Applied Cryptography (UE20CS314)

Lab 5

Name: Vishwa Mehul Mehta

SRN: PES2UG20CS389

Section: F

Task 1:

Screenshot:

```
seed@VM: ~/.../demoCA
[10/25/22]seed@VM:~/.../lab5$ cp /usr/lib/ssl/openssl.cnf .
[10/25/22]seed@VM:~/.../lab5$ ls
Labsetup  openssl.cnf
[10/25/22]seed@VM:~/.../lab5$ mkdir demoCA
[10/25/22]seed@VM:~/.../lab5$ mkdir demoCA/certs demoCA/crl demoCA/newcerts
[10/25/22]seed@VM:~/.../lab5$ cd demoCA/
[10/25/22]seed@VM:~/.../demoCA$ ls
certs  crl  newcerts
[10/25/22]seed@VM:~/.../demoCA$ touch index.txt
[10/25/22]seed@VM:~/.../demoCA$ echo "1000" > serial
[10/25/22]seed@VM:~/.../demoCA$ ls
certs  crl  index.txt  newcerts  serial
[10/25/22]seed@VM:~/.../demoCA$
```

```
[10/25/22]seed@VM:~/.../lab5$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3
650 \-keyout ca.key -out ca.crt \-subj "/CN=www.modelCA.com/O=Model CA LTD./C=US
" \-passout pass:dees
Generating a RSA private key
.....................................++++
.....................................................................
.....................................................................
.....................................................................
.................................++++
writing new private key to 'ca.key'
-----
```

```
[10/25/22]seed@VM:~/.../lab5$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7d:b7:31:19:63:b5:d1:3d:a3:7a:29:ad:57:9a:04:20:4a:34:61:16
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 25 09:17:10 2022 GMT
            Not After : Oct 22 09:17:10 2032 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:c2:5b:08:7e:ae:d5:ba:74:63:fe:37:4e:9f:c2:
                    89:1d:7c:ae:6d:a0:09:cf:7a:e0:08:fd:54:b6:0a:
                    b2:1d:8a:48:88:5b:2a:02:27:f8:cf:73:a0:67:10:
                    55:5f:2d:6e:34:b6:44:57:33:63:b7:56:09:be:fb:
                    c9:5d:14:02:7f:2e:17:9f:64:50:89:36:7e:62:e9:
                    7e:9d:8a:85:b3:ac:00:7c:fb:1a:2b:8f:f4:d3:1a:
                    eb:aa:de:70:89:9c:a3:46:2f:30:6f:3b:55:f5:42:
                    43:7f:76:d6:30:60:da:ba:10:45:d4:c3:9e:96:40:
```

```
[10/25/22]seed@VM:~/.../lab5$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:c2:5b:08:7e:ae:d5:ba:74:63:fe:37:4e:9f:c2:
    89:1d:7c:ae:6d:a0:09:cf:7a:e0:08:fd:54:b6:0a:
    b2:1d:8a:48:88:5b:2a:02:27:f8:cf:73:a0:67:10:
    55:5f:2d:6e:34:b6:44:57:33:63:b7:56:09:be:fb:
    c9:5d:14:02:7f:2e:17:9f:64:50:89:36:7e:62:e9:
    7e:9d:8a:85:b3:ac:00:7c:fb:1a:2b:8f:f4:d3:1a:
    eb:aa:de:70:89:9c:a3:46:2f:30:6f:3b:55:f5:42:
    43:7f:76:d6:30:60:da:ba:10:45:d4:c3:9e:96:40:
    71:93:db:5a:75:75:7b:98:69:81:27:dd:dc:0d:ea:
    e8:f3:e4:7f:a3:09:8a:a5:64:42:c7:51:38:1b:65:
    c8:c1:35:a4:e2:0c:d9:4b:92:9a:a9:bf:0d:c2:65:
    23:55:88:ba:95:2a:09:7f:53:c3:42:23:02:9e:10:
    86:7c:a3:16:56:ee:4b:87:1e:63:3f:88:f5:a9:7d:
    a3:ff:29:6d:21:e9:6b:48:6c:98:34:0a:46:66:91:
    49:38:32:40:af:df:8a:d4:5b:32:f0:dd:30:74:2f:
    38:2c:7c:bb:80:2a:20:5d:a1:67:67:b6:e1:ac:fc:
    d4:5c:ae:f9:0b:7e:50:a4:d6:0c:a8:dd:21:27:8d:
    98:37:14:8d:1c:20:08:15:e6:c4:3f:17:49:1c:91:
    4a:66:11:70:11:af:05:23:88:e3:b5:7f:97:4d:6b:
```

Observation:

Here, we make the machine a CA using the commands given.

Task 2:

Screenshot:

```
[10/25/22]seed@VM:~/.../lab5$ openssl req -newkey rsa:2048 -sha256 \-keyout serv
er.key -out server.csr \-subj "/CN=www.bank32.com/O=Bank32 Inc./C=US" \-passout
pass:dees \-addext "subjectAltName = DNS:www.bank32.com, \DNS:www.bank32A.com, \
DNS:www.bank32B.com"
Generating a RSA private key
.....+++++
.....
.....+++++
writing new private key to 'server.key'
-----
[10/25/22]seed@VM:~/.../lab5$ openssl req -in server.csr-text -noout
Can't open server.csr-text for reading, No such file or directory
139941181330752:error:02001002:system library:fopen:No such file or directory:cr
ypto/bio/bss_file.c:69:fopen('server.csr-text','r')
139941181330752:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio
/bss_file.c:76:
```

```
seed@VM: ~/.../lab5
[10/25/22]seed@VM:~/.../lab5$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:dc:f9:c7:01:cc:b3:ad:4f:9e:d0:29:d4:c5:24:
    0f:48:9a:b7:77:96:39:0e:02:f8:9a:93:32:66:23:
    fb:74:5c:da:27:3f:07:5b:32:9c:7b:49:46:40:44:
    f7:7d:0e:88:f8:b3:b1:a6:3b:cd:f7:a1:7d:ca:6e:
    d5:4d:2b:cf:50:f1:9e:a9:7b:f3:75:70:22:8c:54:
    2e:59:3c:e1:e2:5c:65:df:c1:fc:7d:4a:0c:a7:8e:
    88:a5:3e:b3:39:64:22:cf:24:b6:41:e7:8d:36:fc:
    e7:40:44:60:9c:54:89:27:db:5c:e6:0a:58:49:a3:
    bd:a9:c8:73:76:1f:10:8e:ee:04:9d:e9:33:66:e9:
    b0:ff:2d:81:24:e8:c8:ef:56:cb:7f:8f:99:f7:b0:
    0c:53:63:23:ca:45:43:00:be:8e:81:6f:48:78:3b:
    c8:6f:8c:5c:c7:e5:b7:f0:48:da:ae:af:f0:bb:07:
    bf:48:18:eb:27:be:05:92:41:bb:bd:22:f9:f3:ce:
    80:3d:02:f8:d6:38:c2:db:61:09:7b:33:6e:d3:ea:
    54:38:13:4e:ce:6e:d6:06:73:60:19:31:22:52:d4:
    0d:cd:5b:a4:cc:72:96:a5:9e:bd:ea:36:13:e5:03:
    6b:42:f8:a2:8e:e0:44:c1:6c:1f:a7:b7:18:b6:8b:
    52:1b
publicExponent: 65537 (0x10001)
privateExponent:
```

Observation:

We have generated a certificate request for the web server bank32.com.

Task 3:

Screenshot:

```
[10/25/22]seed@VM:~/.../lab5$ openssl ca -config openssl.cnf -policy policy_anything \-md sha256 -days 3650 \-in
server.csr -out server.crt -batch \-cert ca.crt -keyfile ca.key
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: Oct 25 09:36:12 2022 GMT
            Not After : Oct 22 09:36:12 2032 GMT
        Subject:
            countryName               = US
            organizationName          = Bank32 Inc.
            commonName                = www.bank32.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                57:9B:65:7A:F1:5B:27:43:69:3B:F9:F9:22:E2:E5:AB:CC:1A:74:64
            X509v3 Authority Key Identifier:
                keyid:74:10:9E:45:71:D2:D9:A4:5A:4B:39:47:D0:A6:47:45:69:ED:9A:D9

Certificate is to be certified until Oct 22 09:36:12 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[10/25/22]seed@VM:~/.../lab5$
```

```
[10/25/22]seed@VM:~/.../lab5$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 25 09:36:12 2022 GMT
            Not After : Oct 22 09:36:12 2032 GMT
        Subject: C = US, O = Bank32 Inc., CN = www.bank32.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:dc:f9:c7:01:cc:b3:ad:4f:9e:d0:29:d4:c5:24:
                    0f:48:9a:b7:77:96:39:0e:02:f8:9a:93:32:66:23:
                    fb:74:5c:da:27:3f:07:5b:32:9c:7b:49:46:40:44:
                    f7:7d:0e:88:f8:b3:b1:a6:3b:cd:f7:a1:7d:ca:6e:
                    d5:4d:2b:cf:50:f1:9e:a9:7b:f3:75:70:22:8c:54:
                    2e:59:3c:e1:e2:5c:65:df:c1:fc:7d:4a:0c:a7:8e:
                    88:a5:3e:b3:39:64:22:cf:24:b6:41:e7:8d:36:fc:
                    e7:40:44:60:9c:54:89:27:db:5c:e6:0a:58:49:a3:
                    bd:a9:c8:73:76:1f:10:8e:ee:04:9d:e9:33:66:e9:
                    b0:ff:2d:81:24:e8:c8:ef:56:cb:7f:8f:99:f7:b0:
```

Observation:

We generate a certificate for our server here.

Task 4:

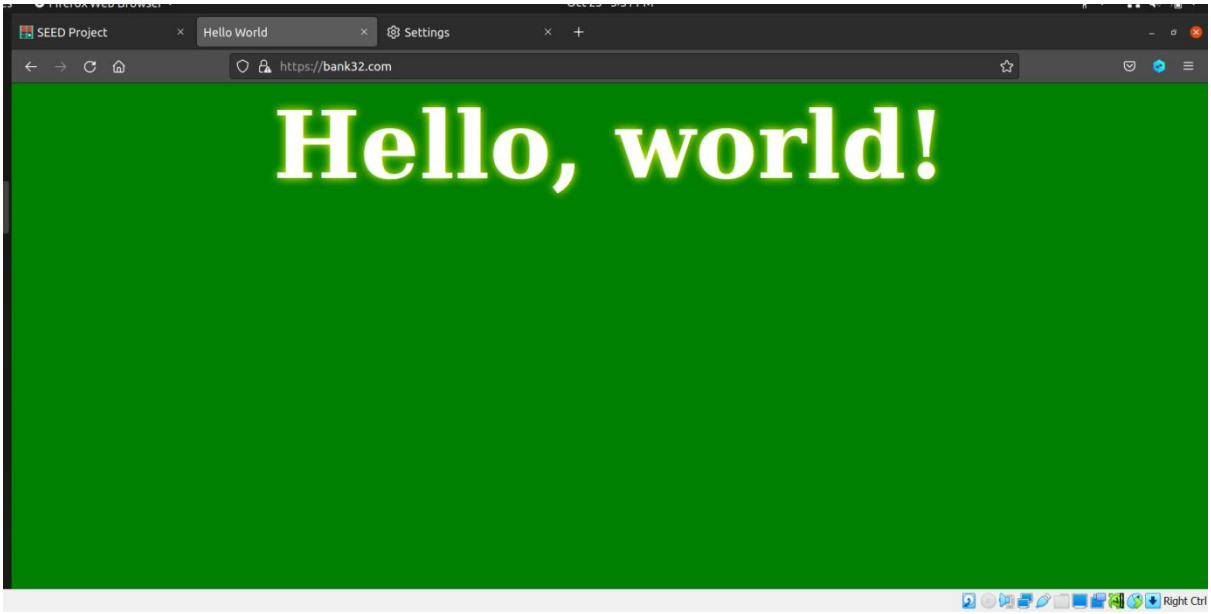
Screenshot:

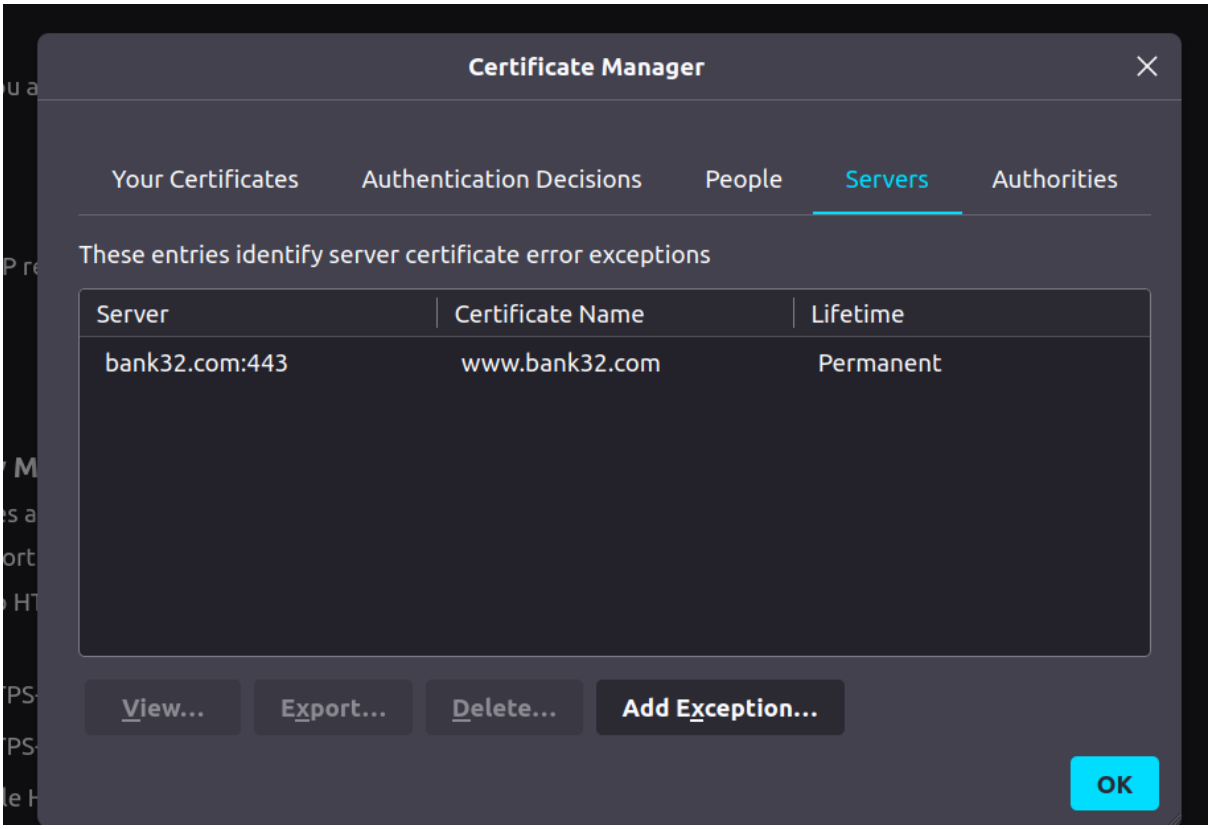
```
seed@VM: ~/.../Labsetup    root@e23ca27e94ae: /    seed@VM: ~/.../Labsetup
[10/25/22]seed@VM:~/.../Labsetup$ docker-compose build
Building web-server
Step 1/7 : FROM handsonsecurity/seed-server:apache-php
apache-php: Pulling from handsonsecurity/seed-server
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
Digest: sha256:fb3b6a03575af14b6a59ada1d7a272a61bc0f2d975d0776dba98eff0948de275
Status: Downloaded newer image for handsonsecurity/seed-server:apache-php
 ---> 2365d0ed3ad9
Step 2/7 : ARG WWWDIR=/var/www/bank32
 ---> Running in 4bbbe443b109
Removing intermediate container 4bbbe443b109
 ---> 0858ad038ae9
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> 611aa8428b7c
Step 4/7 : COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
 ---> d7e9638b248c
Step 5/7 : COPY ./certs/bank32.crt ./certs/bank32.key  /certs/
 ---> da9a09654173
Step 6/7 : RUN  chmod 400 /certs/bank32.key      && chmod 644 $WWWDIR/index.html      && chmod 644 $WWWDIR/index_
red.html      && a2ensite bank32_apache_ssl
 ---> Running in 0b7d931f7d16
Enabling site bank32_apache_ssl.
```

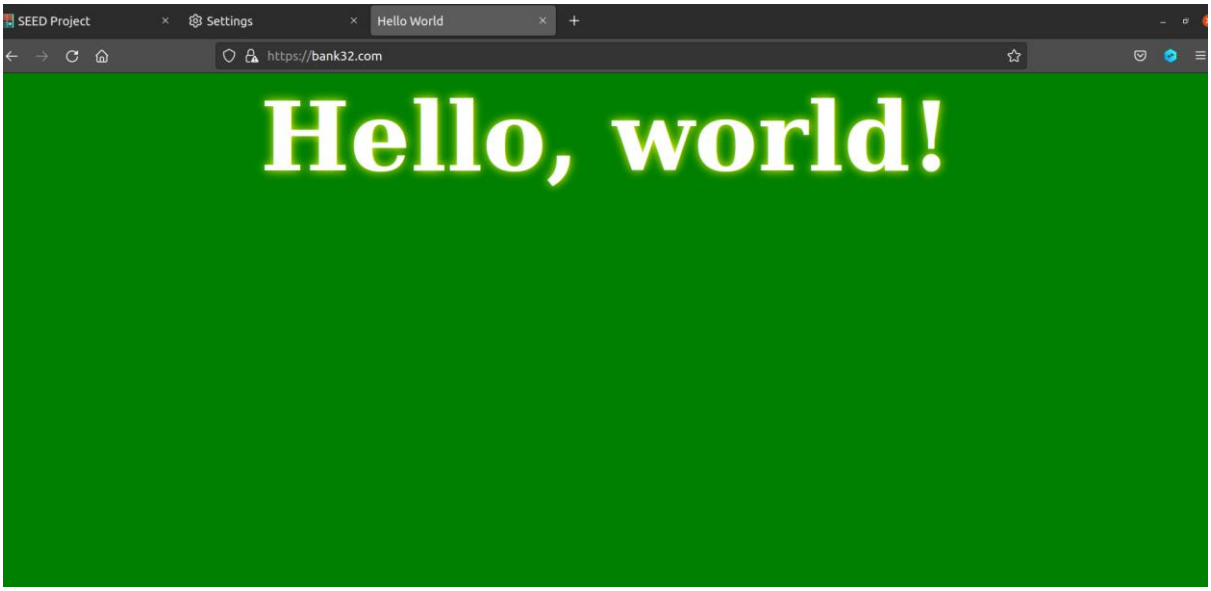
```
 ---> Running in 0b7d931f7d16
Enabling site bank32_apache_ssl.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container 0b7d931f7d16
 ---> fc90475b66eb
Step 7/7 : CMD  tail -f /dev/null
 ---> Running in 67e7c9d8150b
Removing intermediate container 67e7c9d8150b
 ---> b04306fda30d

Successfully built b04306fda30d
Successfully tagged seed-image-www-pki:latest
[10/25/22]seed@VM:~/.../Labsetup$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
Creating www-10.9.0.80 ... done
```

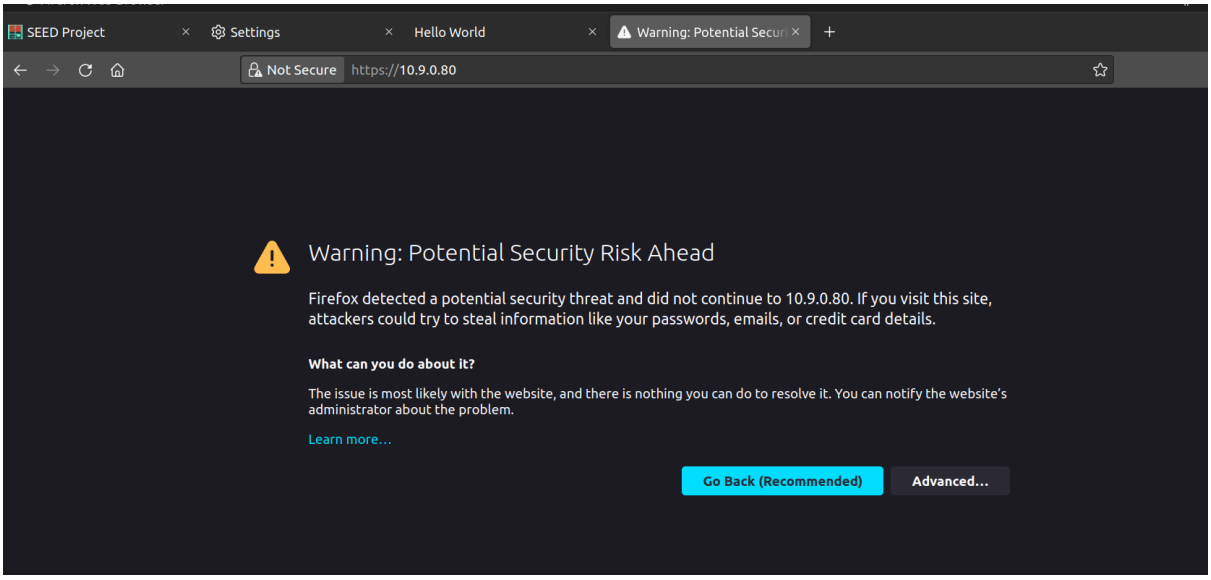
```
root@e23ca27e94ae: /
seed@VM: ~/.../Labsetup    root@e23ca27e94ae: /    seed@VM: ~/.../Labs
[10/25/22]seed@VM:~/.../Labsetup$ dockps
e23ca27e94ae  www-10.9.0.80
[10/25/22]seed@VM:~/.../Labsetup$ docksh e2
root@e23ca27e94ae:/# cat etc/apache2/sites-available/bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    ServerAlias www.bank32A.com
    ServerAlias www.bank32B.com
    ServerAlias www.bank32W.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/bank32.crt
    SSLCertificateKeyFile /certs/bank32.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
```

```
root@e23ca27e94ae:/# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@e23ca27e94ae:/#
```







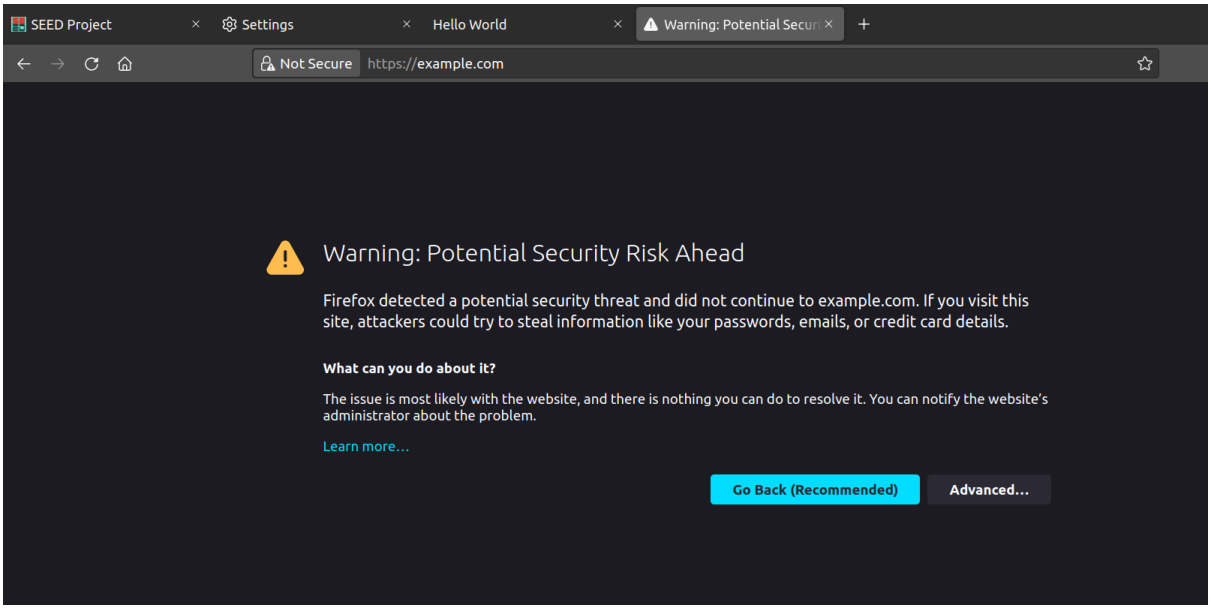


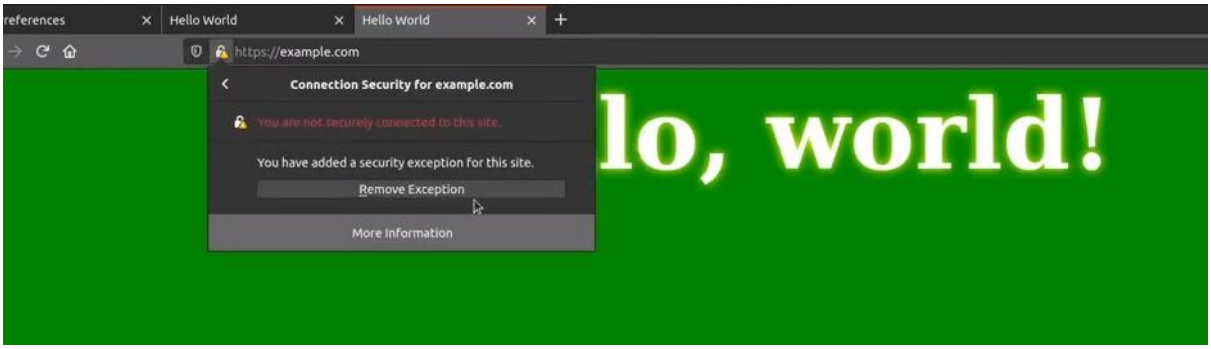
Observation:

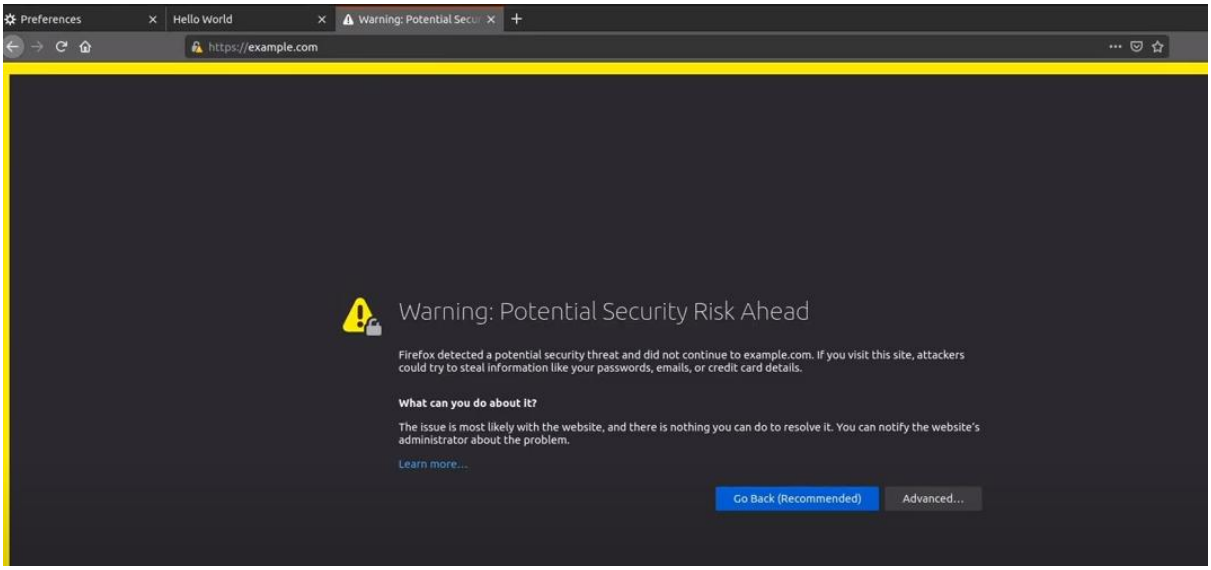
We can see the **Hello World** written when we navigate to https://www.bank32.com, but we see that the site is unsafe. On adding the CA to the list of certificate authorities this warning is no longer seen. We cannot use the IP address to access the website.

Task 5:

Screenshot:







Observation:

We are not able to successfully launch the website using a DNS cache poisoning attack as it is protected against such an attack. We see that we can see that the site is unsafe even after removing the exception.