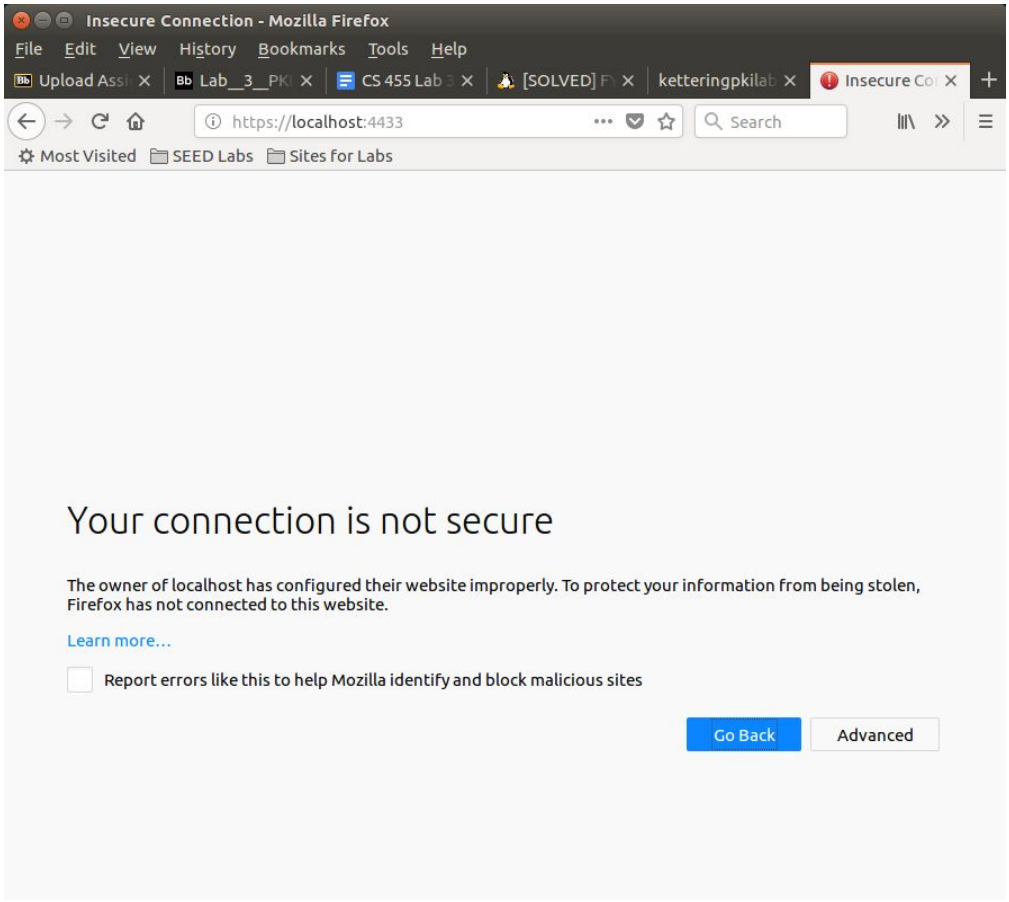
Accepting the CA key



We now have access to our site:



However when we connect through localhost:4433, it is insecure because we have only trusted the CA from KetteringPKILab2020.



Task 4:

Added last VirtualHost to 000-default.conf

```
<VirtualHost *:80>
        ServerName http://www.seedlabclickjacking.com
        DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>
<VirtualHost *:80>
        ServerName www.KetteringPKILab2020.com
        DocumentRoot /var/www/pkilab
        DirectoryIndex index.html
</VirtualHost>
```

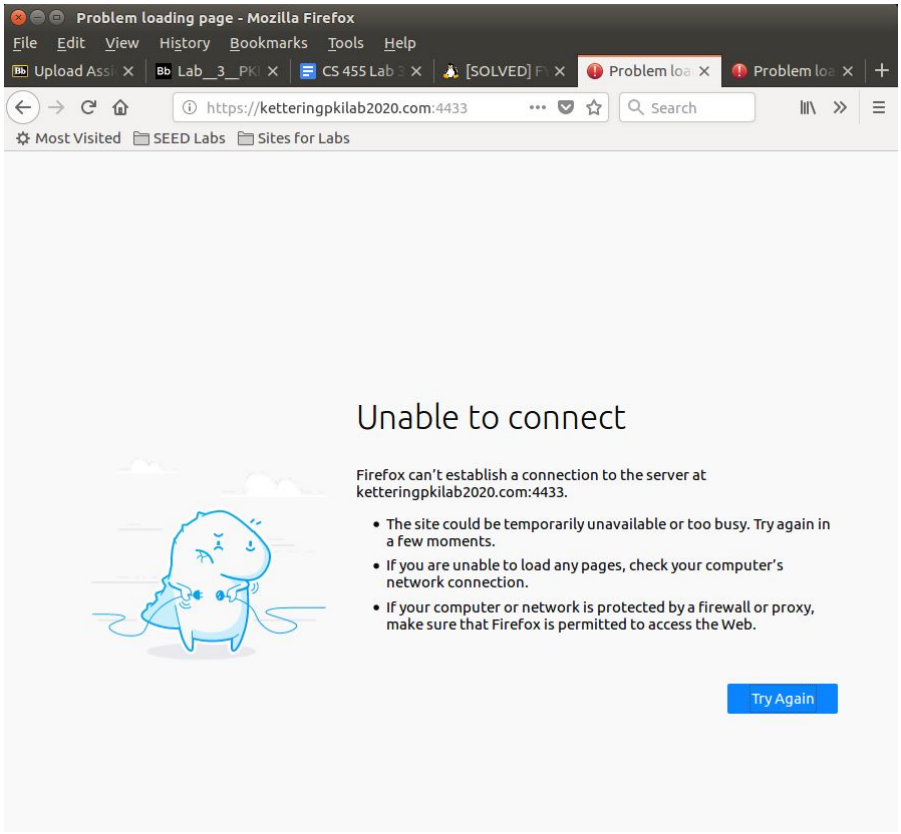
Added this to default-ssl.conf

```
        </VirtualHost>
<VirtualHost *:443>
        ServerName www.KetteringPKILab2020.com
        DocumentRoot /var/www/pkilab
        DirectoryIndex index.html
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/server.pem
        SSLCertificateKeyFile /etc/apache2/ssl/server.key
</VirtualHost>
</IfModule>
```

After enabling the Apache2 server:

```
[02/07/20]seed@VM:.../sites-available$ sudo apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress th
is message
Syntax OK
[02/07/20]seed@VM:.../sites-available$ sudo 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
[02/07/20]seed@VM:.../sites-available$ sudo a2ensite default-ssl.conf
Site default-ssl already enabled
[02/07/20]seed@VM:.../sites-available$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for www.KetteringPKILab2020.com:443 (RSA): ***
**
```

I was unable to get the site to run on the Apache2 server, as a result of restarting the service, the site returned to being unavailable without running it as a test server. Image of site shown here:


Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Upload Assi
Lab__3__PKI
CS 455 Lab 3
[SOLVED] Fi
Problem loa
Problem loa
https://ketteringpkilab2020.com:4433
Search
Most Visited
SEED Labs
Sites for Labs
Unable to connect
Firefox can't establish a connection to the server at ketteringpkilab2020.com:4433.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again