HyperionDev

PKI and Man-in-the-middle Attacks

Model Answer

Visit our website

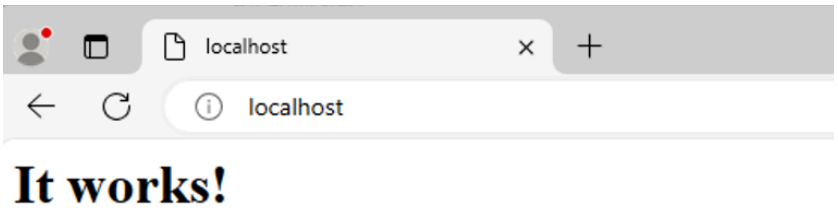
Auto-graded task

Model answers are provided for the following operating systems:

- **Windows**
- **macOS**
- **Ubuntu Linux**

Windows

1. Install the Apache service on your PC. Confirm that it's running, and use your Edge browser to browse to it via the HTTP protocol. Take a screenshot and add it to the **server_hardening** file you just created.



2. Create a certificate authority (CA). Paste the content of this file into the **server_hardening** Google doc.

   C:/Apache/Conf/server.key

```
C:\Apache\conf>type server.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC+COfqAbG8hkEQ
0Tb5+n0SQcztaDvj64M25cBcsuFRe0+jpfCZUyqIcMdhbVm6IgIq9Era/L/vel5Q
pdtIjovLYzC+kuP6GNi1BJPNtpoper5s9yZyUVtO7pSH5Pfx5pO3bjAtOt8jZHQ2
x/A1RVjFk1WLvPBMeKDjg/7HYY5n62WNI26NacjVu+c9jzKj3jimIkH7ZMgu2MSI
BlPVl9/PPQJLSFCgA2UhOTQM2A2GVMQU5FbAJ0DYxU1D2CsJMTsxBfCtX+HywWO9
Ke5KYYccTUne9vE+2xJCIpDjQ4nmg++TCrH4XFKQ3e/KtqrgmLlUheybm0taDnIO
lg4+jdc3AgMBAAECggEAPi1lzB//yoJW2azKgyIdOBMFfQwkxF8zkIu909bHeEST
eyT5QwF+IiRcaBlCSW+FLA7AS0R1fGKaZ2LNC8FwJfzvXvtq0lK83QWBYsaDTF0X
30lCcBcEfB/9wzT8l05tOJA5/SKNDeR5Tc8/Xf6xm/un+s+4BB1X7vkqLIxT7tX6
dacuC/ydEVOMYN1nUQYHmcLi5SZI07idGOdDHqeR4N3PFlzpaHG3vBlRZ+JN8Sdj
x7bLcr5yxxfYtjcuJL2itl1IIuCyI4+rOE2hYTgLt1Z5GVhwG5uUVyJyJoIJBqUJ
fzQCnjIBH2KE68rk0WKRFFiCxkv/wDBiiEe3E5Yj+QKBgQDxnqwvod5aZpWKp5M2
VABIr1lOuwZw4O84LD+yBcolInanfK2iz5oNevf3KnErUfo2+YDjGJEiOF7EKwE5
4dO/aU84C/8fmBlGtuEbAy8Fj0Ot+SAPwI75clZ+2t9Q+c6rOQrZ1OrwDv7XK+6E
N6KipCeai6C8Sl0k3oEpMWyQywKBgQDJWEg8LBbENsSu7wBXTZgvN6RHYe0FFTv/
pMa9P2jdhL+S+erlt+yCjA+UPKZBhFzI1a8Uv4AuoTqRYbbbzvZXHdnc0IBxsZWK
G64m+D33yVlmzAWLJAVloNVIneKAtyaQGWrUFruXbTXBSROept4QBCup3IOW/4zI
2iT4yEDhxQKBgQDVO0//9V1S8Id2xy6+2mEpxD4PojQr+AaFz18jD8L3BLQsWXav
YYE19ljRc05OidlFHOonAK5Mwey4OK+rUmXZ3elAsC2lx0g/RPPiL+wWfvmelmY6
IJjNAZ/d8fD0+JDwQLYXybTQyJsUb7veSW8pE6+zzxe6M/KBsC/Sl8CVAwKBgFKq
H0YtJ8+5WLklwTMW1YOVSapRBzoOBMspwLrUPN6t8OWMHCfigoT6si6/U9cUW+/M
44wWL691XJFx19yZNUSBKgBhzkpfibDhOngfdXm1PjJZU3FUAa8/ADJHOEZ2a6u/
879N8gjyup43vYlmo0daHv8nXRNyqj+QaJuHxDOtAoGBAJ8SmdAuRMSS+JJqSM0T
wxJiPc2r1rGZ1bTk6V4M95XPXq+Vg6l6UztCz187d/m8Fn1Jco3jvMPryaOwL2s7
sxvfpxRiSf2ZZMNHHMI0HOpqT04tvojzymVOPX49+d70uZrSkToY5IegxwqbR/uH
TITY2/TcfxJZwFnev+aGGTDH
-----END PRIVATE KEY-----
```

3. Secure the Apache server. Paste the content of this file into the **server_hardening** Google doc.

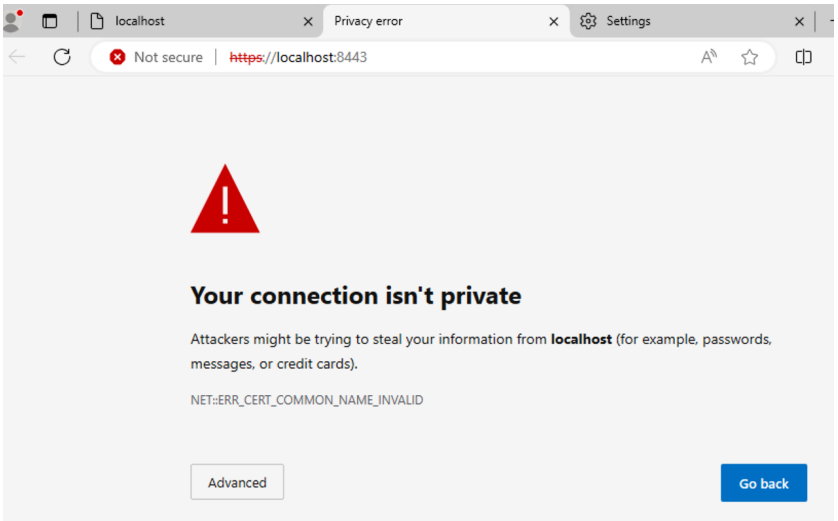
   C:/Apache/Conf/server.crt

```
C:\Apache\conf>type server.crt
-----BEGIN CERTIFICATE-----
MIIC1zCCAb+gAwIBAgIUT8SCPx3yY6RJiG7AI547D7bZfpUwDQYJKoZIhvcNAQEL
BQAwFDESMBAGA1UEAwwJbG9jYWxob3N0MB4XDTI0MDMyMjIxMDU0MFoXDTI1MDMy
MjIxMDU0MFowFDESMBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAvgjn6gGxvIZBENE2+fp9EkHM7Wg74+uDNuXAXLLhUXtP
o6XwmVMqiHDHYW1ZuiICKvRK2vy/73peUKXbSI6Ly2MwvpLj+hjYtQSTzbaaKXq+
bPcmclFbTu6Uh+T38eaTt24wLTrfI2R0NsfwNUVYxZNVi7zwTHig44P+x2GOZ+tl
jSNujWnI1bvnPY8yo944piJB+2TILtjEiAZT1Zffzz0CS0hQoANlITk0DNgNhlTE
FORWwCdA2MVNQ9grCTE7MQXwrV/h8sFjvSnuSmGHHE1J3vbxPtsSQiKQ40OJ5oPv
kwqx+FxSkN3vyraq4Ji5VIXsm5tLWg5yDpYOPo3XNwIDAQABoyEwHzAdBgNVHQ4E
FgQUirLNYBILqLBV6Qpu1+OP6uwjutAwDQYJKoZIhvcNAQELBQADggEBAD+cFIoN
QPaIvMSSvhCGn7Mp/bRGrrIukg7FZatMJpCZwDUym++6qJwASeIEST8ey43qSAEH
9vuyYAdx3VixZHsoVrs3Jy8s7nA594ivKYGnspLtPBxo4uOvF3pmrqPoZCpM2W5S
Cccy2C7xm3v6OtAm94HThxV/y/0JPTU1ipnEGIN8tuf2Hg+FyWwaXQ6jZCUoHl7h
PhSs0O/qtlL/QtOwLHSM7ygDkNDOaaxOlfaAPDj83RFOG9XaWbIGpcF/kWRMQ2Fz
fpoVbr7E7RS4qDvSOXR4aIJTEdVQldhKTWLpbCxdk7bNt69wCOTFyk0BHUa8VB46
lUTXtk+ZBvoPqPY=
-----END CERTIFICATE-----
```

4. Browse to your Apache web server using the browser that is appropriate for your operating system (Windows: Edge; Mac: Safari; Linux: Chrome or Chromium) and using an SSL connection.

   https://localhost:44

   Did you receive a warning message? If so, take a screenshot and paste it into the server_hardening Google doc.

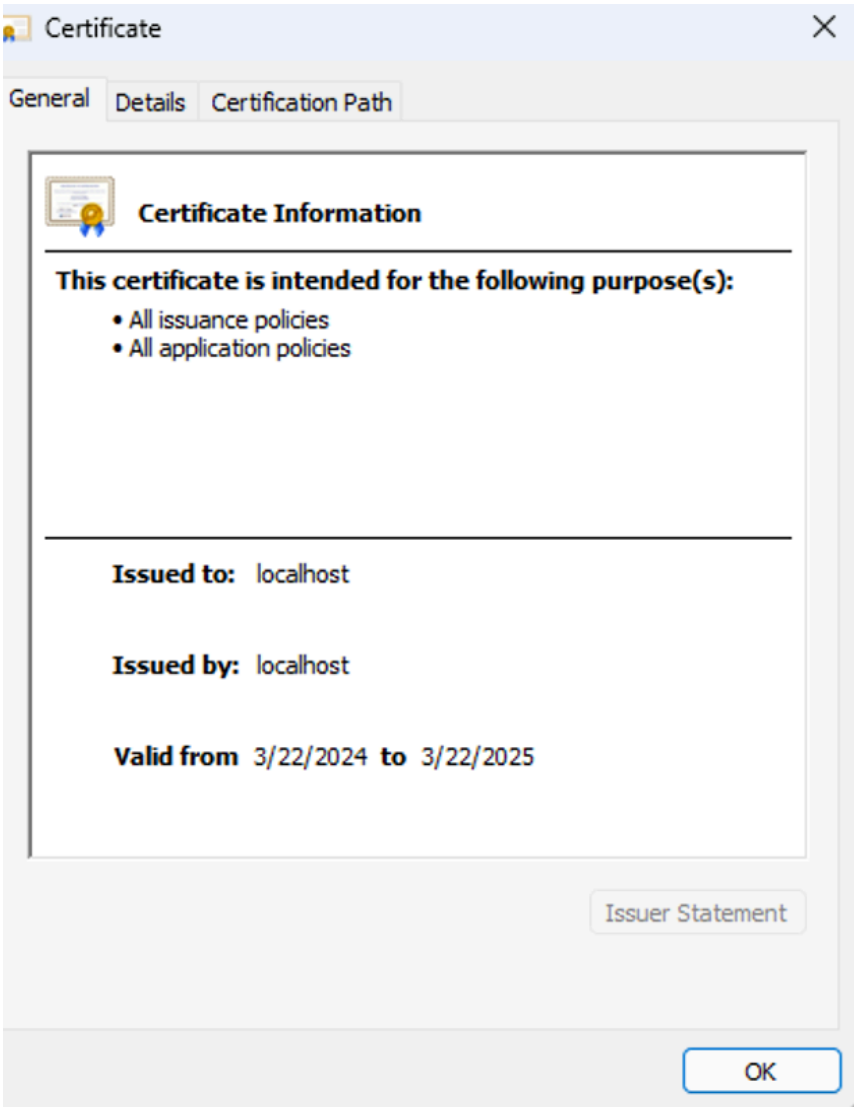


5. Install the self-signed certificate into your Microsoft Certificate Manager's "Trusted Root Certificate Authorities" folder. Bring up another Edge web browser instance and navigate to the Apache web server using an SSL connection. The warning should be gone. Take a snapshot of what you see in your browser and paste it into the **server_hardening** Google doc.

   https://localhost:8443 should show the following since the self-signed certificate is now in Microsoft Certificate Manager and recognised by the browser:

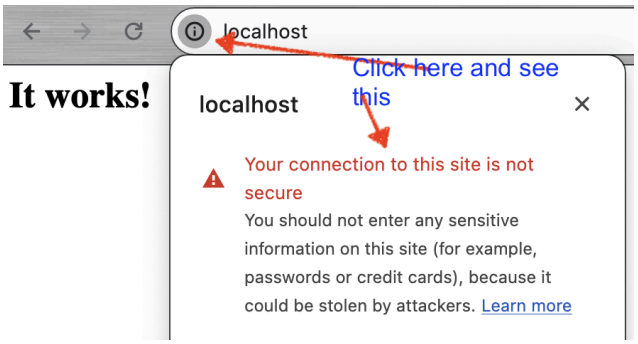
6. Certificate Analysis: Certificate name is set at the time of the CA private key creation, using 'CN=localhost'

   Certificate expiration will vary, but it should have a one-year duration.



macOS

1. Confirm the Apache web server on your Mac is running by browsing to it using the HTTP protocol. Take a screenshot and add it to the **server_hardening** file you just created.



2. Create a CA. Paste the content of this file into the **server_hardening** Google doc..

   /etc/private/apache2/server.key

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCiNf5Vhco79HlG
KotPH2MbyqweUDYVirhdqgjqxASUWH/XkQ8W6HRKmx7Vyc1U83fTRHJubC4280Eu
enKXO0nQa1gTFy0oQtKe8V+yWoB8K0l6HsKtggsz71t2sIbCM7N/kfaTedVJ4lRJ
fN4XL1iqtM7cqGa3bOlWE7phiH3jkAYQO02mrLDnB0UaMzKibJ8Ul7JV1VAKD2vg
xfBzXo9FbHrD7IsREC9QVgbbRp3i7clROTplyBeRg3xaGpxbJZHr3JlI/T2oZz9r
i2vVoVz0vgJF42ORRv5S06AhBQDjqea97trvteqjSNkTWDlPjRRMLTa93wO1WWxw
TNBVe2EvAgMBAAECggEAbsVUY26zxfGTB5lx/JxAf/ANTb4U0O0kLcI5yKgHQI6W
7sx+c3RWRcRccD4Y3BRPFZS+WC3D+X5wWp7/tcqlA5DqWk8PZVkMn8HRSeiHqUOe
L6jl5LrTj6m62fh+bgwEXe99ZQRj5MqMKIr+1vJcKGbEhObzDftv9HoQYx5kaYsQ
ZkUdZKiq+oOPDhROUiiRvDHT6YxR/Ip4W0rb/pT2zQc/od9ow6RLGnxNux75l9Ai
wY2hxg0Nb3jr0G6/XTPoguCyGKxjq/QrZsGG9H9/sYCYx92CRW8iNYK4scS7DmQr
KFo/9UECGSdMQ6451WslesY2oNe1VmlrD0F2ZGR5wQKBgQDM8d08F3NnvNzfrepf
VuATLd+qWKgcG2goBJcIAuZ4W2YBrDigXep+wnIw3HGmA8Jeb5keO+HSX4J9HCZ9
nJCnB/aPHBxsNDypxBeMMoomaVjCZSyId4aCq/B/z1Oc7peE9A3MRqj0TmqALPw2
hMIRapNHMLXkgeSBBtwpbXYiPwKBgQDKntJ23WI4qTf9YBe+fnQNqhZykg8+StBg
XuegnsYmfAa+ahzmpNc9OE7wXmCdup6Ms2GmVIhnybBkg/E3JZ4MbcJLbEzwS382
Wdj/B3cmhbgtw98gAA9yNb+jH/oCRgFK8HWS3hUZmeFHgUUcNAEG/SDjn+LyKOeI
HhRmNlAlEQKBgQCVK/7R/Ge9vFQwY1BSsNNMYnmIbht+ydwYNK8R37qNJEmtMgPN
hk5mkXW4Ztw58EaLokMbJI8MJwS9t720dD89tKgcJmPxxlvZXaeeHjM8HjXC2Q1/
DzDS7/+PqAK+GVQkK9fXNh9II8OVJCk4LY1sS9yDVssuVfVSjQG3DbuM1QKBgBvR
rofPYXryENPi65+l8P0nSymz0A/3aaCxpw+wfPgvsyVVoF4yZ7LqFjx+WLmPM9GR
l2ik1o2ZbXR/gRDXQ1nlf/WnCvE7DF5D+70YI03QsjbmW64jE/vUUVluPH8vaWIG
nb3qa+81525P21NB+JojCu71ts0UvKU9rANUlbBhAoGBAJR3C6FwVmBOw+4Yr028
GD1jJtOY2u12fYQIsUgWxcG56EknguJF+zoTT4CXSdiowf81rILQvNqtWQoIi5M5
hmDvmT4Lqry99esq4DwYff99xkmj+GdFlr+sVRLdxz1RPaqe51rp5RvC3NvFzM+z
4v4GjfHYyhTTmsgjXCQh7btj
-----END PRIVATE KEY-----
```

3. Secure the Apache server. Paste the content of this file into the **server_hardening** Google doc.

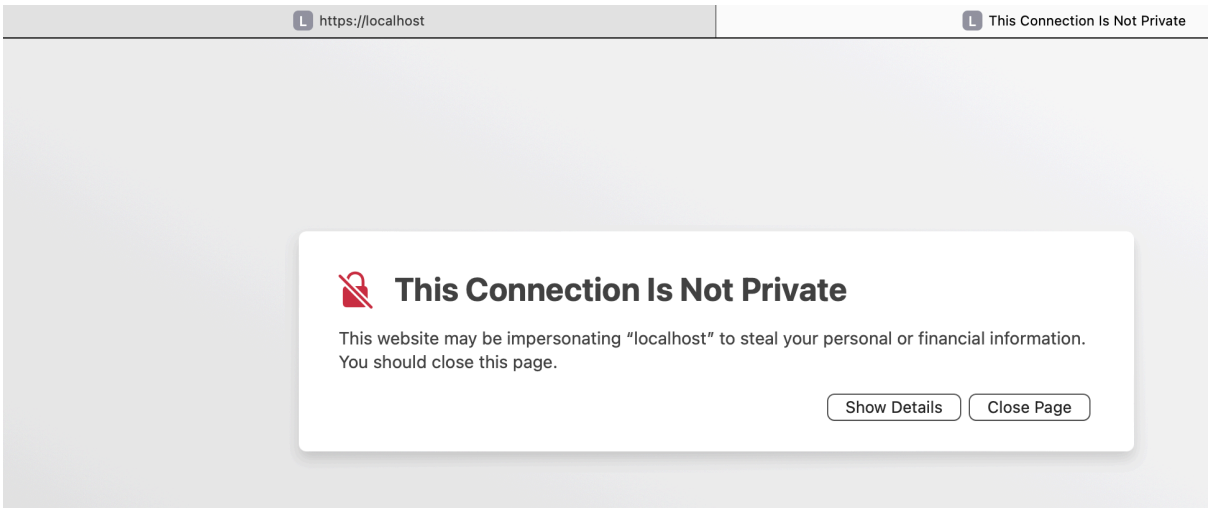
   /etc/private/apache2/server.crt

```
-----BEGIN CERTIFICATE-----
MIICpDCCAYwCCQCGDJHlyE3umTANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjQwMzE0MjIyMzU0WhcNMjUwMzE0MjIyMzU0WjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCi
Nf5Vhco79HlGKotPH2MbyqweUDYVirhdqgjqxASUWH/XkQ8W6HRKmx7Vyc1U83fT
RHJubC4280EuenKXO0nQa1gTFy0oQtKe8V+yWoB8K0l6HsKtggsz71t2sIbCM7N/
kfaTedVJ4lRJfN4XL1iqtM7cqGa3bOlWE7phiH3jkAYQO02mrLDnB0UaMzKibJ8U
l7JV1VAKD2vgxfBzXo9FbHrD7IsREC9QVgbbRp3i7clROTplyBeRg3xaGpxbJZHr
3JlI/T2oZz9ri2vVoVz0vgJF42ORRv5S06AhBQDjqea97trvteqjSNkTWDlPjRRM
LTa93wO1WWxwTNBVe2EvAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAAPm6E4pHLDD
PldtKr7F2jU/opZIseH/l3HRcg0G+QyiaZISaWY3v7mSdU/1ZoY2BmUHiIx+9+l3
VowqcK24LBQ/TBys3Vw8TBBEpRvCqUSbC15ybYvdCZ2YA+STJfH4FCHtwda3pXeo
lXXhBIGGvBzyJ2Qph2tENuvy7VQBBqQfeSwqUF8EXcjJj21P7+UT1oFQleLbPP6f
4iymL/Zuw8lNaJ6H9ao4oMxnWohqpewu0/3+w0yBggXqtNou8foswa9jrnZKMZVA
/j0v2EJY8QgD7NbJlPWLBPCXgIBTNhgVEBtfJ/7wFdbVRj8zRf1B1FiWT1BoU80p
/vLn2+hgWNM=
-----END CERTIFICATE-----
```

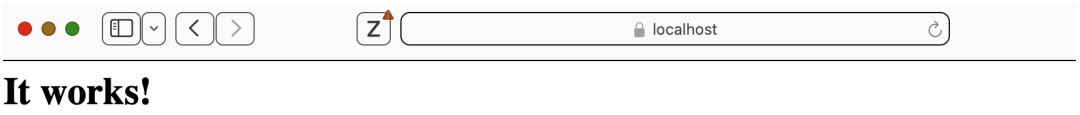
4. Browse to your Apache web server using the browser that is appropriate for your operating system (Windows: Edge; Mac: Safari; Linux: Chrome or Chromium) and using an SSL connection.

   https://localhost:44

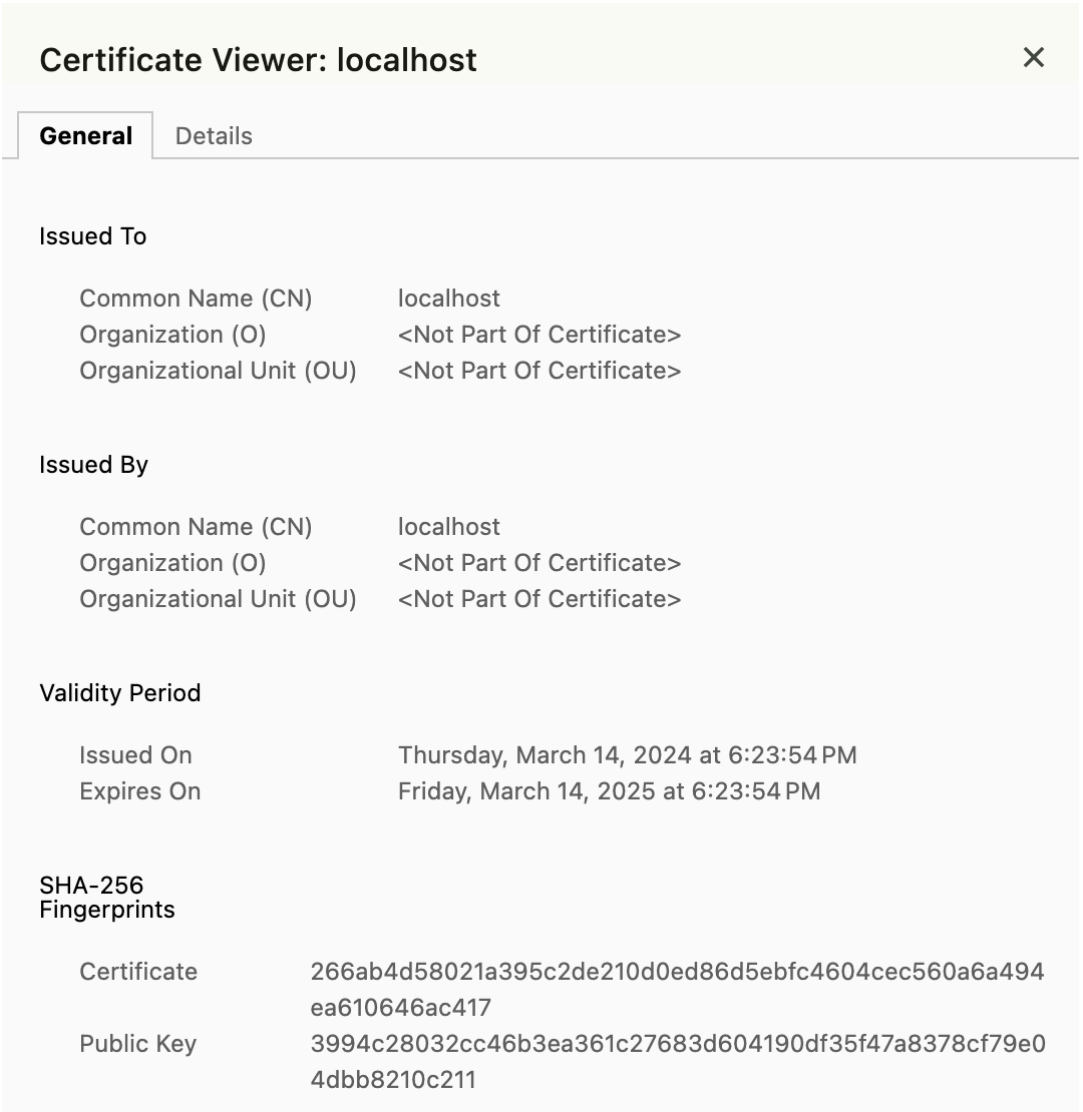
   Do you receive a warning message? If so, take a screenshot and paste it into the server_hardening Google doc.



5. Install the self-signed certificate into your Mac's Keychain. Bring up another Safari web browser instance and navigate to the Apache web server using an SSL connection. The warning should be gone. Take a snapshot of what you see in your browser and paste it into the **server_hardening** Google doc.



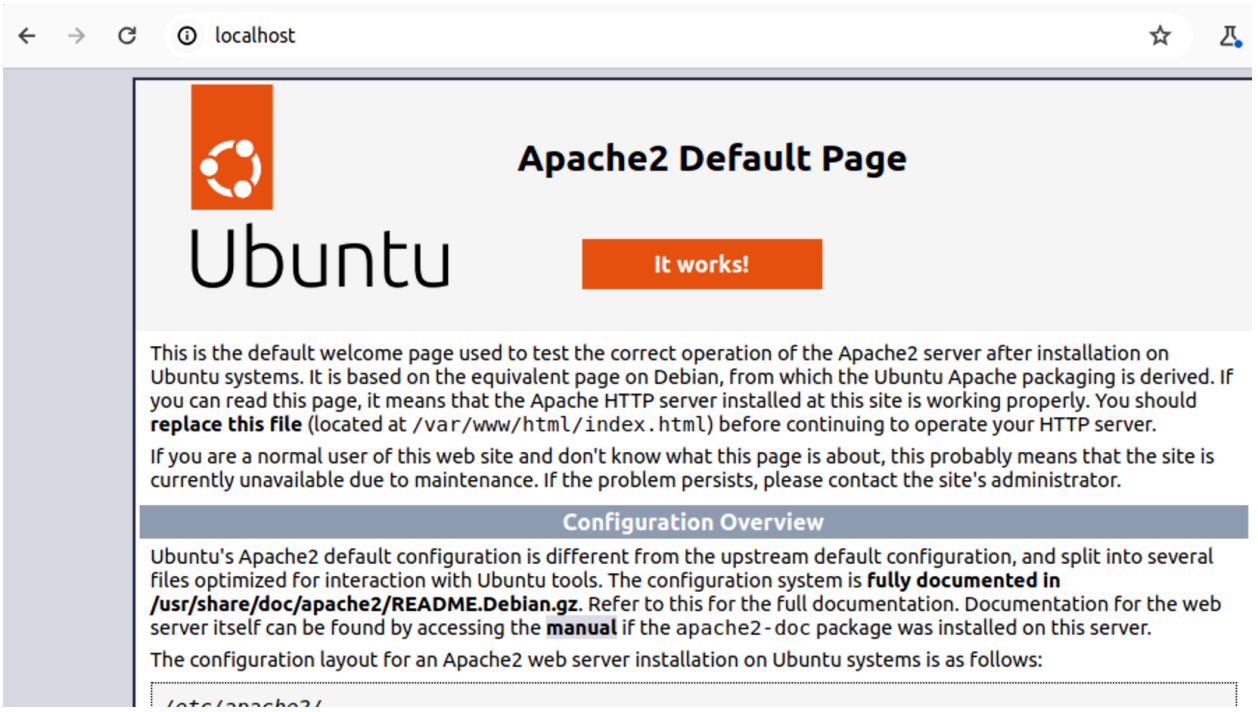
6. The certificate name is set at the time of the CA private key creation, using 'CN=localhost' Certificate expiration will vary based on when the certificate was created and what value was given for the '-days' parameter when the certificate was created.



Ubuntu Linux

Note: The screenshots are outputs from a Chromium-based browser. Chrome-based browsers could produce slightly different formats.

1. Install the Chrome browser on Ubuntu if you do not already have it installed (if this is not possible based on your system architecture – i.e., your system uses ARM architecture – install the Chromium browser instead). Then, install the Apache server on Ubuntu. Confirm that it's running by browsing to it via the HTTP protocol. Take a screenshot and add it to the **server_hardening** file you just created.



2. Create a CA. Paste the content of this file into the **server_hardening** Google doc. Type out its contents.

   /etc/apache2/server.key

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCfg3iDLk/5A6tv
/wJ7ZYESYYoBkliiYU4whw0Ni3c7envqmQUfAP03oDVFM8HA5CdM9sezQ6G6qyJT
5JthUSi4c+OgIgzt/4OmpC59CmZbt4yS7Th9U86LtUg5HTMQkR2bRAjAQqdvaRTx
EhyQEr+u5znDzopnCsP/mrcQpBsEqvtveUBfGtJXGr5wqr2FpJ9Sved5F6w/gTim
uRAEiv0s4oJnhO151jP3jjE7w1+9meHEaq/0ufAeXsugtueVE4iRfMFXAwFtWXSt
zDj6rn7YWrs5ODMALqrpXx7wx+eFgV1VHfmPYqMXDATNJZLOJZjkhi6Rj2EQHg8j
/nVQFGxZAgMBAAECggEAEbU3Pc3Yfi76e02CjacOKfeWydegnA8kDlZRvEMTJpDR
fJDF7SQPmDsiasck/1g8pio/r16Gz9mTbx+B4c7wD7D60CIzkACIcVyI1iP/SreA
xSdNRfl1pJQIe2Gq03AeqqfF9mz32DIAy4XMkrBoI98iriJpwihja4bWA4SKRM1W
+s3pfkRzTetGGX/ypDO5u7+O8oRbOOU5MEgZngaKKSbq7yEBXtlalJ++m10APxyb
yrKu4AGvcvxpu4VMpOKbzLasowm1CnNWCMYQUSC7inYHxWvNaJP5xJ4hZa72P0vb
QRJU0m4sCvuAP3QXvvNvWjjQJW2MejWqlH1k4YKkUQKBgQDVgT76W2nSjzvcaPoC
wz3pUkhmjMQP4hjx0Y9nBuDtHt1JczpdPRDUin3rHQDC2OAyMaUz1tPtFzv1gMFI
WPaH+q0db0XqvDUAwOwbDKxlgKI5PqhKTqs6CspqK8WiYO1aYPCVA1o7DCRi9icw
Y024y0zabqiAqFbpgjzaXqWeMQKBgQC/QzH/mTnKjTBYUvsAFOga9YuLv9W84LXS
aCkGofzDfm+yJWbJuIVVpQ+z6eD9Hh7o2gfgR3zUf/7oMh+sd65C/3wvl0VhCXUw
vGNyDRgmqbnzdqtO5PhQ8C2UrBVtdDQAYz8/5i2gaVP96KDJzfjvr3IHVhID183y
Dh261/leqQKBgGgSqmpLaRgUbe+Q1F3IYkN7soMalu/PHK2zox1rgvTTGLcXDhop
DC0unRageqCAKzkMbiUI0SE/NCEF9DGZ/AJotT4l4YT83TFS2USONvL7cxhIbKxc
EKcoX2bFk38FlG1714orqi4iSxJaPtwda+NqZjoLuu0MK2GD9LnVbRHhAoGBALoV
04h+eRbURaw5mBIdRTItosamL3tkGiMLypa0dityUZQ/BYHP8JJCVUPTkl5StvoQ
X8dbZl2N5uHdGqn/i2GOFzJqeEsQG5/+OrcVfGDpk40H8WaCKgL9mytiPjrO62VR
KpGuDshakiig9AdESiZRSZ1PpZltluchytUmGm55AoGABYcBUE49OYN93+BhnwjX
uiModeXZEQYs3M3xb4DmP+QztXvijuZUjWTz/ZVWWXFaxrfuAIYYBxkpK6T6RzuO
U6LTT9P0EZngmjuWIo1uycIxxMUJOucioSGWj6PmhyVOhT0OXZbFQHH10Dx5f8bW
cl3N3RD2bmyUlCMeHKgFPsg=
-----END PRIVATE KEY-----
```

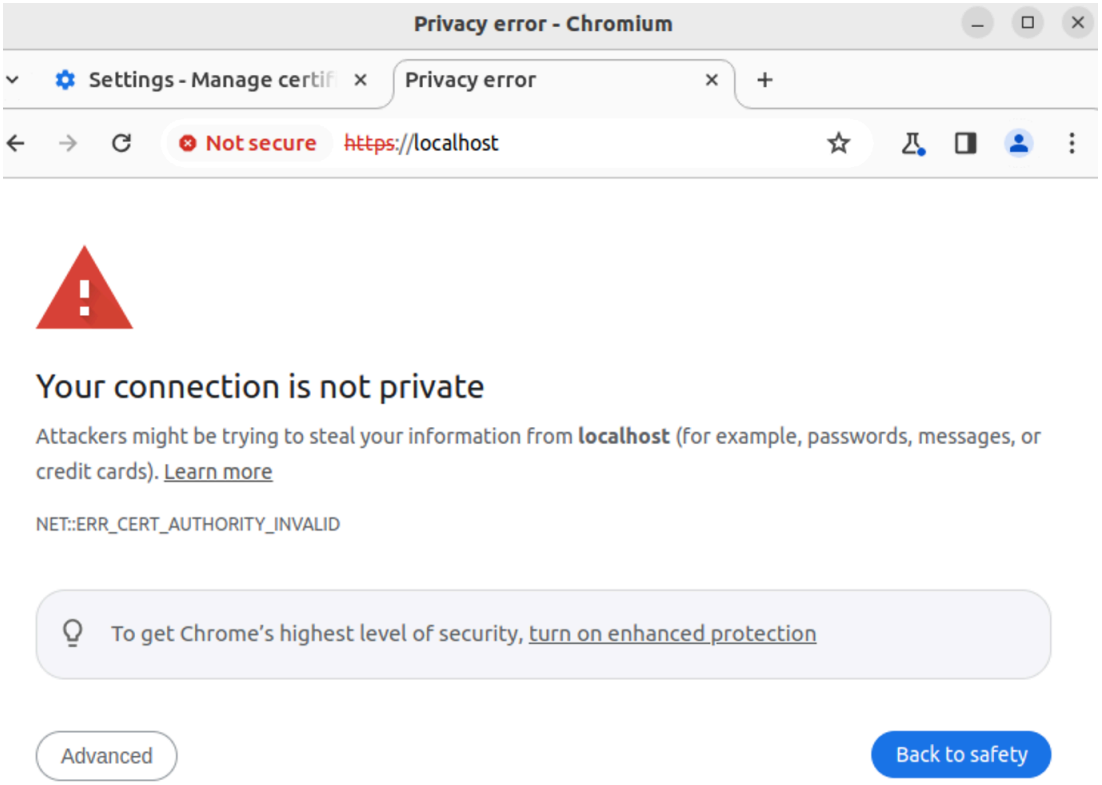
3. Secure the Apache server. Paste the content of this file into the **server_hardening** Google doc.

   /etc/apache2/server.crt

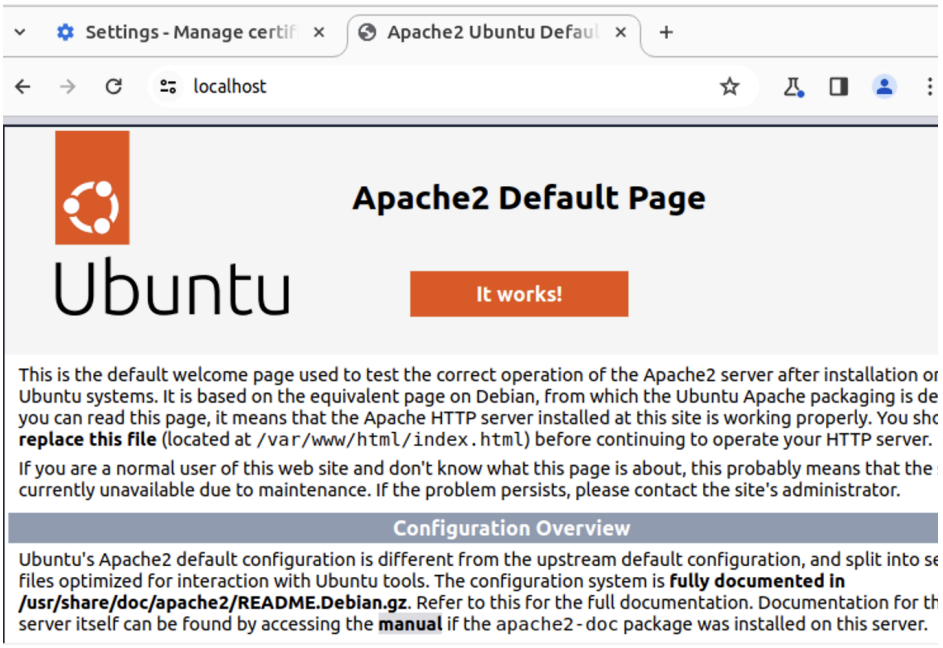
```
-----BEGIN CERTIFICATE-----
MIICrzCCAZcCFGw08XLVEmpr/2Zx6bOlzVjC/sV1MA0GCSqGSIb3DQEBCwUAMBQx
EjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0yNDAzMjUxODEyNDVaFw0yNTAzMjUxODEy
NDVaMBQxEjAQBgNVBAMMCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAJ+DeIMuT/kDq2//AntlgRJhigGSWKJhTjCHDQ2Ldzt6e+qZBR8A
/TegNUUzwcDkJ0z2x7NDobqrIlPkm2FRKLhz46AiDO3/g6akLn0KZlu3jJLtOH1T
zoulSDkdMxCRHZtECMBCp29pFPESHJASv67nOcPOimcKw/+atxCkGwSq+295QF8a
0lcavnCqvYWkn1K953kXrD+B0Ka5EASK/SzigmeE7XnWM/eOMTvDX72Z4cRqr/S5
8B5ey6C255UTiJF8wVcDAW1ZdK3MOPqufthauzk4MwAuqulfHvDH54WBXVUd+Y9i
oxcMBM0lks4lmOSGLpGPYRAeDyP+dVAUbFkCAwEAATANBgkqhkiG9w0BAQsFAAOC
AQEAM4BSXCekpIB0y97gtTc/WjCuk1tkUz1ufEq9zQqUzXzP80GOOeLznbYh51Ib
MWBlkqq+EQi+M1QEdxwBb3m62ST7Qp1WGCe/dG2zNuDqG37ELwNe7zzsGR+YUGPZ
1srNAZVPPXyuOclRFTsljwR1FtquJPIOZPJ9wILWwzW3r0bSf05IO3flfuBWSA0m
AgWn8h4MkmCE4hkEwWDfPBocwyAQqY1OYwJr12waavor7m7XJMSYqtw/LRhxCC7M
fZ1QDP9j0z5YCO/8Wq5yZMssViMHTjvgl6VNmJIiVNmCD1TGbZuqTetKX6ak+4tR
OHN2Ih3Ekiwf8V39K+xveGncDw==
-----END CERTIFICATE-----
```

4. Browse to your Apache web server using the browser that is appropriate for your operating system (Windows: Edge; Mac: Safari; Linux: Chrome or Chromium) and using an SSL connection.

   Do you receive a warning message? If so, take a screenshot and paste it into the **server_hardening** Google doc.



5. Add Apache's web certificate to the Chrome or Chromium database and then browse to your Apache web server's SSL service by using an SSL connection. The warning should be gone. Take a screenshot and place it in your **server_hardening** Google doc.



6. Certificate name is set at the time of the CA private key creation, using 'CN=localhost'

   Expiration date will vary, but it should have a 1-year validity. This is based on the value specified for the '-days' parameter in the command that was issued for key creation.

   All of this is shown in the certificate contents: