SEED Lab 1: PKI
Andrew Simon, N00695969

Task 1: Becoming a Certificate Authority (CA)

I began this lab by locating the openssl.conf file located at **/usr/lib/ssl/openssl.conf** in the prebuilt Ubuntu 16.04 VM from the SEED website. Once locating this file, I copied it into a Labs directory I made to organize all of my work for the semester

```
[01/14/24]seed@VM:~/Labs$ ls
openssl.cnf
```

I then began to create the necessary subdirectories to generate certificates with OpenSSL, as well as the empty index.txt file and serial file with a numeric string, as directed in the lab instructions.

```
[01/14/24]seed@VM:~/.../demoCA$ mkdir certs crl newcert
s
[01/14/24]seed@VM:~/.../demoCA$ ls
certs  crl  newcerts
[01/14/24]seed@VM:~/.../demoCA$ touch index.txt
[01/14/24]seed@VM:~/.../demoCA$ touch serial
[01/14/24]seed@VM:~/.../demoCA$ echo "1000" > serial
[01/14/24]seed@VM:~/.../demoCA$ ls
certs  crl  index.txt  newcerts  serial
[01/14/24]seed@VM:~/.../demoCA$ cat serial
1000
```

Once able to generate my own certificates i ran the following command to create one as directed:

Openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf

Once ran, I completed the setup information and passphrase for the key

```
[01/14/24]seed@VM:~/Labs$ openssl req -new -x509 -keyou
t ca.key -out ca.crt -config 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 wil
l be incorporated
into your certificate request.
```

Task 2: Creating a Certificate for SEEDPKILAB2020.com

Next, I generated an RSA key pair to begin creating a digital certificate for SEEDPKILab2020.com. I executed the following command as directed:

openssl genrsa -aes128 -out server.key 1024

```
[01/14/24]seed@VM:~/Labs$ openssl genrsa -aes128 -out s
erver.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.........................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[01/14/24]seed@VM:~/Labs$ ls
ca.crt  ca.key  demoCA  openssl.cnf  server.key
```

I then created a Certificate Signing Request (CSR) for SEEDPKILab2020.com using the following command as directed:

openssl req -new -key server.key -out server.csr -config openssl.cnf

```
[01/14/24]seed@VM:~/Labs$ openssl req -new -key server.
key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that wil
l be incorporated
into your certificate request.
```

Once request was made, I ran the following command as directed in order to turn the request into an X509 certificate:

Openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf

```
[01/14/24]seed@VM:~/Labs$ openssl ca -in server.csr -ou
t server.crt -cert ca.crt -keyfile ca.key -config opens
sl.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: Jan 14 17:28:58 2024 GMT
            Not After : Jan 13 17:28:58 2025 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Florida
            organizationName          = UNF
            organizationalUnitName    = Cyber
            commonName                = SEEDPKILab2020.
com
            emailAddress              = n00695969@unf.e
du
```

Task 3: Deploying Certificate in an HTTPS Web Server

To begin deploying the certificate in an HTTPS web server, I configured the /etc/hosts file by adding in the following entry, allowing my system to recognize the hostname (sudo was needed):

127.0.0.1 SEEDPKILab2020.com (Directions say 2018 but I assume this is outdated/typo)

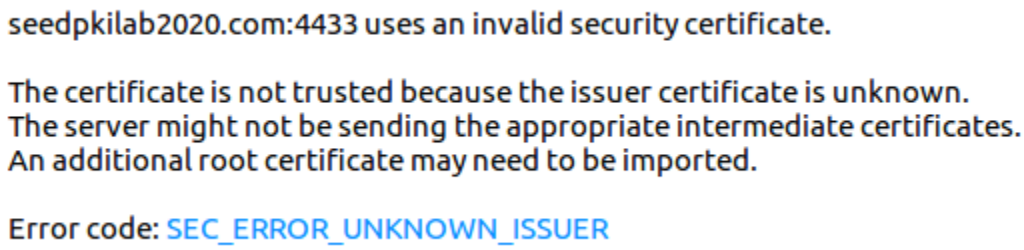
```
  GNU nano 2.5.3        File: hosts          Modified

127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1       SEEDPKILab2020.com
```

I then used the following commands to combine the secret key and certificate into one file and launch the website using server.pem:

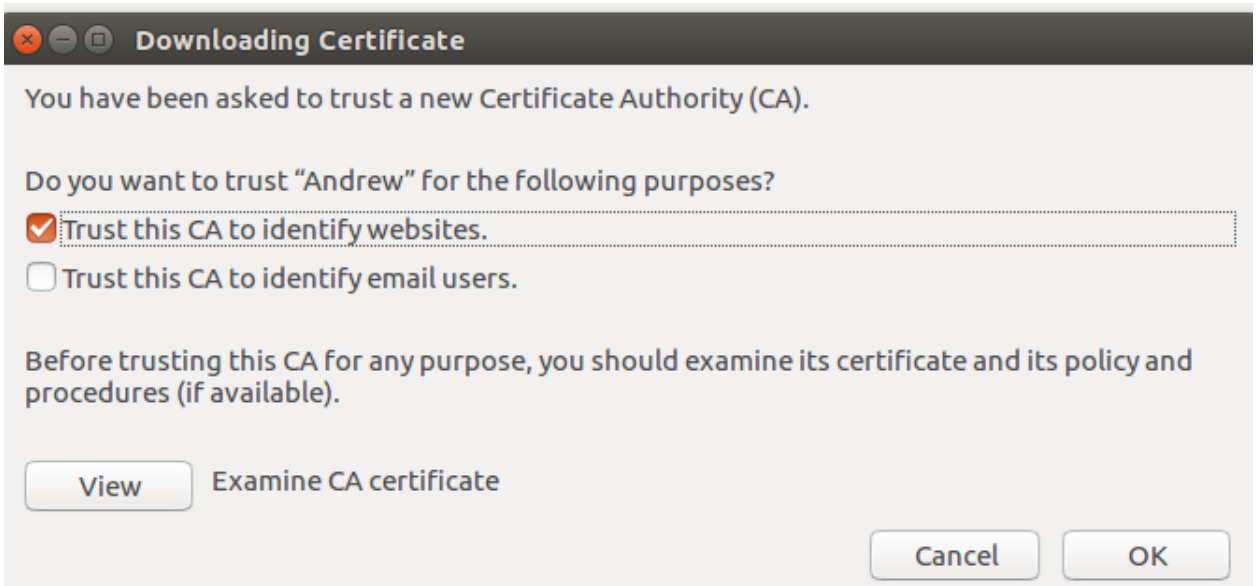
cp server.key server.pem
Cat server.crt >> server.pem
Openssl s_server -cert server.pem -www

```
[01/14/24]seed@VM:~/Labs$ cp server.key server.pem
[01/14/24]seed@VM:~/Labs$ cat server.crt >> server.pem
[01/14/24]seed@VM:~/Labs$ openssl s_server -cert server
.pem -www
```

I receive the following error message (as intended) when trying to access the site through the URL: https://SEEDPKILab2020.com:4433/



In order to have the browser (Mozilla FireFox) accept my CA certificate, I then went into my Mozilla Firefox settings (Edit > Preference > Privacy & Security > View Certificates) and imported my ca.crt file.



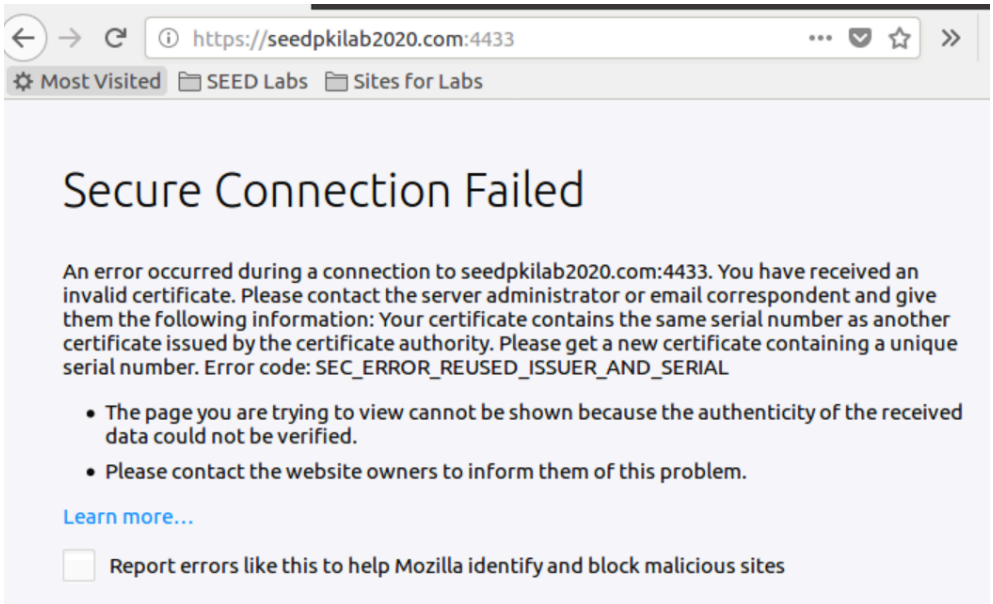
When adding one character to the file of server.pem I received the following error message

```
[01/23/24]seed@VM:~/Labs$ nano server.pem
[01/23/24]seed@VM:~/Labs$ openssl s_server -cert server
.pem -www
unable to load server certificate private key file
3071260352:error:0906D066:PEM routines:PEM_read_bio:bad
 end line:pem_lib.c:809:
```

When simply altering one character in server.pem I received the following error message

```
[01/23/24]seed@VM:~/Labs$ nano server.pem
[01/23/24]seed@VM:~/Labs$ openssl s_server -cert server
.pem -www
Enter pass phrase for server.pem:
unable to load server certificate private key file
3070805696:error:0D0680A8:asn1 encoding routines:ASN1_C
HECK_TLEN:wrong tag:tasn_dec.c:1197:
3070805696:error:0D07803A:asn1 encoding routines:ASN1_I
TEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=RSA
3070805696:error:04093004:rsa routines:OLD_RSA_PRIV_DEC
ODE:RSA lib:rsa_ameth.c:119:
3070805696:error:0D0680A8:asn1 encoding routines:ASN1_C
HECK_TLEN:wrong tag:tasn_dec.c:1197:
3070805696:error:0D07803A:asn1 encoding routines:ASN1_I
TEM_EX_D2I:nested asn1 error:tasn_dec.c:374:Type=PKCS8_
PRIV_KEY_INFO
3070805696:error:0907B00D:PEM routines:PEM_READ_BIO_PRI
VATEKEY:ASN1 lib:pem_pkey.c:141:
```

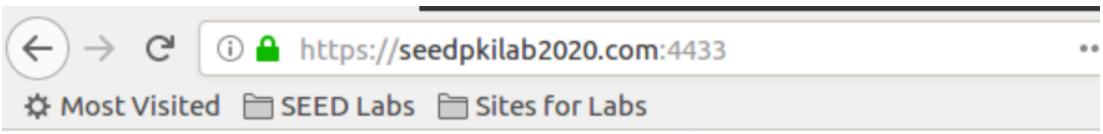
When altering another character (to get a still working request) the browser provides this error message:



Running the openssl command with the proper server.pem file provided me with the following:

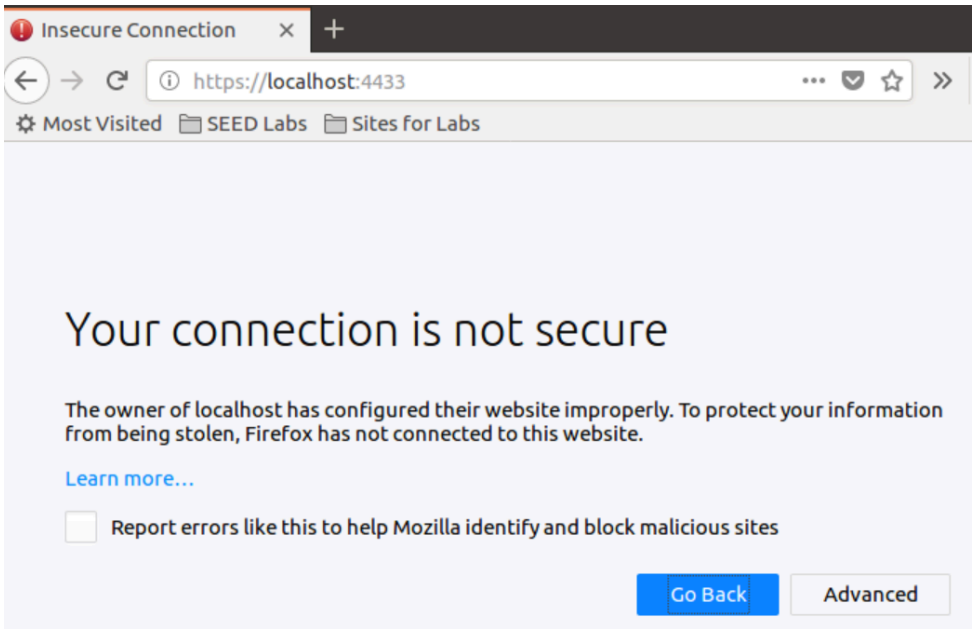
```
[01/23/24]seed@VM:~/Labs$ openssl s_server -cert server
.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```

When following the URL (https://seedpkilab2020.com:4433) in the FireFox browser, I receive the following:




```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
```

When attempting to reach the website using the URL https://localhost:4433 I receive the following:



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

In order to deploy the certificate in an Apache-based HTTPS server I added the following entry, the **default-ssl.conf** file in the **etc/apache2/sites-available** directory:

```
        <VirtualHost *:443>
                ServerName seedpkilab2020.com
                DocumentRoot /home/seed/Labs/pkilab
                DirectoryIndex index.txt

                SSLEngine On
                SSLCertificateFile /home/seed/Labs/pkil
ab/server.crt
                SSLCertificateKeyFile /home/seed/Labs/p
kilab/server.key
        </VirtualHost>
```

I followed this up with the commands provided in the directions to test the Apache configuration file, enable SSL module/site, and restart Apache.

```
[02/05/24]seed@VM:.../sites-available$ sudo apachectl c
onfigtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickja
cking] does not exist
AH00558: apache2: Could not reliably determine the serv
er's fully qualified domain name, using 127.0.1.1. Set
the 'ServerName' directive globally to suppress this me
ssage
Syntax OK
[02/05/24]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
```

```
[02/05/24]seed@VM:.../sites-available$ sudo a2ensite de
fault-ssl
Site default-ssl already enabled
[02/05/24]seed@VM:.../sites-available$ sudo service apa
che2 restart
Enter passphrase for SSL/TLS keys for seedpkilab2020.co
m:443 (RSA): ******
```

I received the following error when attempting to access the web server: