Crypto Lab - 5

Name: H M Mythreya
SRN: PES2UG20CS130

Task 1: Becoming a certificate authority (CA)

ca.crt

```
[10/26/22]seed@VM:~/.../week5$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            28:c8:3d:f4:33:73:b0:5c:93:7a:a0:44:8c:64:3d:3f:b5:1c:e6:fc
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 26 16:18:40 2022 GMT
            Not After : Oct 23 16:18:40 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:d7:32:3d:94:b3:f2:db:fb:ab:a4:c7:ad:d1:2c:
                    cf:2f:86:40:a1:7c:c3:18:64:68:5c:99:61:c9:d6:
                    7d:52:07:73:d5:01:e1:c2:c7:90:fd:eb:c5:c9:2f:
                    77:4d:69:56:ce:96:f8:96:28:0c:9e:67:a2:30:1a:
                    2a:bb:a4:49:f0:20:06:9b:d6:00:24:e0:28:d5:ad:
                    b1:3f:ce:7c:1a:6b:ee:8c:b7:7c:40:56:51:ba:a5:
                    c9:b4:3c:d9:4b:40:b4:90:a1:7b:2b:2b:e1:21:49:
                    ca:d9:ea:1e:0a:76:9c:13:c4:19:3e:22:f7:c5:4f:
                    fa:6b:17:f7:92:7d:b3:b5:3a:5a:11:a1:3f:c8:33:
                    19:7b:24:ce:2c:ca:9e:61:1f:13:49:2d:56:9e:45:
                    d5:b4:26:80:6d:17:ab:3e:93:f8:a8:34:37:28:36:
                    7b:38:d6:ef:e7:5b:f9:59:66:68:90:e9:21:33:3d:
                    3d:5d:13:fe:7d:6b:35:7c:41:64:a6:a7:c3:e4:a2:
                    c0:ce:b5:c4:27:1e:ad:c7:cc:56:fa:9a:68:c5:28:
                    62:ca:b7:0d:cf:4a:0f:b0:fb:8e:04:5e:12:a6:c6:
                    a2:15:49:a8:f2:69:d7:11:5c:7d:0e:c5:75:59:1c:
```

ca.key

```
[10/26/22]seed@VM:~/.../week5$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:d7:32:3d:94:b3:f2:db:fb:ab:a4:c7:ad:d1:2c:
    cf:2f:86:40:a1:7c:c3:18:64:68:5c:99:61:c9:d6:
    7d:52:07:73:d5:01:e1:c2:c7:90:fd:eb:c5:c9:2f:
    77:4d:69:56:ce:96:f8:96:28:0c:9e:67:a2:30:1a:
    2a:bb:a4:49:f0:20:06:9b:d6:00:24:e0:28:d5:ad:
    b1:3f:ce:7c:1a:6b:ee:8c:b7:7c:40:56:51:ba:a5:
    c9:b4:3c:d9:4b:40:b4:90:a1:7b:2b:2b:e1:21:49:
    ca:d9:ea:1e:0a:76:9c:13:c4:19:3e:22:f7:c5:4f:
    fa:6b:17:f7:92:7d:b3:b5:3a:5a:11:a1:3f:c8:33:
    19:7b:24:ce:2c:ca:9e:61:1f:13:49:2d:56:9e:45:
    d5:b4:26:80:6d:17:ab:3e:93:f8:a8:34:37:28:36:
    7b:38:d6:ef:e7:5b:f9:59:66:68:90:e9:21:33:3d:
    3d:5d:13:fe:7d:6b:35:7c:41:64:a6:a7:c3:e4:a2:
    c0:ce:b5:c4:27:1e:ad:c7:cc:56:fa:9a:68:c5:28:
    62:ca:b7:0d:cf:4a:0f:b0:fb:8e:04:5e:12:a6:c6:
    a2:15:49:a8:f2:69:d7:11:5c:7d:0e:c5:75:59:1c:
    a6:f1:df:0a:1a:62:6e:95:7b:16:0c:eb:17:9e:52:
    e1:d4:1a:bc:17:d6:17:da:cc:ba:60:4a:80:47:61:
    c4:de:8e:d2:34:65:e6:16:64:6b:2c:dc:90:06:93:
    c3:ad:42:30:9a:4f:98:bd:ca:6b:27:68:43:dc:e6:
    a0:a8:be:cb:7e:7b:88:e4:65:6c:ed:7c:c4:a6:7d:
    52:c0:3f:de:c8:33:b7:46:3b:37:f3:dc:dd:d7:a8:
    67:b8:35:b8:ae:25:b7:05:c7:15:a4:4f:41:94:09:
    78:be:c8:1a:62:75:d7:f5:a4:f1:2e:03:10:59:95:
    b9:0b:1e:e6:96:97:56:3f:4a:97:e0:b1:4d:e7:d5:
    dc:29:5b:8a:3a:0b:87:bf:b5:b2:79:28:ff:07:65:
    22:4c:58:d7:8a:ea:b8:77:3d:a7:61:28:62:8c:4d:
    5b:eb:dc:48:4f:2c:82:5c:50:74:e1:04:b5:94:76:
    13:f5:57:47:b7:ee:bc:88:52:a5:49:f7:55:9b:7f:
```

Task 2: Generating a Certificate Request for the web server

server.csr

```
[10/26/22]seed@VM:~/.../week5$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32.com, O = Bank32 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:cb:a9:10:6b:ef:ad:80:25:17:12:f7:ec:8d:b8:
                    05:01:f8:03:d2:35:ed:9b:22:b0:d2:ac:2d:f1:0b:
                    99:af:c2:1b:d6:c6:47:56:9f:2e:dc:51:6e:9c:99:
                    dc:21:ed:c4:b7:4e:5e:e6:21:6d:89:d3:3b:60:49:
                    f3:8b:59:9d:8c:49:18:fb:7c:51:79:e0:f9:3f:52:
                    ba:fd:d3:d9:e0:d4:3d:f1:57:a8:fe:16:81:cb:2e:
                    c1:4d:bd:37:f8:d4:04:9a:49:df:e6:cf:11:2f:df:
                    a1:3b:f5:3b:57:95:00:4b:d6:3f:5b:c4:1c:2d:6c:
                    48:b7:5d:f2:0f:bd:dd:31:1a:80:ec:8c:43:72:f7:
                    d4:2a:5e:67:53:5b:c5:59:33:33:c3:6c:da:87:c3:
                    7b:e5:97:3c:74:e3:d5:b3:20:ec:bc:90:76:c1:a8:
                    77:60:ac:fb:ea:d4:89:93:86:19:16:3d:39:31:8e:
                    42:88:e0:2e:f9:61:90:45:01:a4:9b:42:e1:a7:81:
                    75:d6:d8:0c:93:05:bc:53:bb:67:0a:48:17:e0:b6:
                    96:d8:81:b3:57:09:63:f5:5d:0e:9c:f6:f2:86:ae:
                    dc:cc:42:4e:ff:9d:22:d5:f2:ae:9a:fb:8c:84:86:
                    ce:f3:5d:97:d2:a3:4e:e5:ff:55:72:1f:81:ba:91:
                    29:81
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com
    Signature Algorithm: sha256WithRSAEncryption
         3a:e1:5a:1d:f6:bd:89:c0:88:b8:3d:57:0e:38:fb:fe:f3:87:
```

server.key

```
[10/26/22]seed@VM:~/.../week5$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:ac:c9:58:17:37:d5:87:0e:b0:a3:eb:08:8f:82:
    66:63:e9:7c:a2:71:32:ae:0d:b1:66:b2:28:2d:64:
    1e:7f:34:34:b3:6d:2d:af:84:d0:76:15:21:80:ac:
    78:f5:32:59:31:55:b0:f4:fa:51:93:f2:dd:56:d6:
    cf:ce:0c:56:d1:d4:7a:eb:38:78:56:e8:97:53:14:
    1f:0c:aa:46:52:ad:72:b0:e6:00:21:35:21:d7:10:
    b8:23:6e:5b:d6:29:c3:be:bd:7c:ca:61:1b:4d:26:
    c3:ab:67:e3:69:00:95:c1:cd:79:0a:6e:bd:ba:92:
    6e:76:4d:1e:52:03:d5:cb:1e:a2:78:fe:ea:d5:82:
    e8:65:a5:8d:6c:25:10:90:4a:38:f6:6f:f0:41:d4:
    8c:d7:7c:89:1a:9f:06:97:59:db:3a:a7:5c:17:3d:
    d8:10:a1:df:5e:4d:0f:1d:ca:d2:4a:13:16:80:67:
    4f:00:83:64:33:e8:82:94:3d:1c:b3:07:b9:9e:fa:
    1d:ac:b9:75:cc:ab:2b:81:30:1b:79:ab:96:e3:92:
    4d:8a:0d:8e:1c:97:9d:25:4e:01:ac:65:20:54:d7:
    6d:9c:2f:d9:4b:bb:4a:75:b3:6c:8b:9e:d9:ee:23:
    5b:ba:a8:be:ce:ad:f5:3d:7d:2e:bc:e3:d3:bd:27:
    ee:19
publicExponent: 65537 (0x10001)
privateExponent:
    00:a8:6f:05:ee:6c:41:3c:8c:f7:68:73:1f:3f:36:
    30:b5:c8:cf:f4:52:40:c3:27:19:fe:30:41:b6:2d:
    d9:04:cb:51:6c:6f:4b:8f:c3:fa:aa:81:62:cd:5a:
    53:f7:42:03:6c:72:4a:34:25:28:0c:ff:3d:01:00:
    1a:46:94:04:b6:3b:59:2f:9f:36:c0:11:b0:22:0e:
    85:4e:05:56:d4:15:bc:ad:f1:27:c3:37:56:2b:9e:
    62:c2:37:3c:53:03:17:8c:02:8f:79:81:3b:e9:f3:
    95:de:ab:41:26:04:a9:f7:e8:62:cb:e6:b4:11:01:
    d9:a8:7c:f8:c7:9e:71:74:b4:68:3b:74:8a:cc:07:
    b6:a5:fd:2c:82:2d:0e:01:f4:50:db:3f:0e:06:d0:
```

Task 3: Generating a Certificate for your server

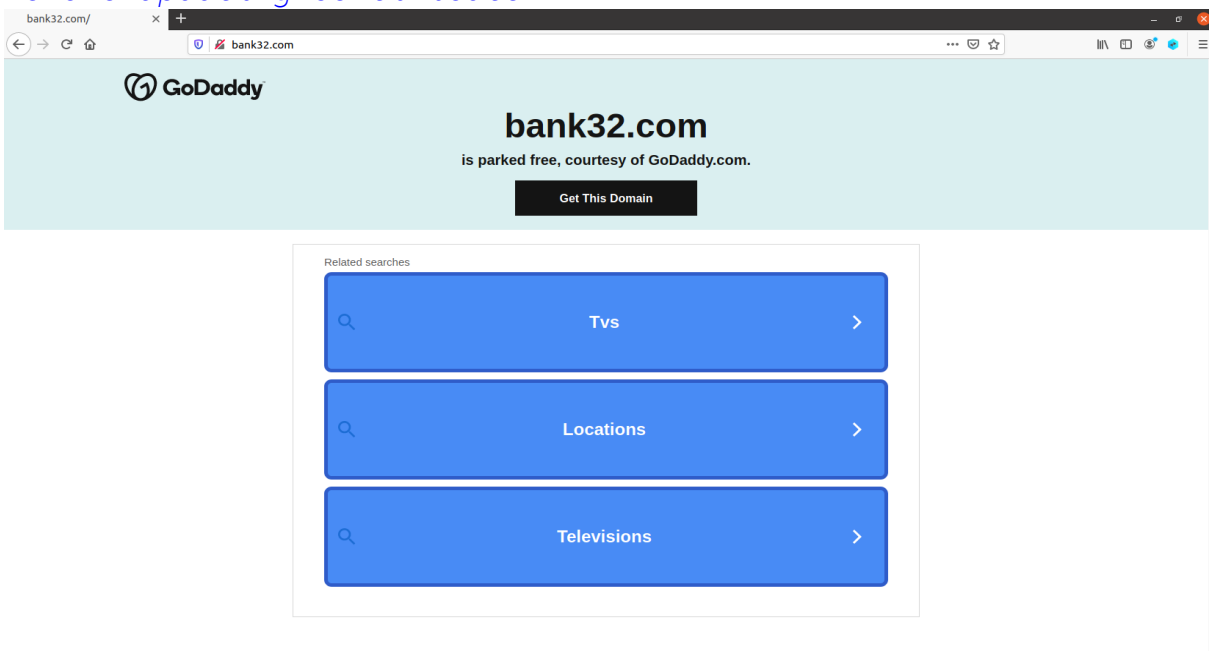
```
[10/26/22]seed@VM:~/.../pki_lab$ openssl ca -config openssl.cnf -policy policy_anything \-md sha256 -days 3650 \-in server.csr
 -out server.crt -batch \-cert ca.crt -keyfile ca.key
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4660 (0x1234)
        Validity
            Not Before: Oct 26 16:33:10 2022 GMT
            Not After : Oct 23 16:33:10 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:
                7B:D0:A0:CF:3C:68:AB:92:87:B7:42:05:57:44:40:50:45:F0:CE:36
            X509v3 Authority Key Identifier:
                keyid:AB:67:23:38:68:0D:0B:B5:25:0A:85:11:CE:80:CC:49:3E:79:EC:0A

Certificate is to be certified until Oct 23 16:33:10 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

server.crt

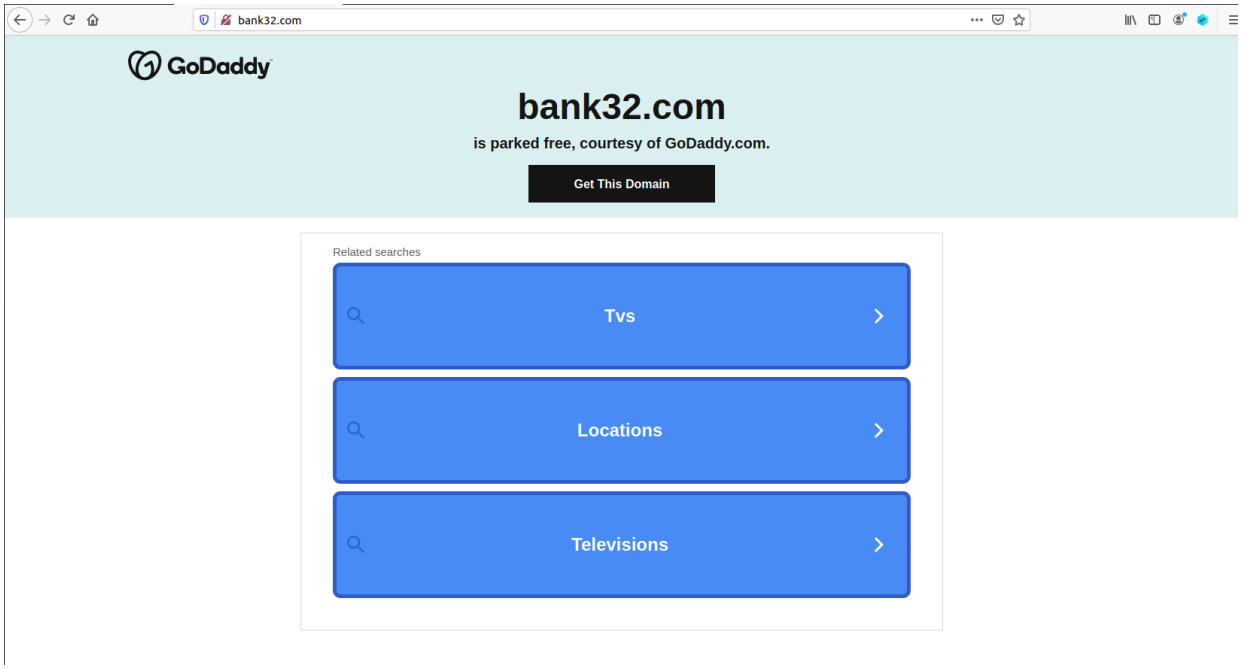
```
[10/26/22]seed@VM:~/.../pki_lab$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4660 (0x1234)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: Oct 26 16:33:10 2022 GMT
            Not After : Oct 23 16:33:10 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:ac:c9:58:17:37:d5:87:0e:b0:a3:eb:08:8f:82:
                    66:63:e9:7c:a2:71:32:ae:0d:b1:66:b2:28:2d:64:
                    1e:7f:34:34:b3:6d:2d:af:84:d0:76:15:21:80:ac:
                    78:f5:32:59:31:55:b0:f4:fa:51:93:f2:dd:56:d6:
                    cf:ce:0c:56:d1:d4:7a:eb:38:78:56:e8:97:53:14:
                    1f:0c:aa:46:52:ad:72:b0:e6:00:21:35:21:d7:10:
                    b8:23:6e:5b:d6:29:c3:be:bd:7c:ca:61:1b:4d:26:
                    c3:ab:67:e3:69:00:95:c1:cd:79:0a:6e:bd:ba:92:
                    6e:76:4d:1e:52:03:d5:cb:1e:a2:78:fe:ea:d5:82:
                    e8:65:a5:8d:6c:25:10:90:4a:38:f6:6f:f0:41:d4:
                    8c:d7:7c:89:1a:9f:06:97:59:db:3a:a7:5c:17:3d:
                    d8:10:a1:df:5e:4d:0f:1d:ca:d2:4a:13:16:80:67:
                    4f:00:83:64:33:e8:82:94:3d:1c:b3:07:b9:9e:fa:
                    1d:ac:b9:75:cc:ab:2b:81:30:1b:79:ab:96:e3:92:
                    4d:8a:0d:8e:1c:97:9d:25:4e:01:ac:65:20:54:d7:
                    6d:9c:2f:d9:4b:bb:4a:75:b3:6c:8b:9e:d9:ee:23:
                    5b:ba:a8:be:ce:ad:f5:3d:7d:2e:bc:e3:d3:bd:27:
```

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

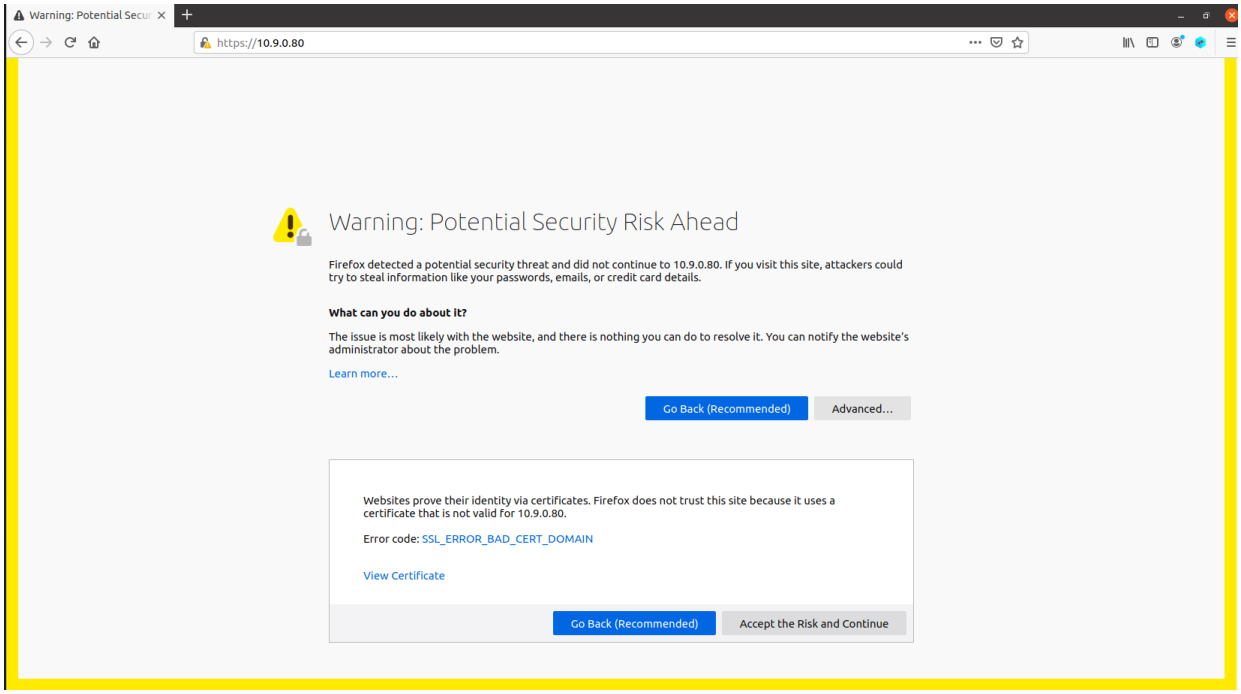
Before updating certificate



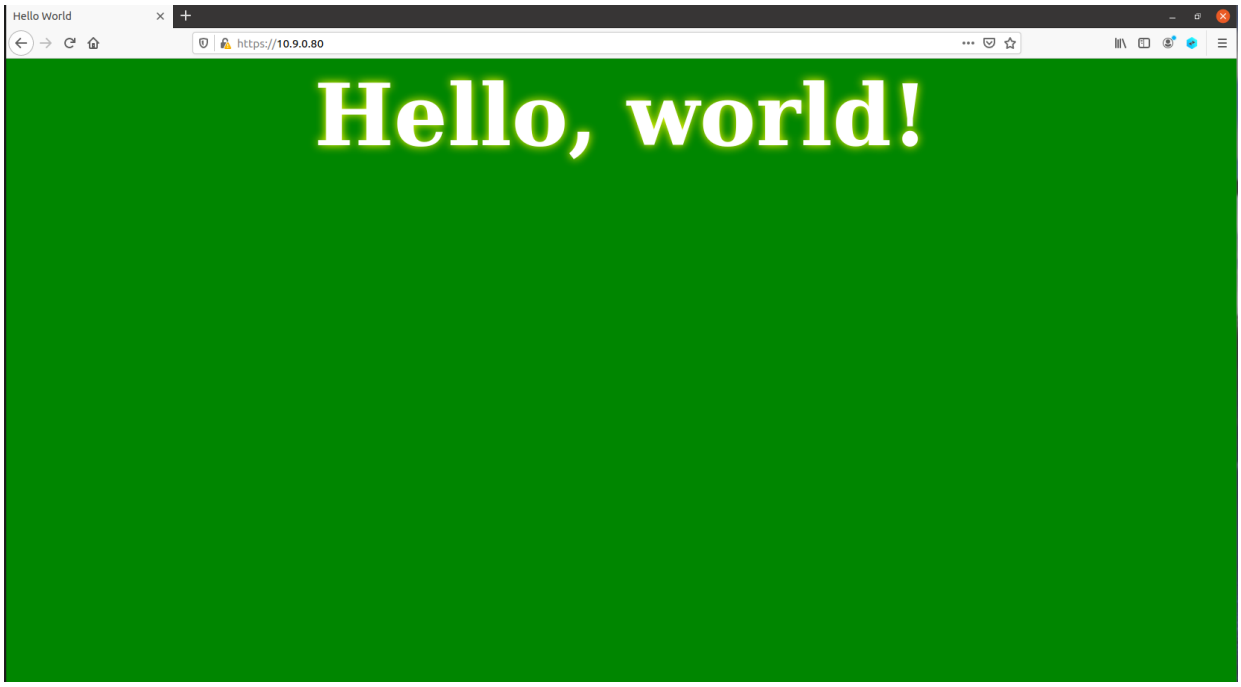
After



Trying to connect to https://10.9.0.80

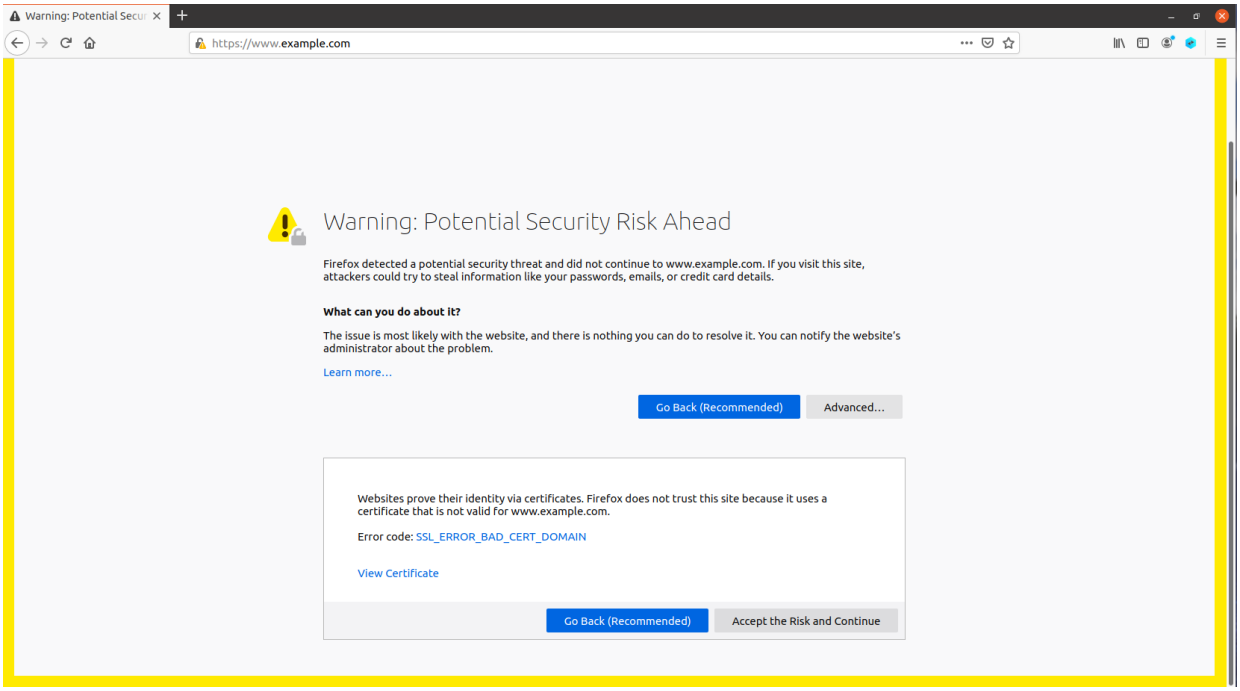


Accepting the risk and proceeding:



Task 5: Launching a Man-In-The-Middle Attack

https://www.example.com on victim machine:



Accepting the risk and proceeding: