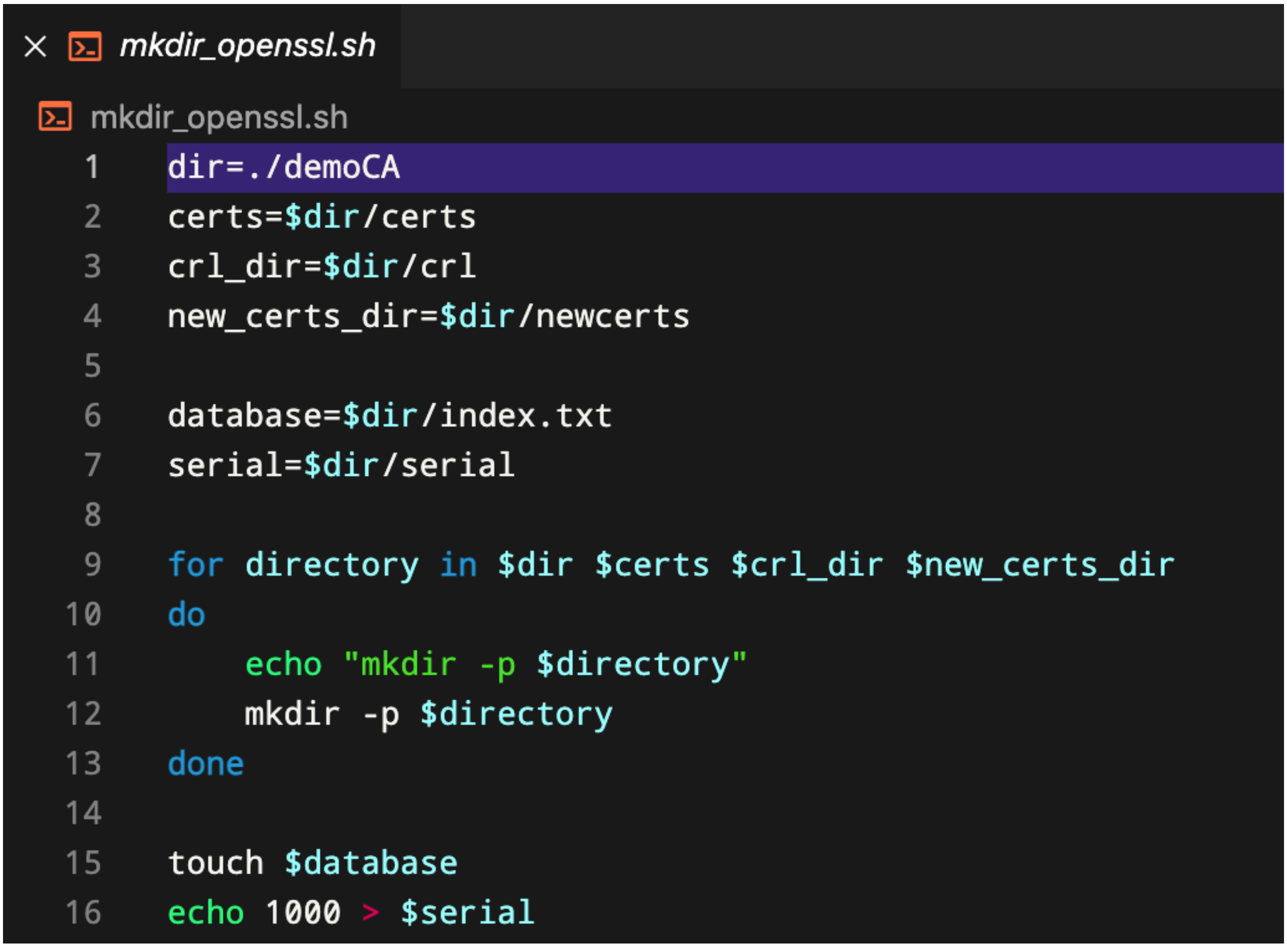
Lab4 Report

2021 02 28 00:22

task1
# create root CA

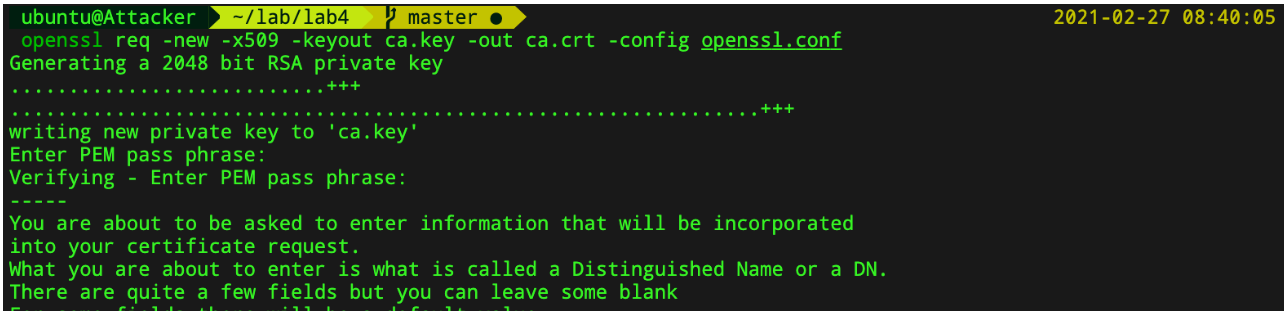
a bash script is created to automate the process:



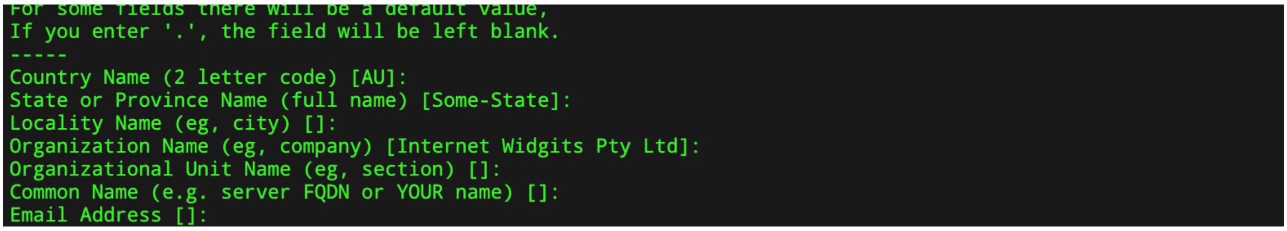
mkdir_openssl.sh

```
dir=./demoCA
certs=$dir/certs
crl_dir=$dir/crl
new_certs_dir=$dir/newcerts

database=$dir/index.txt
serial=$dir/serial

for directory in $dir $certs $crl_dir $new_certs_dir
do
    echo "mkdir -p $directory"
    mkdir -p $directory
done

touch $database
echo 1000 > $serial
```

# generate self-signed
openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.conf
alex

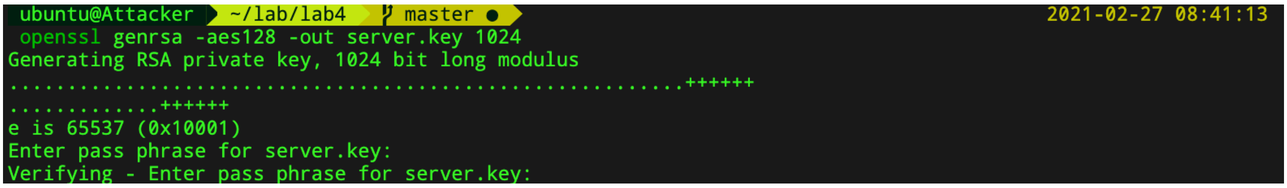


```
 ubuntu@Attacker  ~/lab/lab4  master ●                                          2021-02-27 08:40:05
 openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.conf
Generating a 2048 bit RSA private key
...........................+++
..................................................................+++
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
```



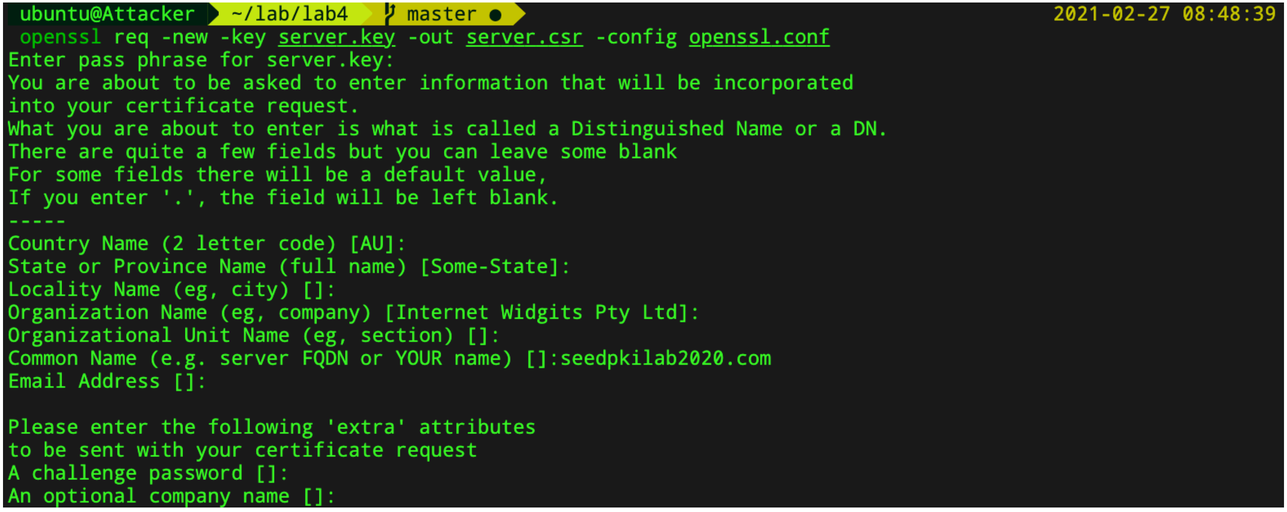
```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

task2
# create rsa keys
openssl genrsa -aes128 -out server.key 1024
alex



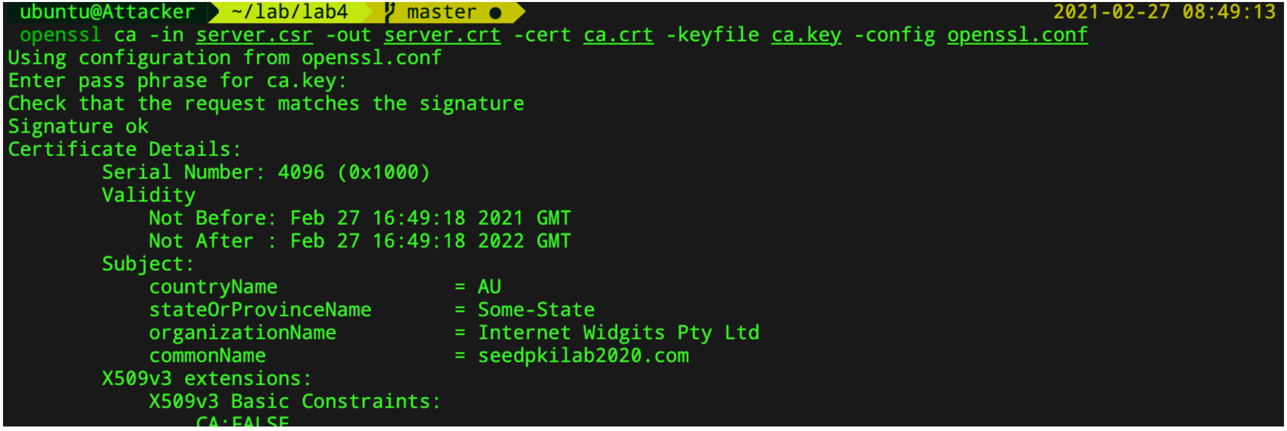
```
 ubuntu@Attacker  ~/lab/lab4  master ●                                2021-02-27 08:41:13
 openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
..........................................................++++++
.............++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

# create csr
openssl req -new -key server.key -out server.csr -config openssl.conf
seedpkilab2020.com

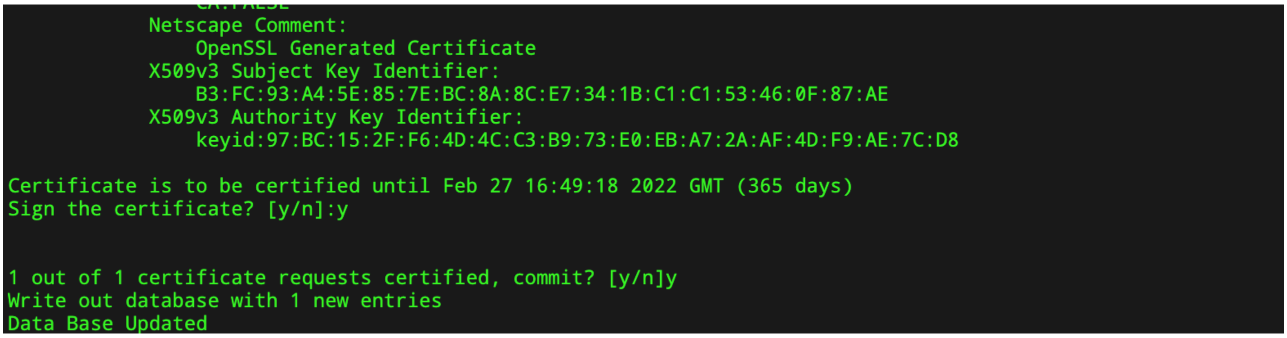


```
 ubuntu@Attacker  ~/lab/lab4  master ●                                2021-02-27 08:48:39
 openssl req -new -key server.key -out server.csr -config openssl.conf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
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]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:seedpkilab2020.com
Email Address []:

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

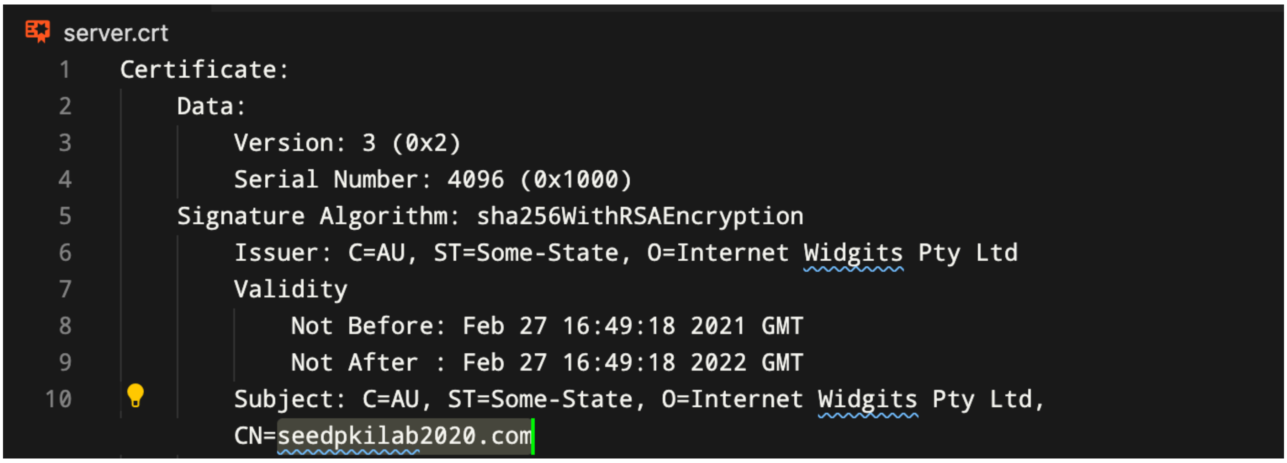
# sign cert
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.conf



```
 ubuntu@Attacker  ~/lab/lab4  master ●                                2021-02-27 08:49:13
 openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.conf
Using configuration from openssl.conf
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 27 16:49:18 2021 GMT
            Not After : Feb 27 16:49:18 2022 GMT
        Subject:
            countryName               = AU
            stateOrProvinceName       = Some-State
            organizationName          = Internet Widgits Pty Ltd
            commonName                = seedpkilab2020.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```



```
            CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                B3:FC:93:A4:5E:85:7E:BC:8A:8C:E7:34:1B:C1:C1:53:46:0F:87:AE
            X509v3 Authority Key Identifier:
                keyid:97:BC:15:2F:F6:4D:4C:C3:B9:73:E0:EB:A7:2A:AF:4D:F9:AE:7C:D8

Certificate is to be certified until Feb 27 16:49:18 2022 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
```

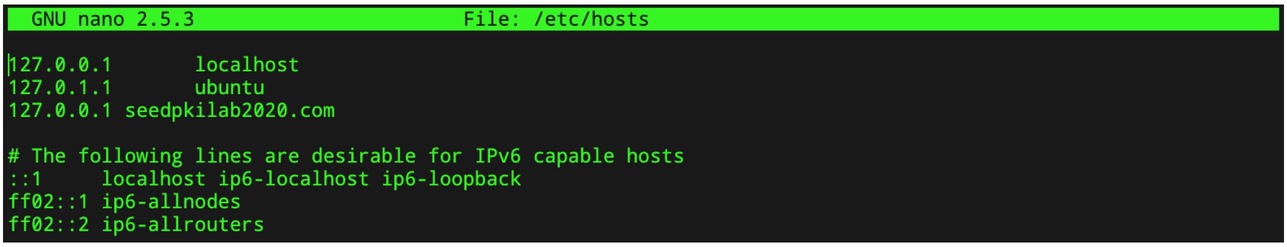


server.crt

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Validity
            Not Before: Feb 27 16:49:18 2021 GMT
            Not After : Feb 27 16:49:18 2022 GMT
        Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd,
        CN=seedpkilab2020.com
```

checking the signed server.cert
confirms that Common Name is indeed seedpkilab2020.com

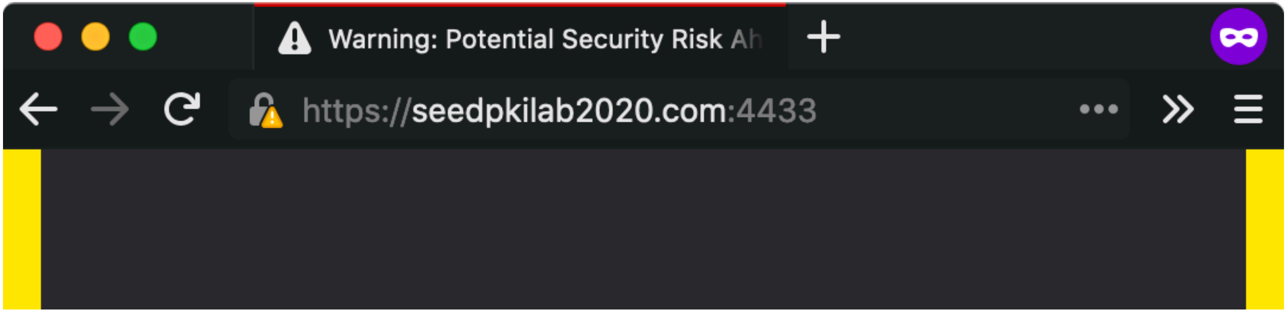
task3
sudo nano /etc/hosts

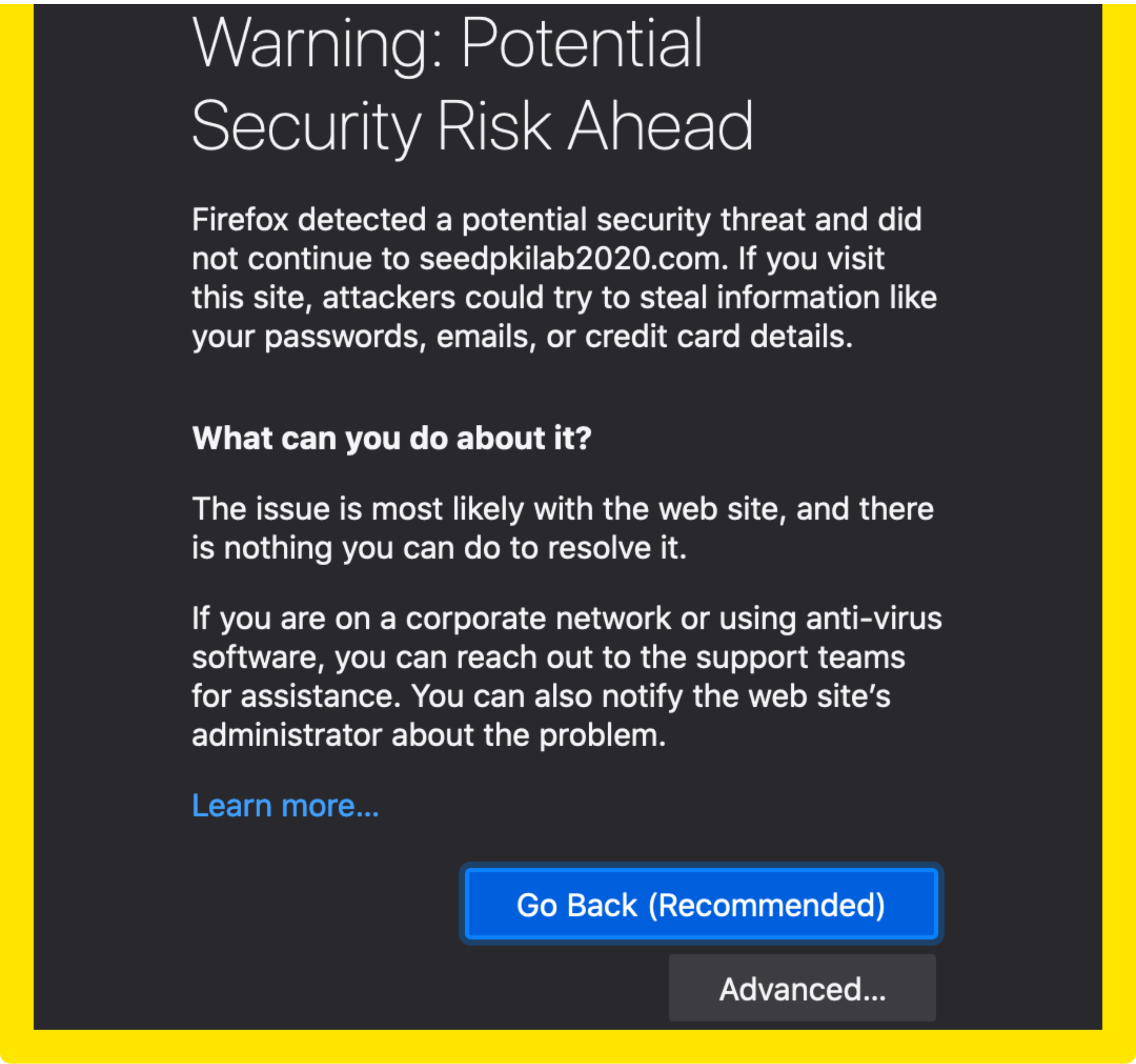


```
  GNU nano 2.5.3                     File: /etc/hosts

127.0.0.1       localhost
127.0.1.1       ubuntu
127.0.0.1 seedpkilab2020.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
cp server.key server.pem
cat server.crt >> server.pem

openssl s_server -cert server.pem -www # default listen at
4433
```

the following screen is oberved


Warning: Potential Security Risk Ah
https://seedpkilab2020.com:4433



Warning: Potential Security Risk Ahead

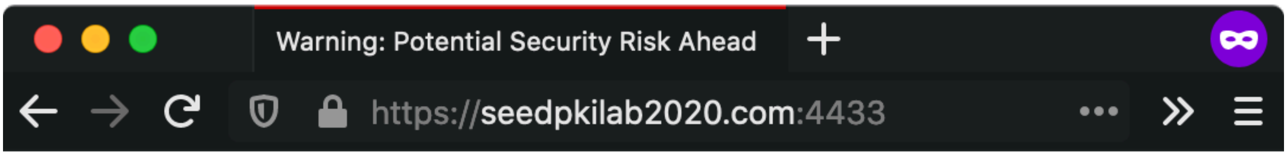
Firefox detected a potential security threat and did not continue to seedpkilab2020.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

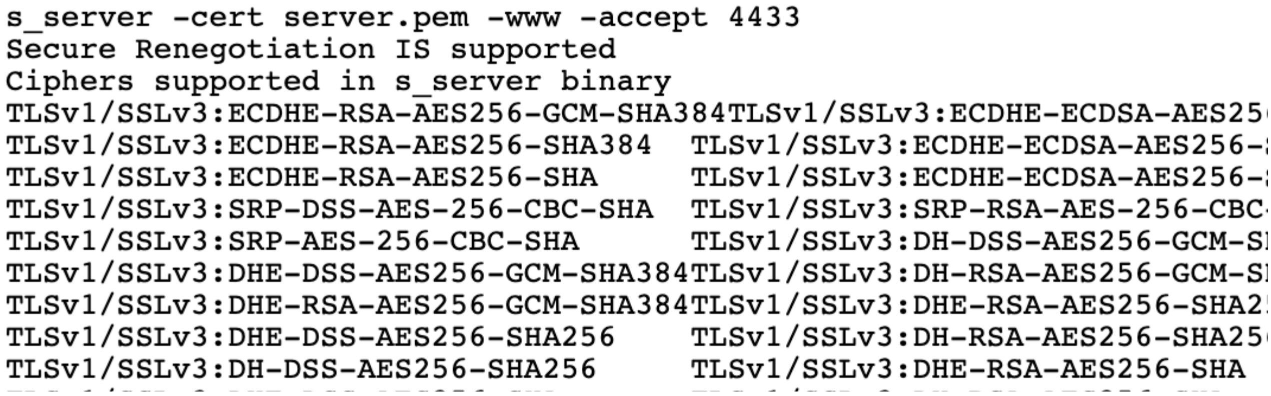
What can you do about it?

The issue is most likely with the web site, and there is nothing you can do to resolve it.

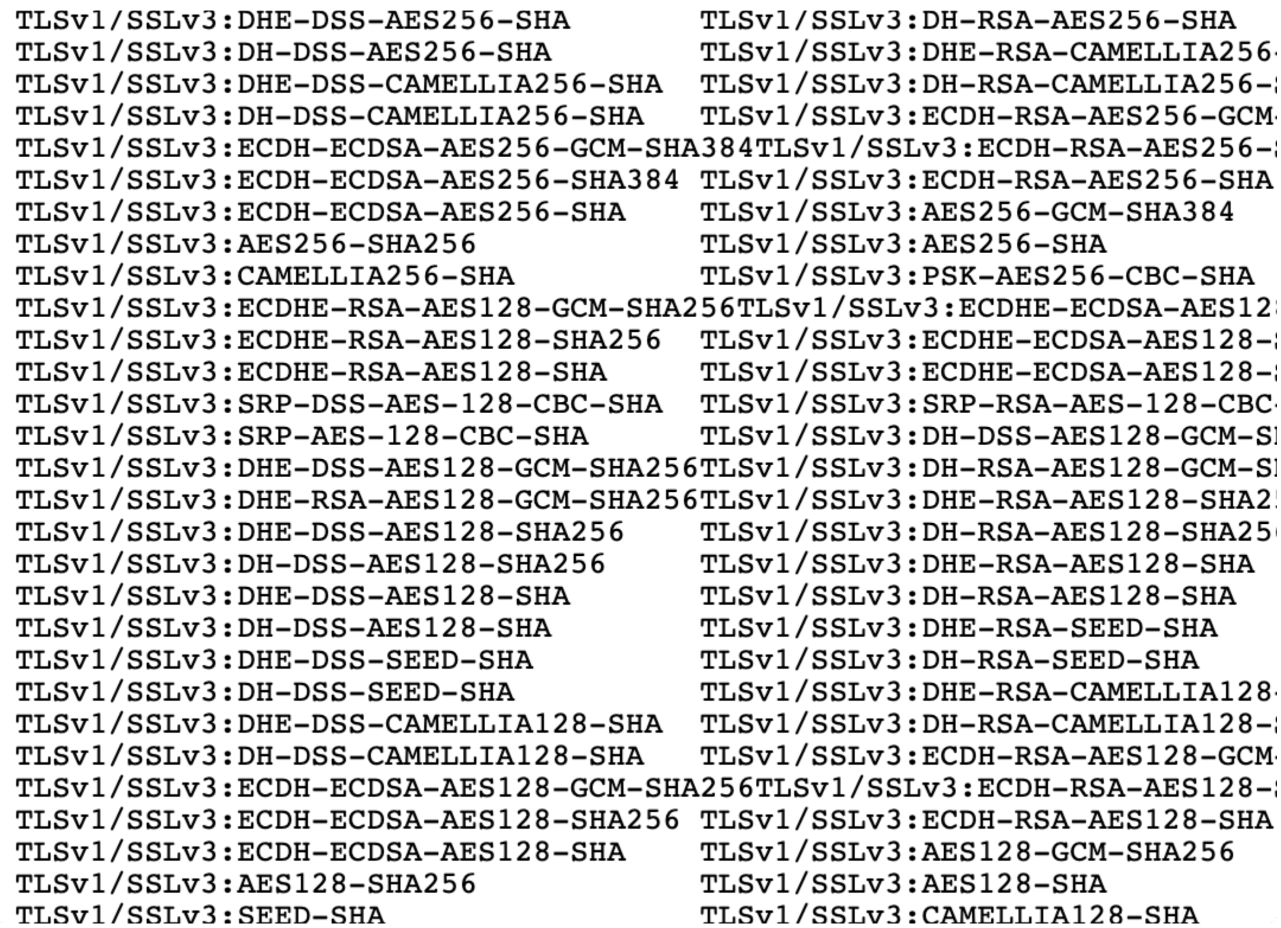
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.

after importing ca.crt into firefox, reloading the page gives the following


Warning: Potential Security Risk Ahead
https://seedpkilab2020.com:4433

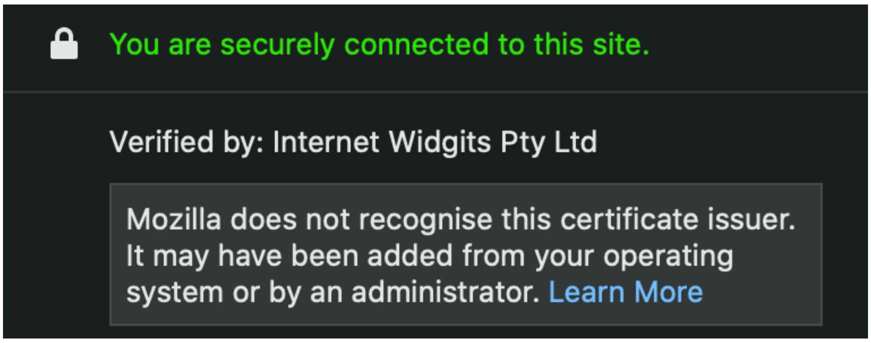


```
s_server -cert server.pem -www -accept 4433
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES25
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-S
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-S
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA2
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA25
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
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-
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-AES12
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-S
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-S
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA2
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA25
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
```

the page loads properly, using https, with the lock icon showing that encryption is working (secure connection), despite the cert issuer (Internet Widgits Pty Ltd) is not recognised by the browser

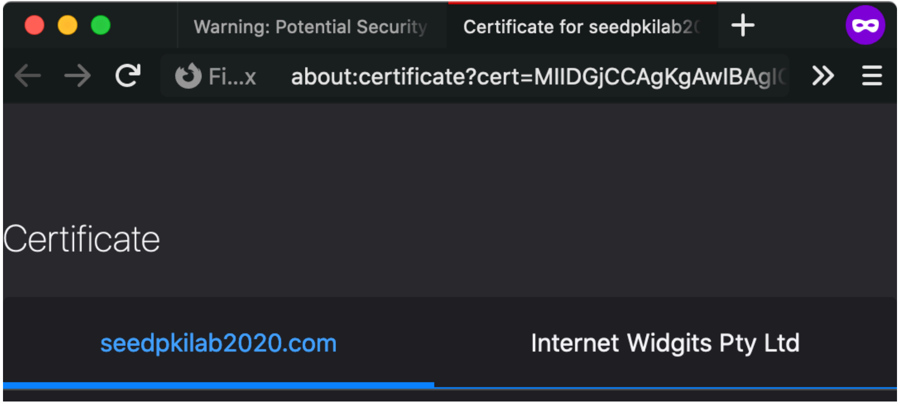


You are securely connected to this site.

Verified by: Internet Widgits Pty Ltd

Mozilla does not recognise this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

viewing the certificate in firefox:

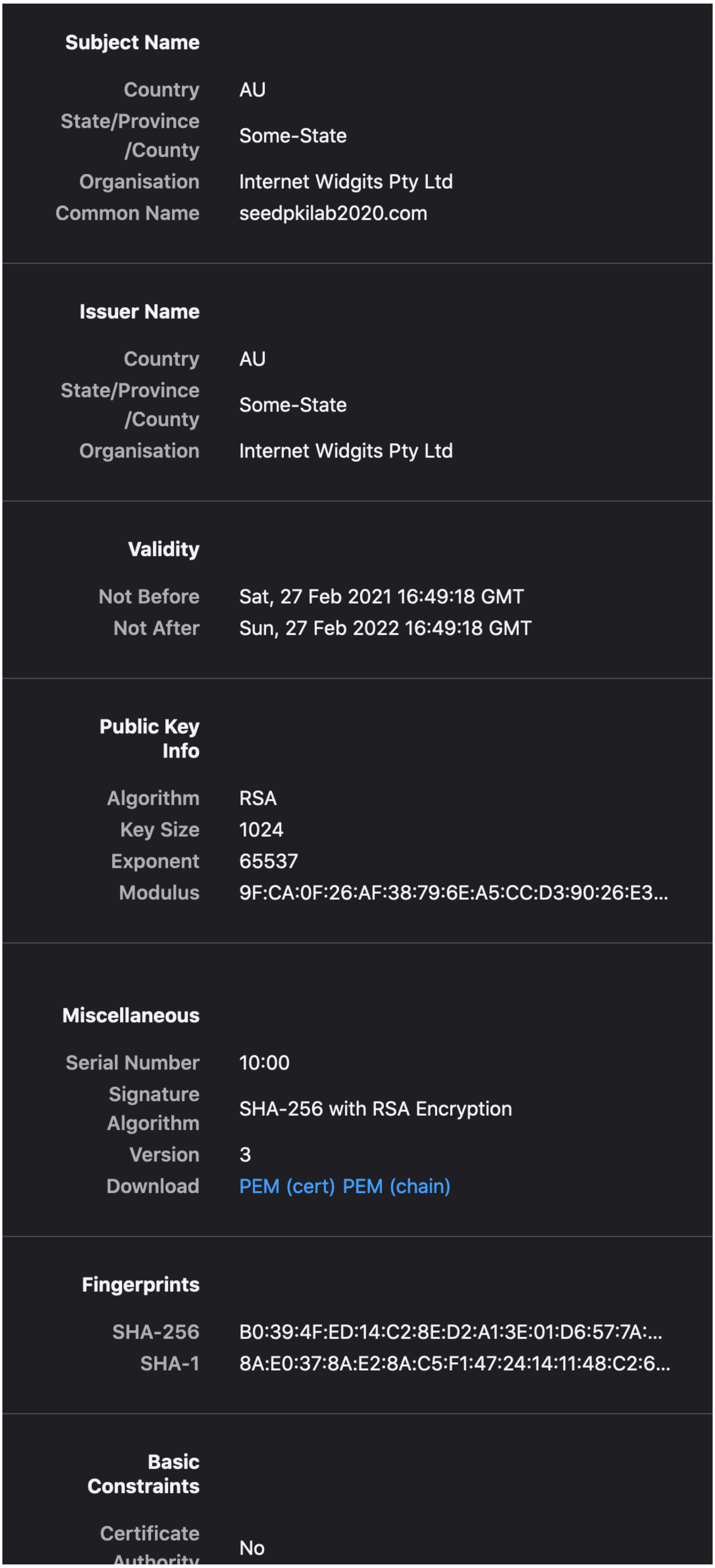


Warning: Potential Security
Certificate for seedpkilab2(
Fi...x
about:certificate?cert=MIIDGjCCAgKgAwIBAgI(

Certificate

seedpkilab2020.com

Internet Widgits Pty Ltd



Subject Name

Country	AU
State/Province /County	Some-State
Organisation	Internet Widgits Pty Ltd
Common Name	seedpkilab2020.com

Issuer Name

Country	AU
State/Province /County	Some-State
Organisation	Internet Widgits Pty Ltd

Validity

Not Before	Sat, 27 Feb 2021 16:49:18 GMT
Not After	Sun, 27 Feb 2022 16:49:18 GMT

Public Key Info

Algorithm	RSA
Key Size	1024
Exponent	65537
Modulus	9F:CA:0F:26:AF:38:79:6E:A5:CC:D3:90:26:E3...

Miscellaneous

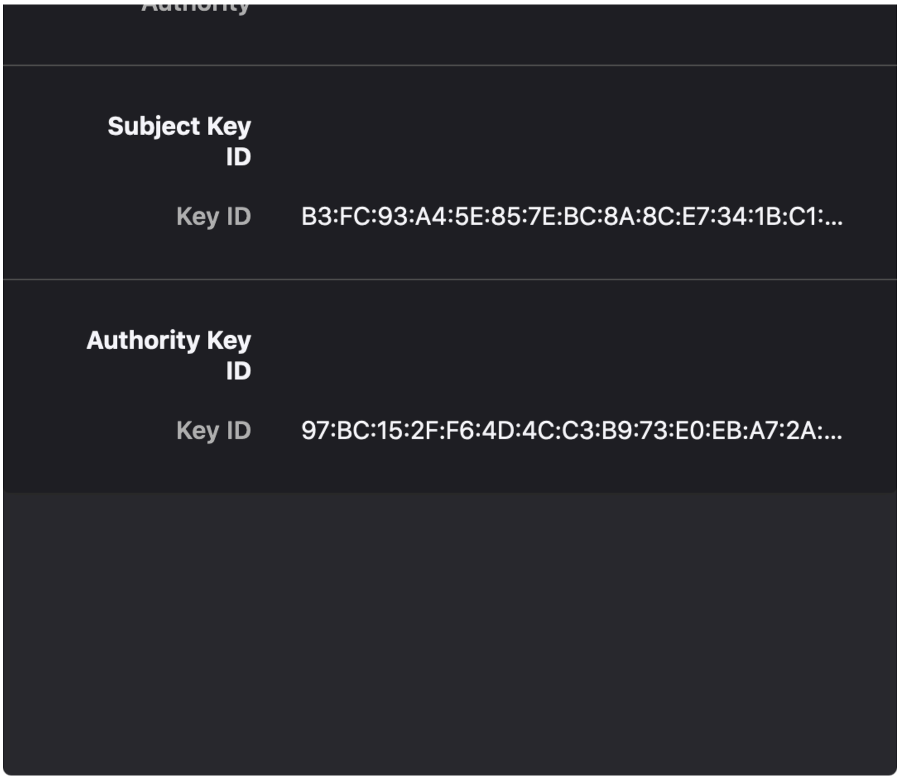
Serial Number	10:00
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	B0:39:4F:ED:14:C2:8E:D2:A1:3E:01:D6:57:7A:...
SHA-1	8A:E0:37:8A:E2:8A:C5:F1:47:24:14:11:48:C2:6...

Basic Constraints

Certificate Authority	No



Authority

Subject Key ID

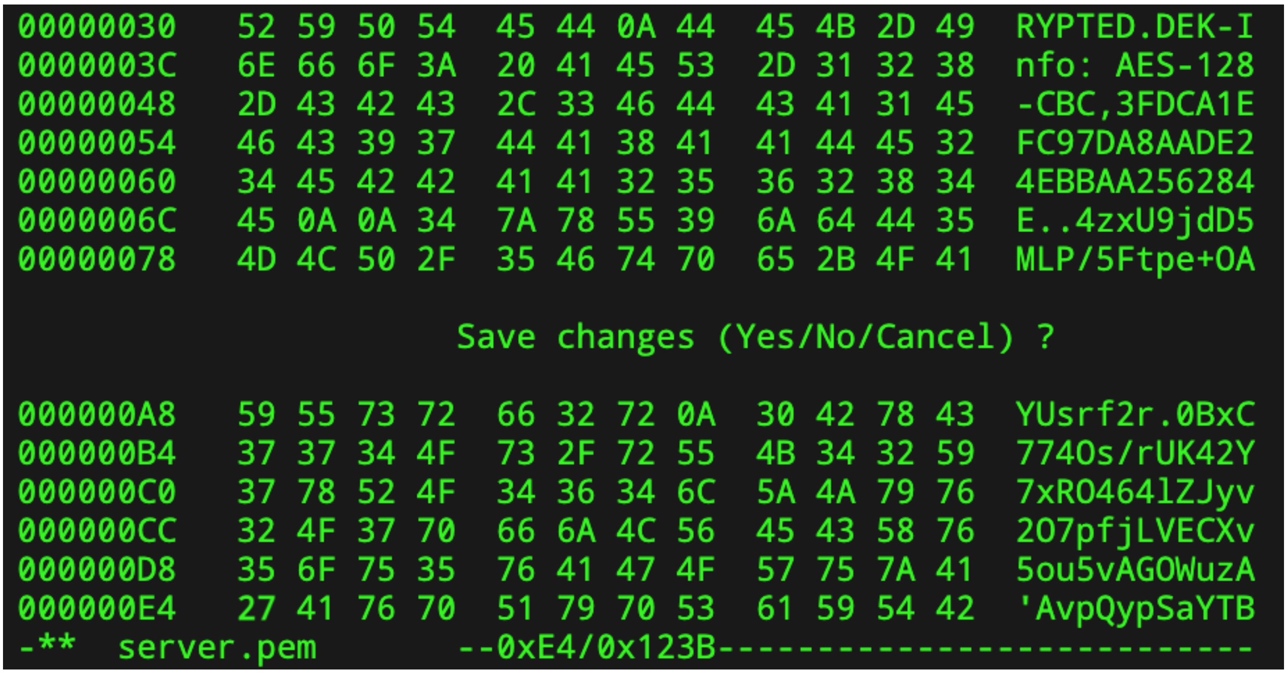
Key ID B3:FC:93:A4:5E:85:7E:BC:8A:8C:E7:34:1B:C1:...

Authority Key ID

Key ID 97:BC:15:2F:F6:4D:4C:C3:B9:73:E0:EB:A7:2A:...

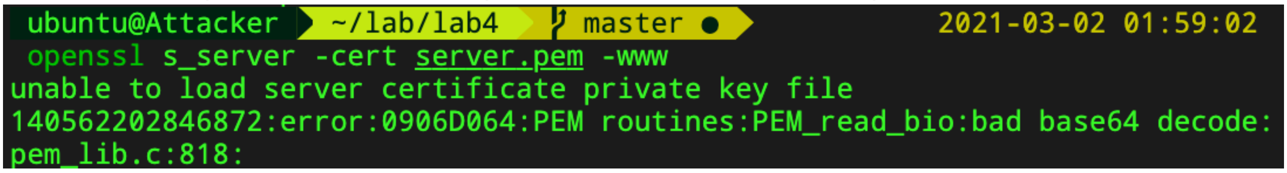
the content match that of server.crt screenshot

change 1 byte
using hexedit
hexedit server.pem



```
00000030   52 59 50 54  45 44 0A 44  45 4B 2D 49  RYPTED.DEK-I
0000003C   6E 66 6F 3A  20 41 45 53  2D 31 32 38  nfo: AES-128
00000048   2D 43 42 43  2C 33 46 44  43 41 31 45  -CBC,3FDCA1E
00000054   46 43 39 37  44 41 38 41  41 44 45 32  FC97DA8AADE2
00000060   34 45 42 42  41 41 32 35  36 32 38 34  4EBBAA256284
0000006C   45 0A 0A 34  7A 78 55 39  6A 64 44 35  E..4zxU9jdD5
00000078   4D 4C 50 2F  35 46 74 70  65 2B 4F 41  MLP/5Ftpe+OA

                    Save changes (Yes/No/Cancel) ?

000000A8   59 55 73 72  66 32 72 0A  30 42 78 43  YUsrf2r.0BxC
000000B4   37 37 34 4F  73 2F 72 55  4B 34 32 59  774Os/rUK42Y
000000C0   37 78 52 4F  34 36 34 6C  5A 4A 79 76  7xRO464lZJyv
000000CC   32 4F 37 70  66 6A 4C 56  45 43 58 76  2O7pfjLVECXv
000000D8   35 6F 75 35  76 41 47 4F  57 75 7A 41  5ou5vAGOWuzA
000000E4   27 41 76 70  51 79 70 53  61 59 54 42  'AvpQypSaYTB
-**  server.pem       --0xE4/0x123B----------------------------
```

restarting the server gives the following error

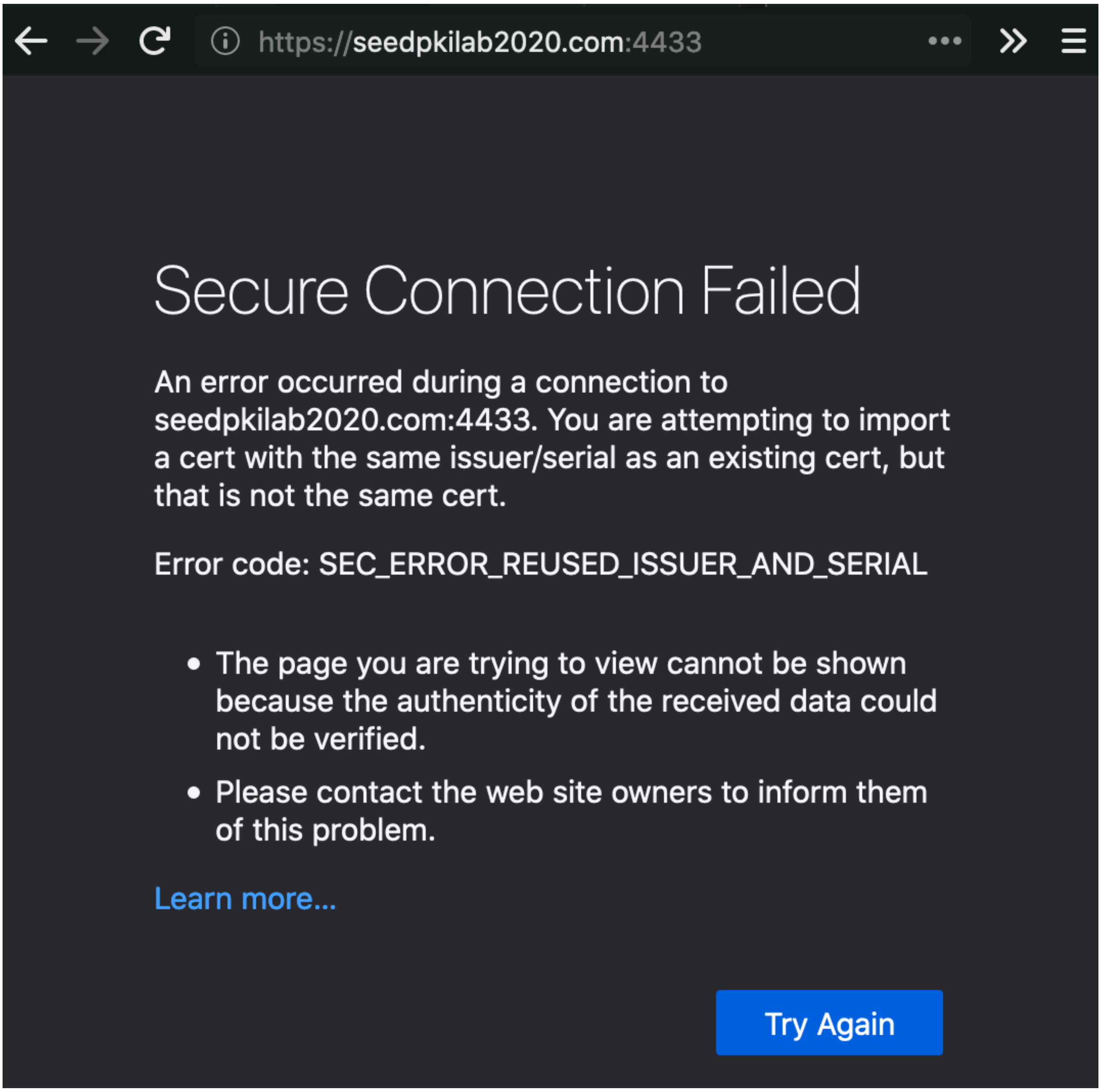


```
 ubuntu@Attacker  ~/lab/lab4  master ●                2021-03-02 01:59:02
 openssl s_server -cert server.pem -www
unable to load server certificate private key file
140562202846872:error:0906D064:PEM routines:PEM_read_bio:bad base64 decode:
pem_lib.c:818:
```

this shows that the edit is made at a crucial place in the

file, corrupting the whole certificate
through trial and error, modifying a single bit near the end of the certificate still allows the server to run

upon connecting from browser, the following screen is encountered



Secure Connection Failed

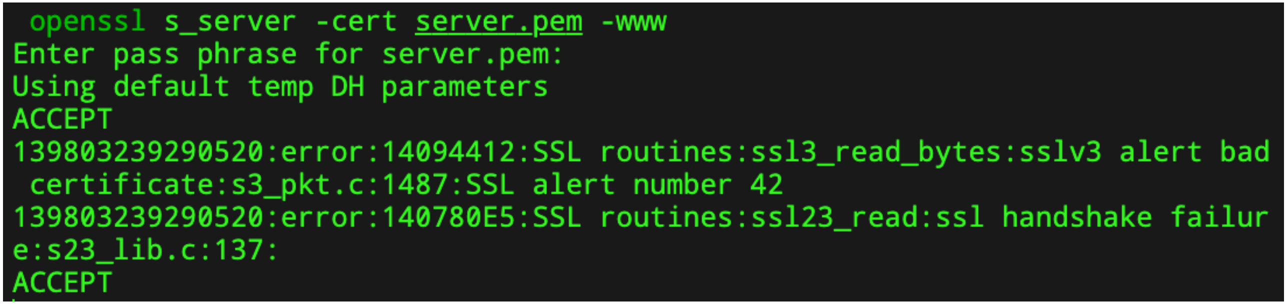
An error occurred during a connection to seedpkilab2020.com:4433. You are attempting to import a cert with the same issuer/serial as an existing cert, but that is not the same cert.

Error code: SEC_ERROR_REUSED_ISSUER_AND_SERIAL

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the web site owners to inform them of this problem.

Learn more…

with the terminal giving the error



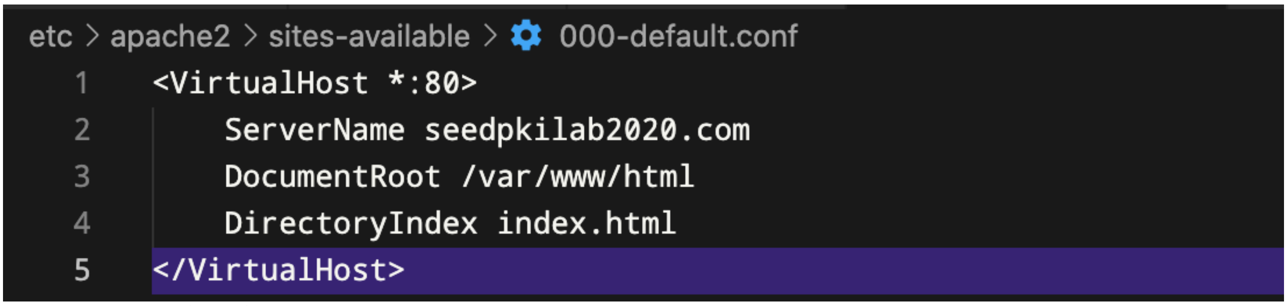
```
 openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
139803239290520:error:14094412:SSL routines:ssl3_read_bytes:sslv3 alert bad
 certificate:s3_pkt.c:1487:SSL alert number 42
139803239290520:error:140780E5:SSL routines:ssl23_read:ssl handshake failur
e:s23_lib.c:137:
ACCEPT
```

this shows that there is an error in the certificate file, that is caused by only changing 1 byte of the file. the result is inability to handshake properly to establish secure connection

tastk4

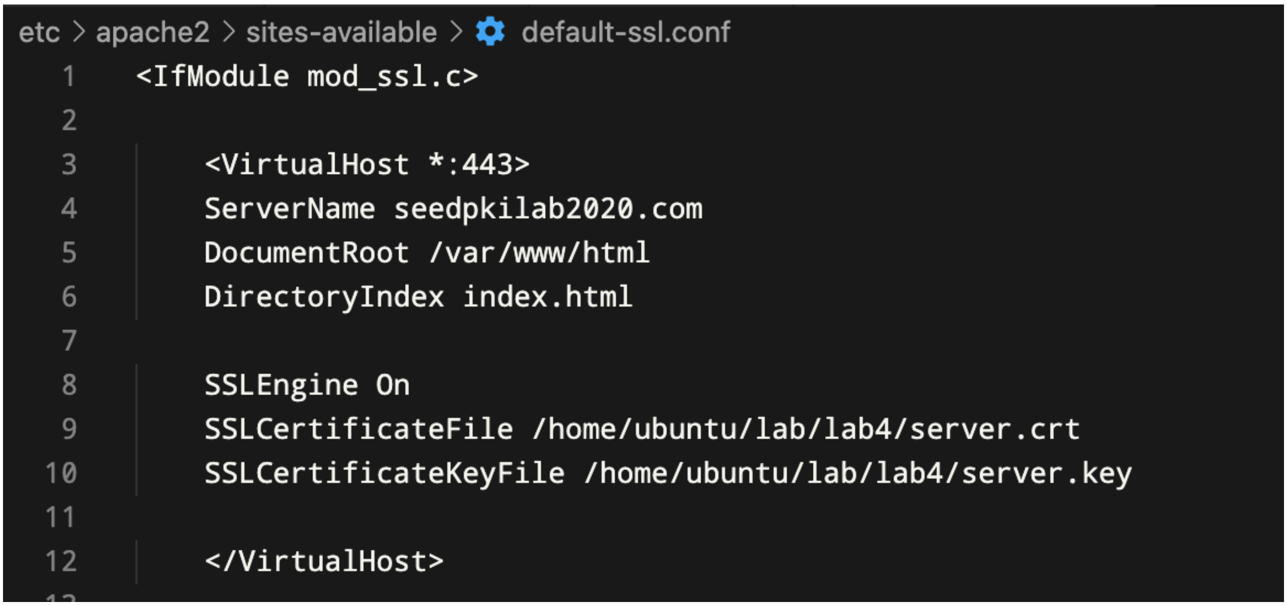
as the vm used is not standard SEED VM, and doesnt come with apache
install apache with the following command

```
# install apache2
sudo apt install apache2 -y

# add virtual hosts
```



```
<VirtualHost *:80>
    ServerName seedpkilab2020.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html
</VirtualHost>
```

in http (80) website, server name is changed to seedpkilab2020.com
the document root is changed to /var/www/html, to serve the default apache index.html



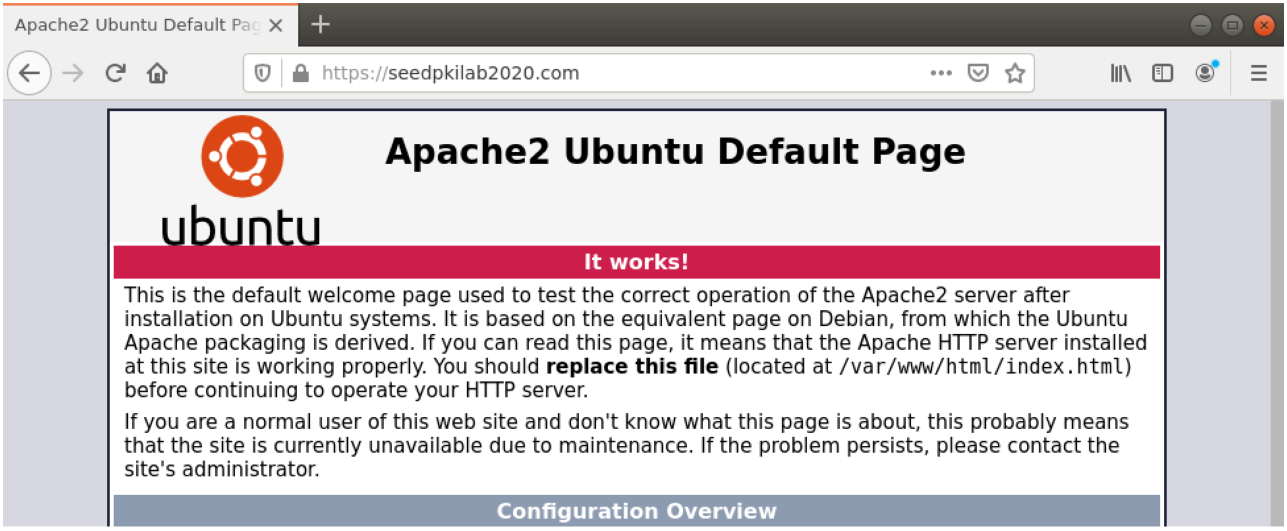
```
<IfModule mod_ssl.c>

    <VirtualHost *:443>
    ServerName seedpkilab2020.com
    DocumentRoot /var/www/html
    DirectoryIndex index.html

    SSLEngine On
    SSLCertificateFile /home/ubuntu/lab/lab4/server.crt
    SSLCertificateKeyFile /home/ubuntu/lab/lab4/server.key

    </VirtualHost>
```

in http (443) website, server name is changed to seedpkilab2020.com
the document root is changed to /var/www/html, to serve the

default apache index.html
SSLCertificateFile now points to server's certificate, located at /home/ubuntu/lab/lab4/server.crt
SSLCertificateKeyFile now points to server's private key file, located at /home/ubuntu/lab/lab4/server.key

to test :80 and :443, it requires the local host to visit using a browser

i install a desktop server and envirnoment and launched a local instance of firefox to view the page



Apache2 Ubuntu Default Page

It works!

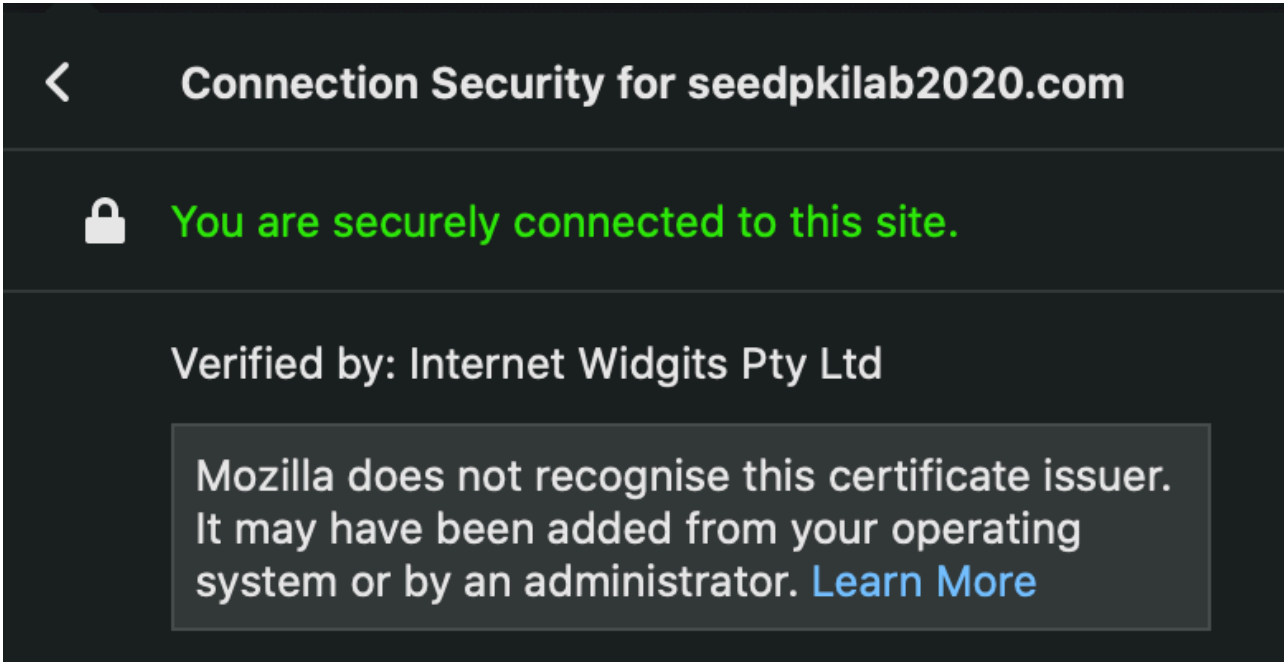
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

notice the lock icon, it shows that SSL encryption is working and the https connection is secured

this is further confirmed by clicking into the lock icon and sees that the cert is signed by the root CA created earlier



Connection Security for seedpkilab2020.com

You are securely connected to this site.

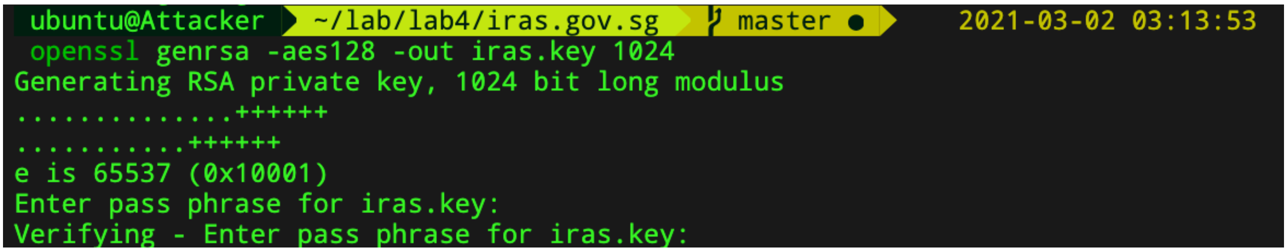
Verified by: Internet Widgits Pty Ltd

Mozilla does not recognise this certificate issuer. It may have been added from your operating system or by an administrator. Learn More

task5
https://www.iras.gov.sg is selected for this task
the website's index.html is saved using Firefox's SingleFile extension, to contain all downloaded images and other web assets

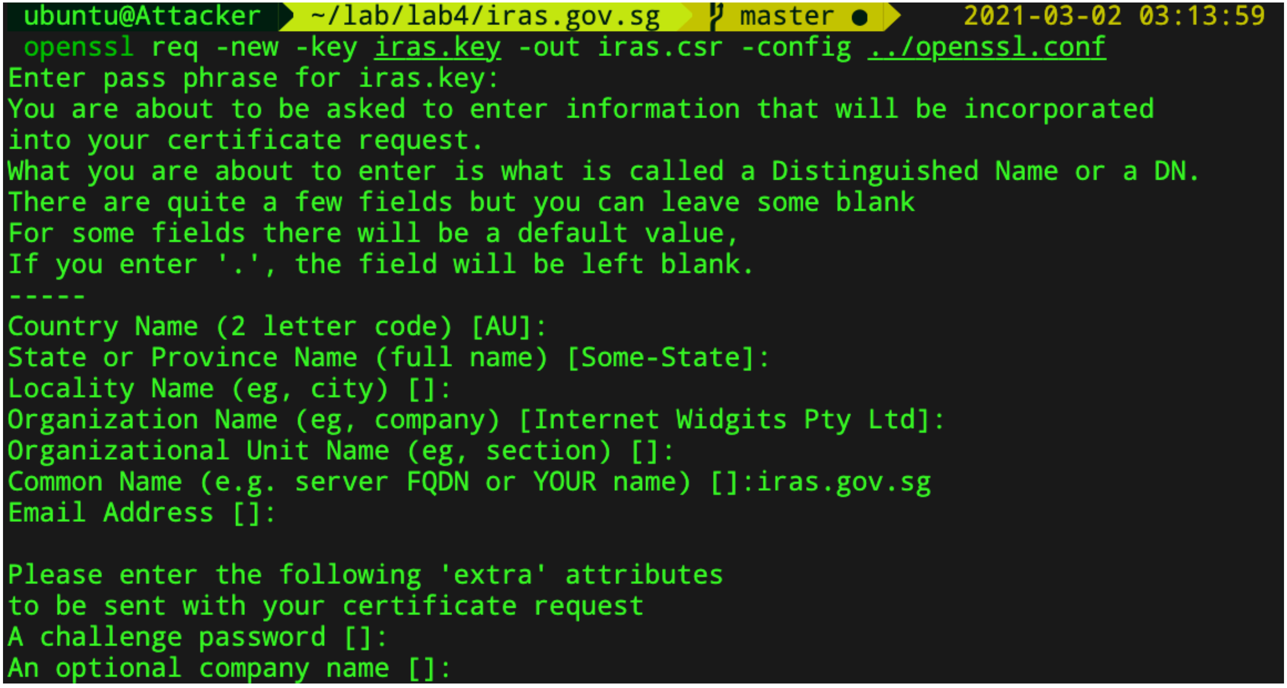
following the same tasks as previous:

```
# create rsa keys
openssl genrsa -aes128 -out iras.key 1024
iras
```



```
ubuntu@Attacker  ~/lab/lab4/iras.gov.sg   master ●        2021-03-02 03:13:53
 openssl genrsa -aes128 -out iras.key 1024
Generating RSA private key, 1024 bit long modulus
..............++++++
...........++++++
e is 65537 (0x10001)
Enter pass phrase for iras.key:
Verifying - Enter pass phrase for iras.key:
```

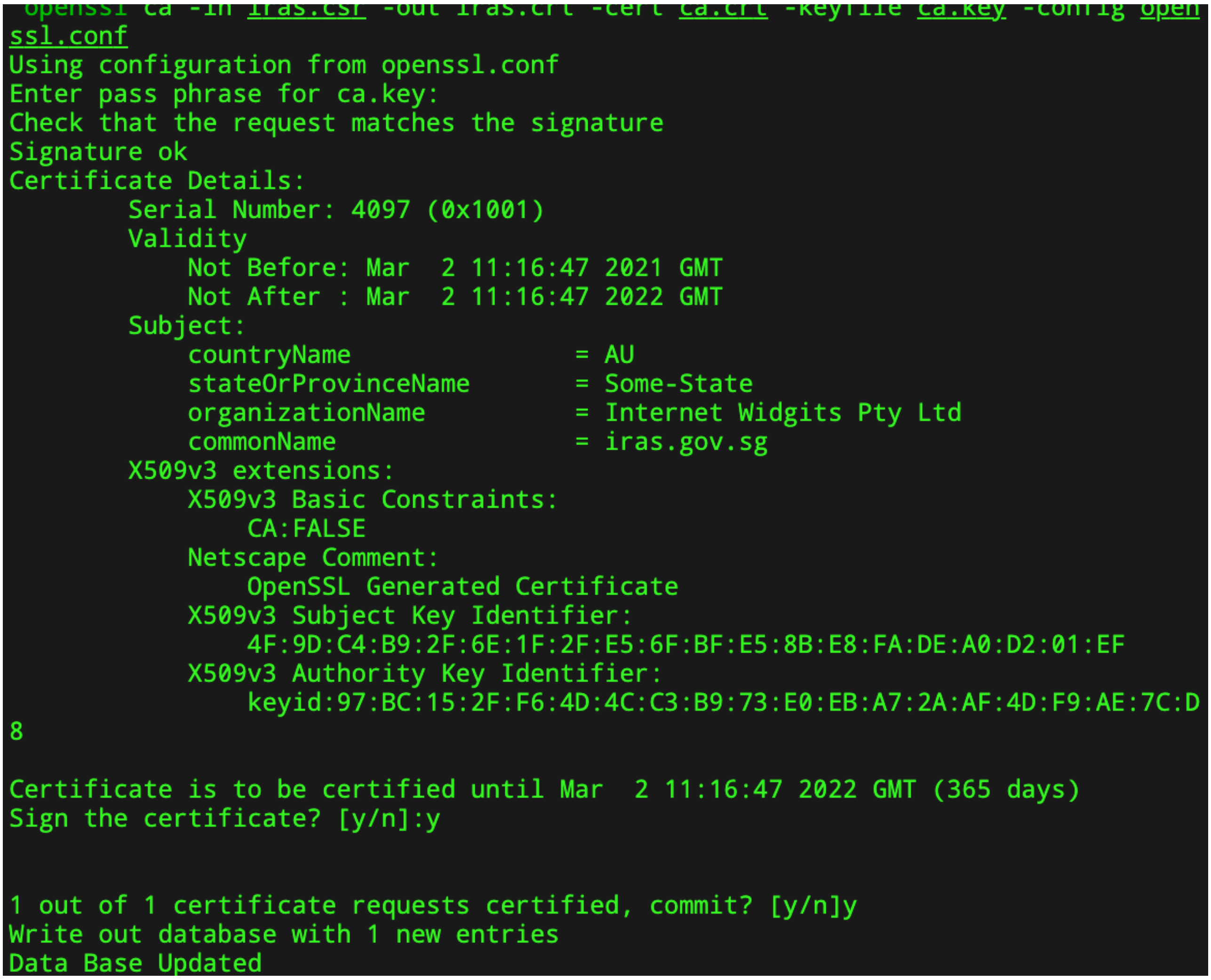
```
# create csr
openssl req -new -key iras.key -out iras.csr -config openssl.conf
iras.gov.sg
```



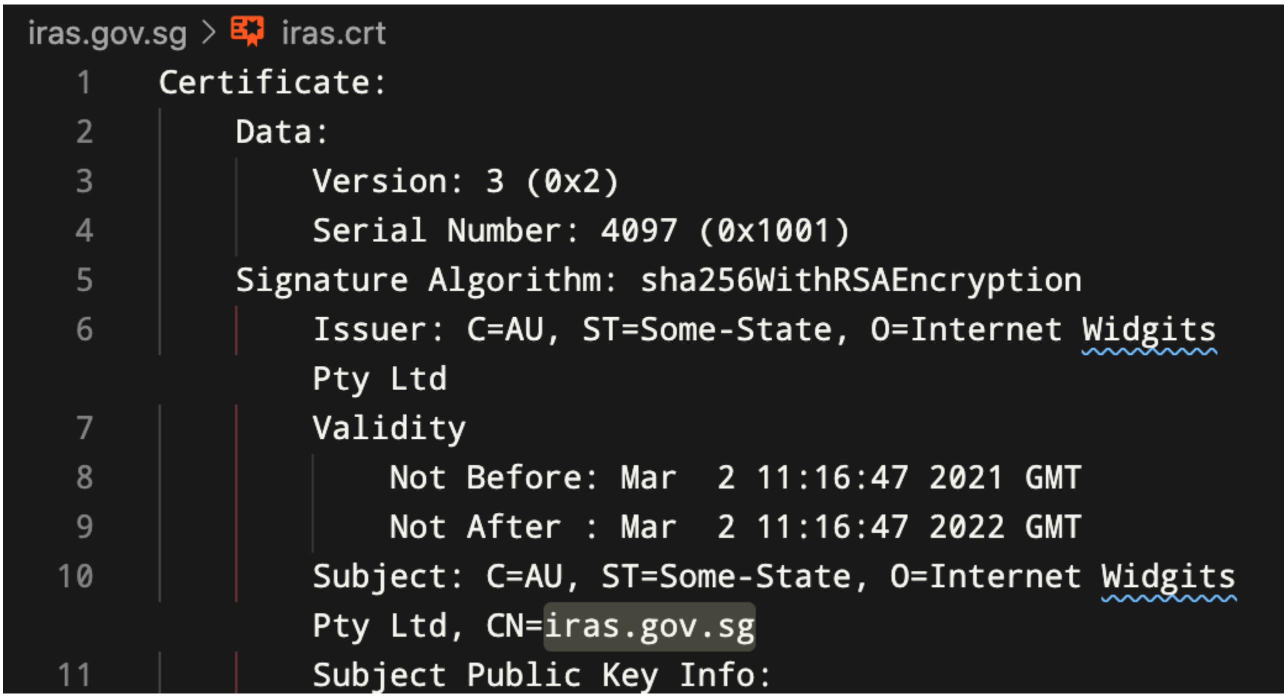
```
ubuntu@Attacker  ~/lab/lab4/iras.gov.sg   master ●        2021-03-02 03:13:59
 openssl req -new -key iras.key -out iras.csr -config ../openssl.conf
Enter pass phrase for iras.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are 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]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:iras.gov.sg
Email Address []:

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

```
# sign cert
openssl ca -in iras.csr -out iras.crt -cert ca.crt -keyfile ca.key -config openssl.conf
```

```
ubuntu@Attacker  ~/lab/lab4   master ●                    2021-03-02 03:16:44
```



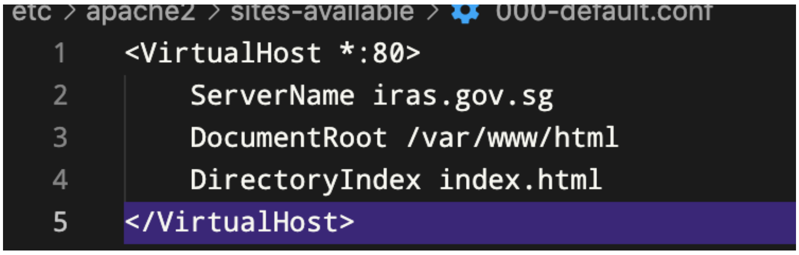
```
openssl ca -in iras.csr -out iras.crt -cert ca.crt -keyfile ca.key -config open
ssl.conf
Using configuration from openssl.conf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Mar  2 11:16:47 2021 GMT
            Not After : Mar  2 11:16:47 2022 GMT
        Subject:
            countryName               = AU
            stateOrProvinceName       = Some-State
            organizationName          = Internet Widgits Pty Ltd
            commonName                = iras.gov.sg
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                4F:9D:C4:B9:2F:6E:1F:2F:E5:6F:BF:E5:8B:E8:FA:DE:A0:D2:01:EF
            X509v3 Authority Key Identifier:
                keyid:97:BC:15:2F:F6:4D:4C:C3:B9:73:E0:EB:A7:2A:AF:4D:F9:AE:7C:D
8

Certificate is to be certified until Mar  2 11:16:47 2022 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
```



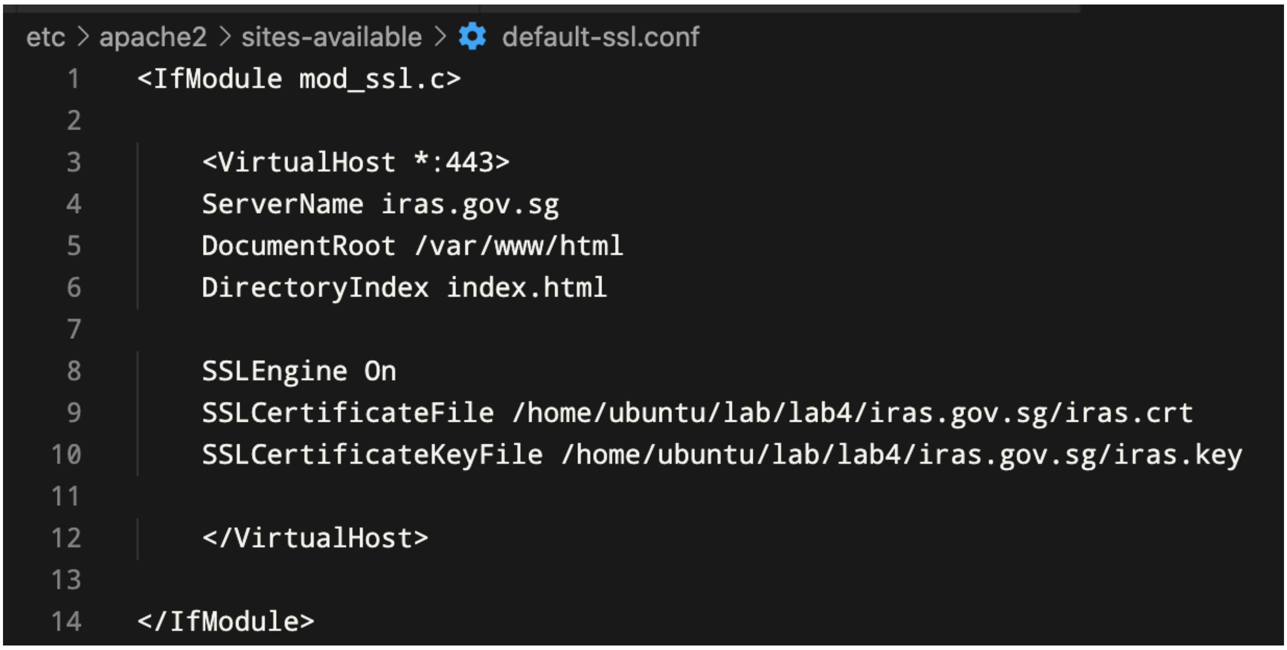
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits
        Pty Ltd
        Validity
            Not Before: Mar  2 11:16:47 2021 GMT
            Not After : Mar  2 11:16:47 2022 GMT
        Subject: C=AU, ST=Some-State, O=Internet Widgits
        Pty Ltd, CN=iras.gov.sg
        Subject Public Key Info:
```

checking the signed iras.cert
confirms that Common Name is indeed iras.gov.sg

add the following config to apache2



```
<VirtualHost *:80>
    ServerName iras.gov.sg
    DocumentRoot /var/www/html
    DirectoryIndex index.html
</VirtualHost>
```

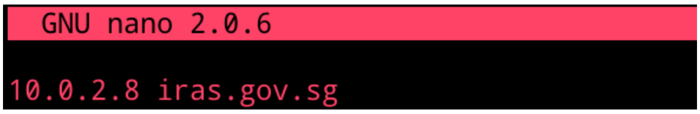


```
<IfModule mod_ssl.c>

    <VirtualHost *:443>
    ServerName iras.gov.sg
    DocumentRoot /var/www/html
    DirectoryIndex index.html

    SSLEngine On
    SSLCertificateFile /home/ubuntu/lab/lab4/iras.gov.sg/iras.crt
    SSLCertificateKeyFile /home/ubuntu/lab/lab4/iras.gov.sg/iras.key

    </VirtualHost>

</IfModule>
```

restart the apache2 server

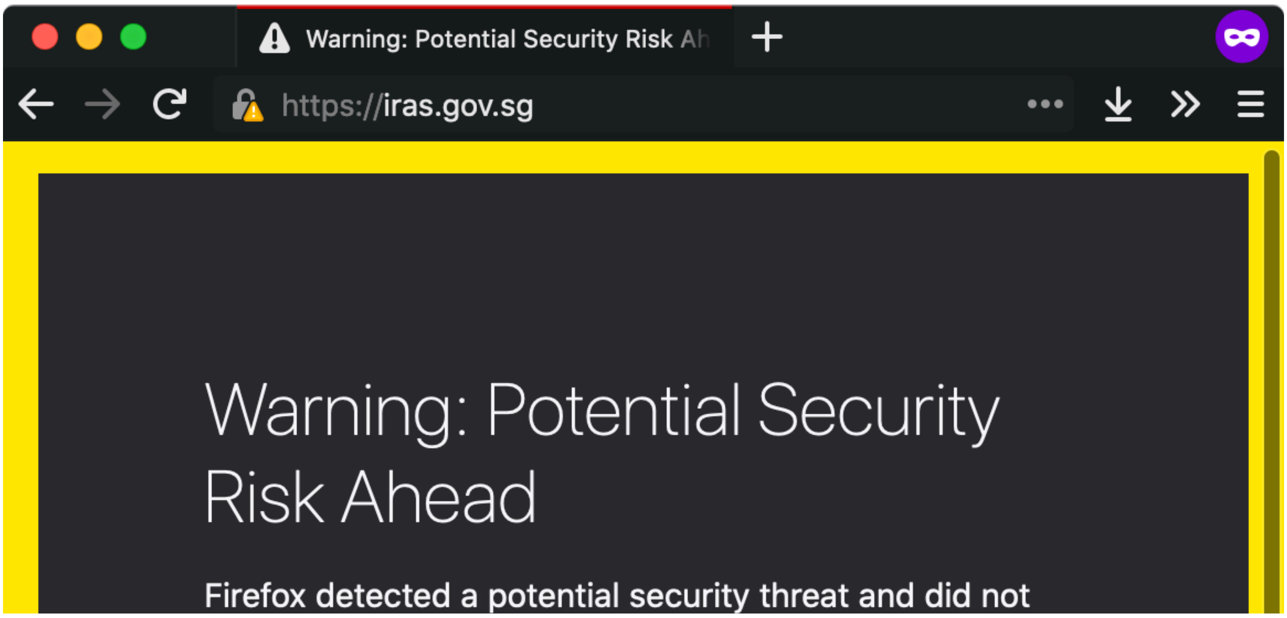
sudo service apache2 restart

on user side, edit the hosts file to emulate a DNS attack



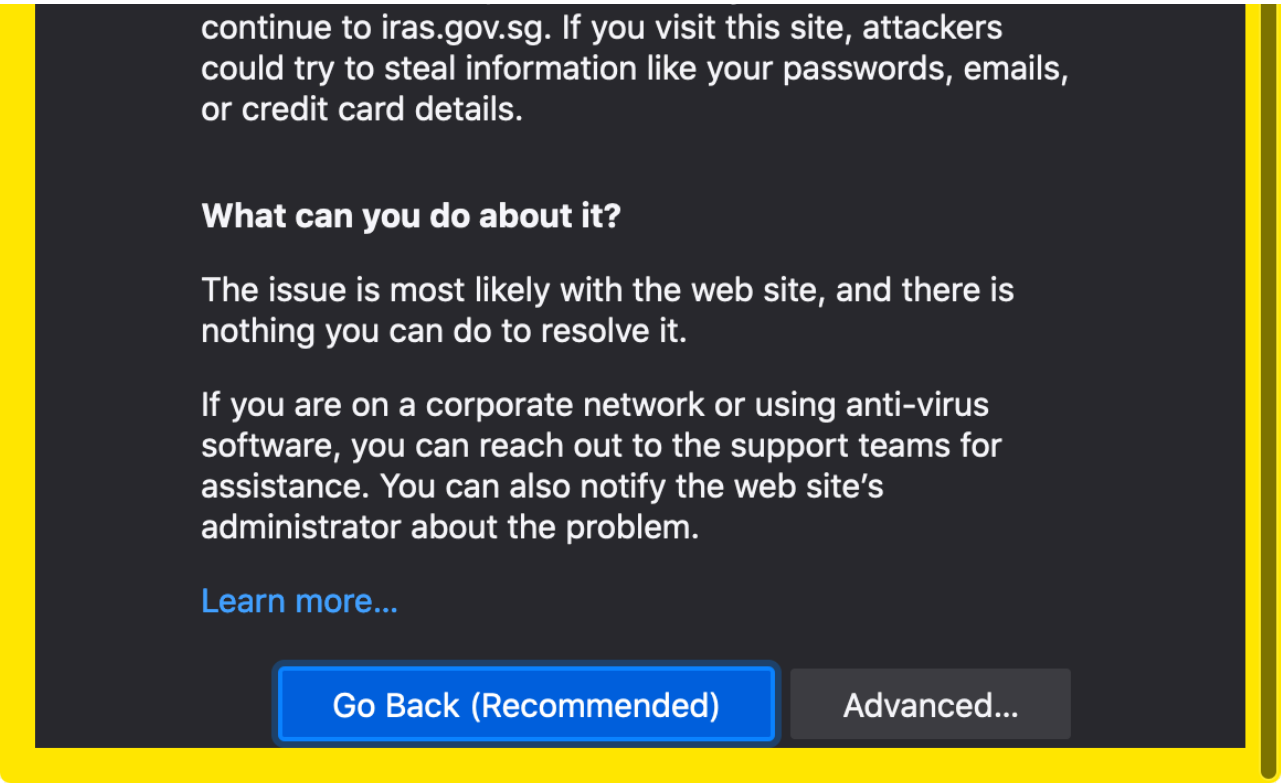
```
10.0.2.8 iras.gov.sg
```

when the user visits the website



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not



continue to iras.gov.sg. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the web site, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the web site's administrator about the problem.

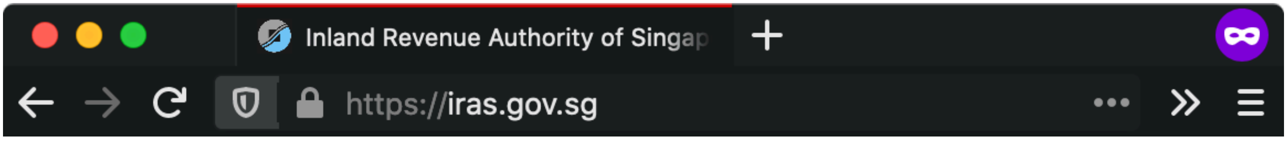
when user visits, the browser quickly prompts that the connection is not private, telling the user that there might be attackers trying to steal the user's information
normal users are usually detered by this warning and will not visit the website.
this is caused by self-signed certificate created by the attacker, that is not verified by the browser, as the root CA is not added manually.
hence, certificate defeats this type of MITM attack

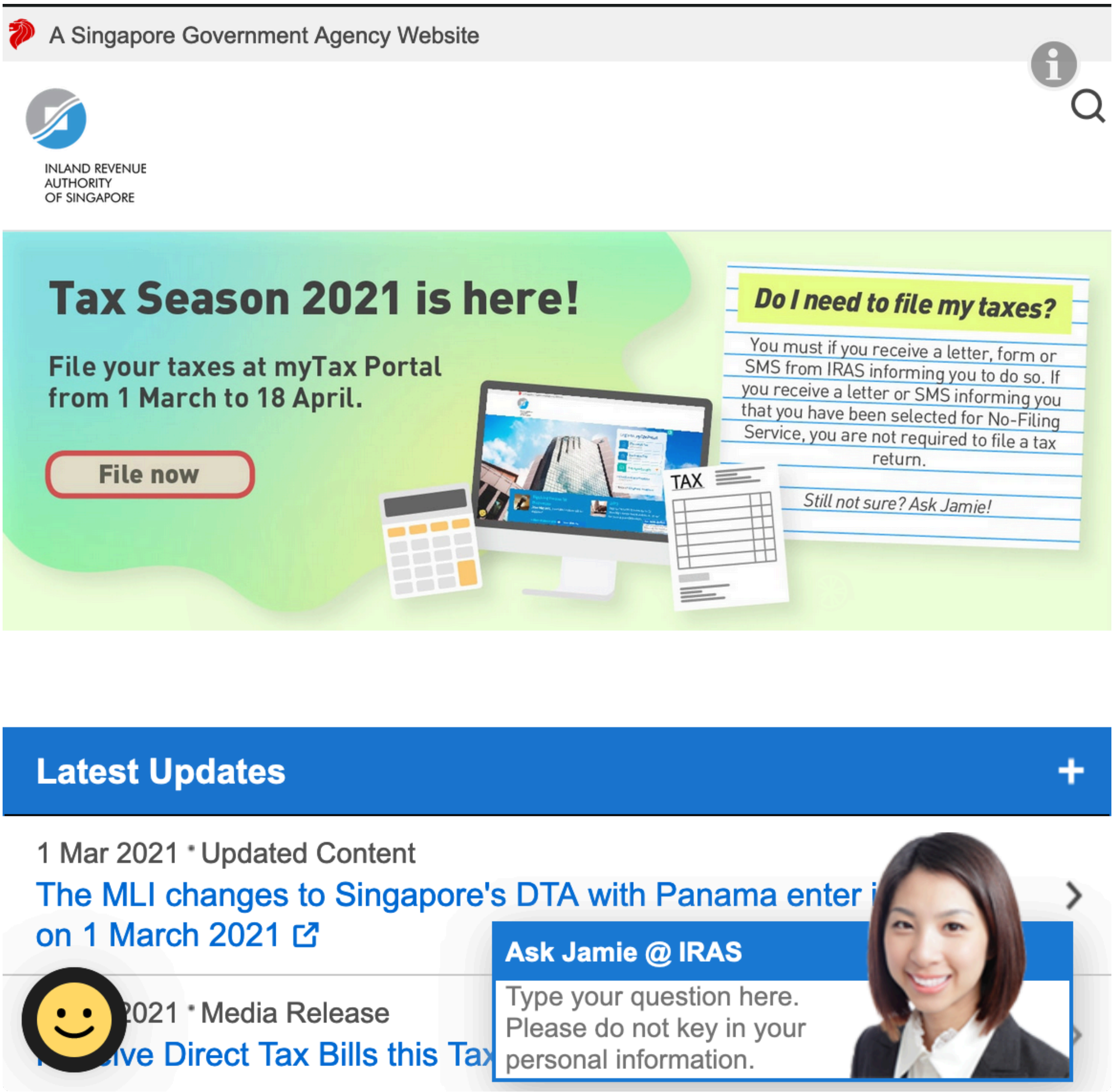
task6
if the root CA is compromised by the attacker, we can assume that the CA is one of the trusted ones by the browser

to emulate, we manually adding the root CA to the browser per task 3

using the same example as above, let say the attacker want to impersonate iras.gov.sg
he follows the same process as task 5

when the user visits the website, it behaves normally, without any browser warnings





A Singapore Government Agency Website

INLAND REVENUE AUTHORITY OF SINGAPORE

Tax Season 2021 is here!

File your taxes at myTax Portal from 1 March to 18 April.

File now

Do I need to file my taxes?

You must if you receive a letter, form or SMS from IRAS informing you to do so. If you receive a letter or SMS informing you that you have been selected for No-Filing Service, you are not required to file a tax return.

Still not sure? Ask Jamie!

Latest Updates +

1 Mar 2021 • Updated Content

The MLI changes to Singapore's DTA with Panama enter i on 1 March 2021

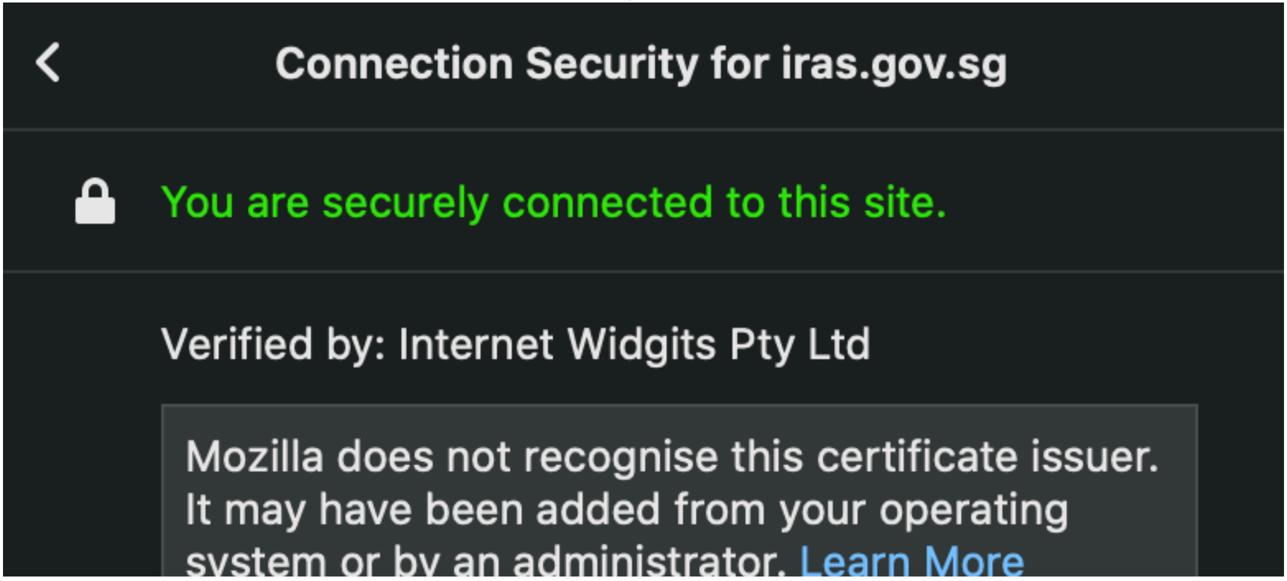
2021 • Media Release

ive Direct Tax Bills this Tax

Ask Jamie @ IRAS

Type your question here. Please do not key in your personal information.

upon inspection, it shows that the connection is secure, and the certificate is verified by a trusted CA

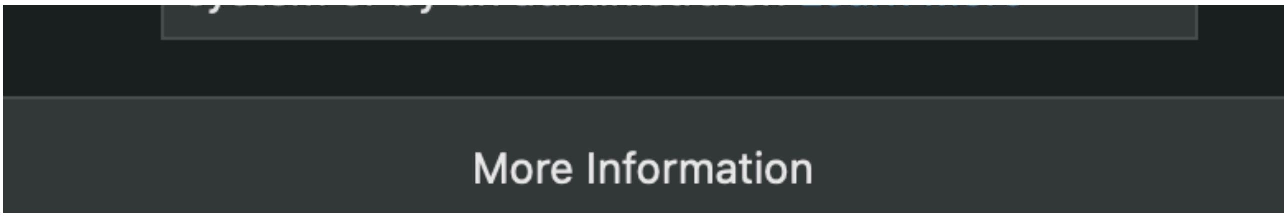


Connection Security for iras.gov.sg

You are securely connected to this site.

Verified by: Internet Widgits Pty Ltd

Mozilla does not recognise this certificate issuer. It may have been added from your operating system or by an administrator. Learn More



hence, this experiment demonstrates that if a CA is compromised, the attacker can sign as many certs as he want and spoof any legit websites without the browser raising any warnings, and the users will be fooled to enter personal info for the attacker.