



PKI and Man-in-the-middle Attacks

Model Answer

[](http://www.hyperiondev.com/portal/)

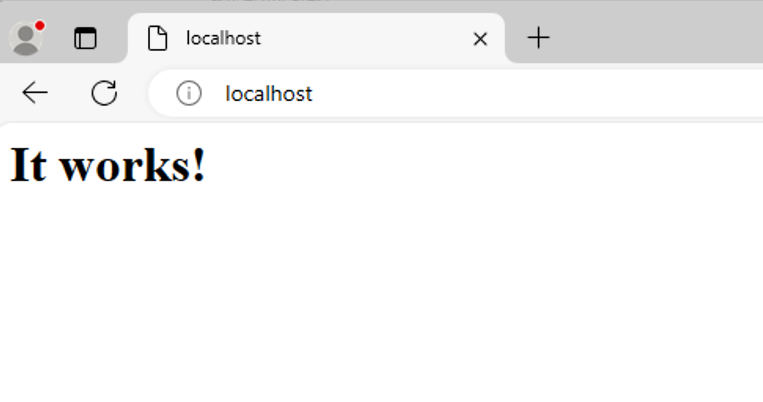
# Auto-graded task

Model answers are provided for the following operating systems:

* [**Windows**](#_o4odmvoyzxtf)
* [**macOS**](#_yo7bh0seqz9h)
* [**Ubuntu Linux**](#_z6jwo3193uy3)

## 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.



1. Create a certificate authority (CA). Paste the content of this file into the **server\_hardening** Google doc.

C:/Apache/Conf/server.key



1. Secure the Apache server. Paste the content of this file into the **server\_hardening** Google doc.

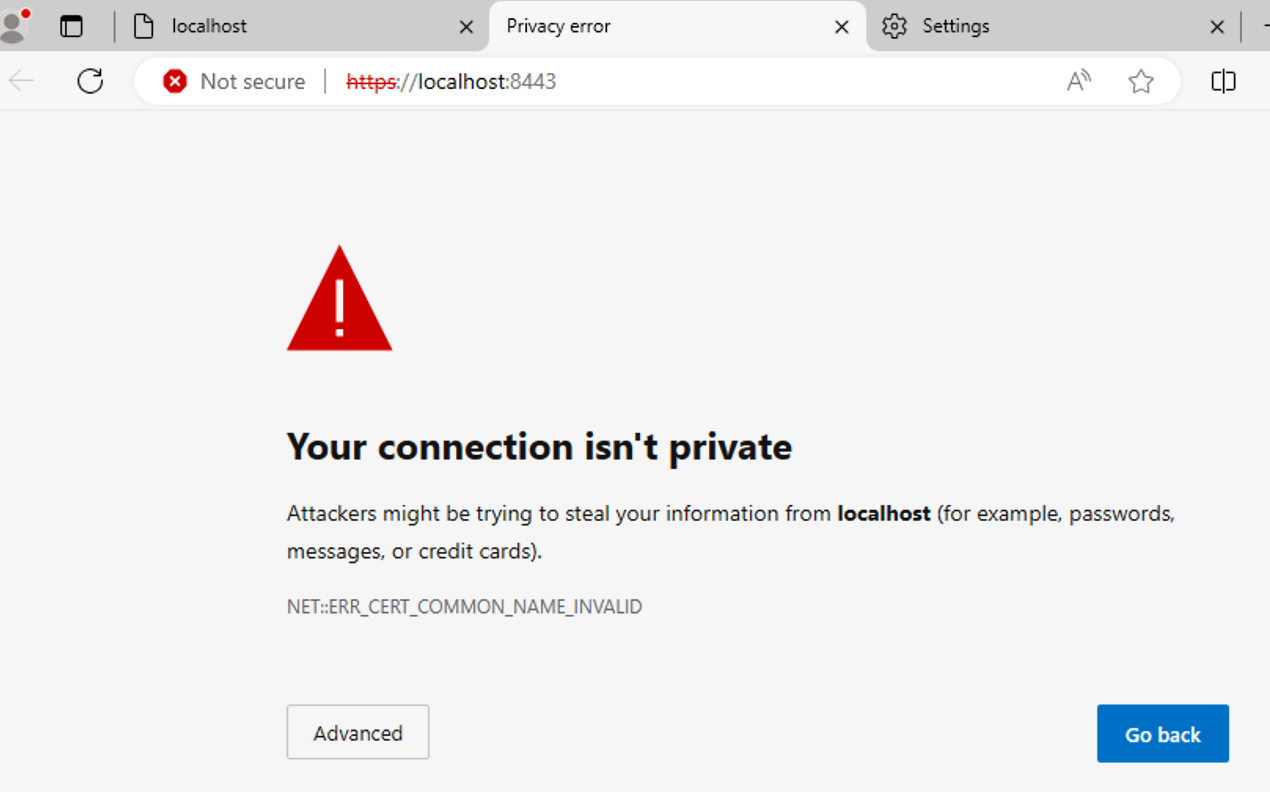
C:/Apache/Conf/server.crt



1. 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.

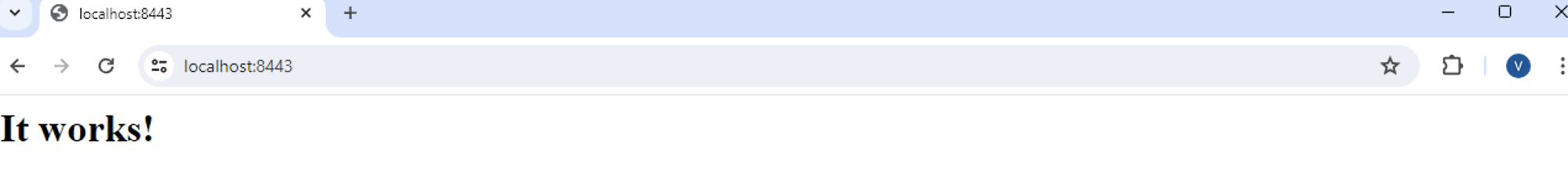
[**https://localhost:44**](https://localhost:443)

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



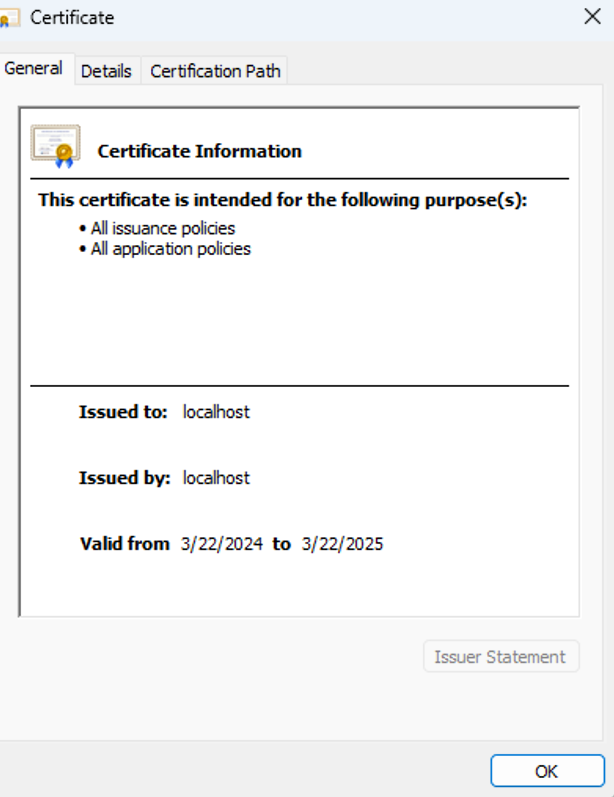
1. Install the self-signed certificate into your Microsoft Certificate Manager’s “Trusted Root Certificate Authorities” folder. Bring up another Edge web browser instance and navigate to the Apache web server using an SSL connection. The warning should be gone. Take a snapshot of what you see in your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

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



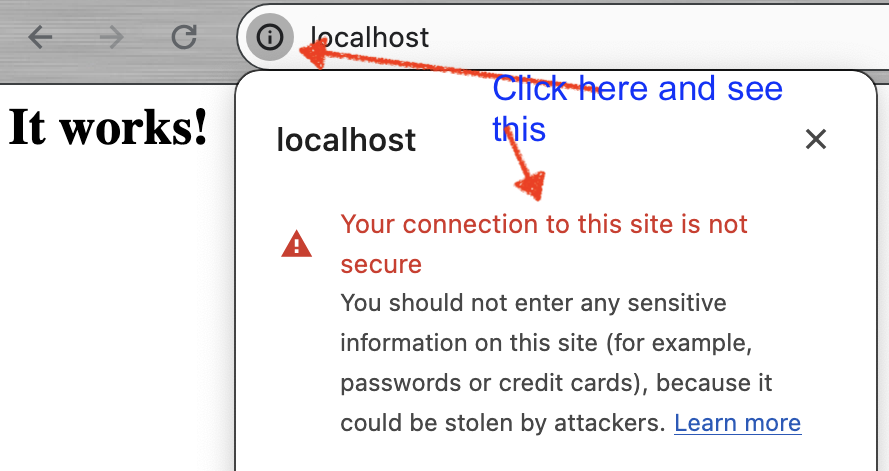
1. Certificate Analysis: Certificate name is set at the time of the CA private key creation, using ‘CN=localhost’

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.



1. Create a CA. Paste the content of this file into the **server\_hardening** Google doc..

/etc/private/apache2/server.key



1. Secure the Apache server. Paste the content of this file into the **server\_hardening** Google doc.

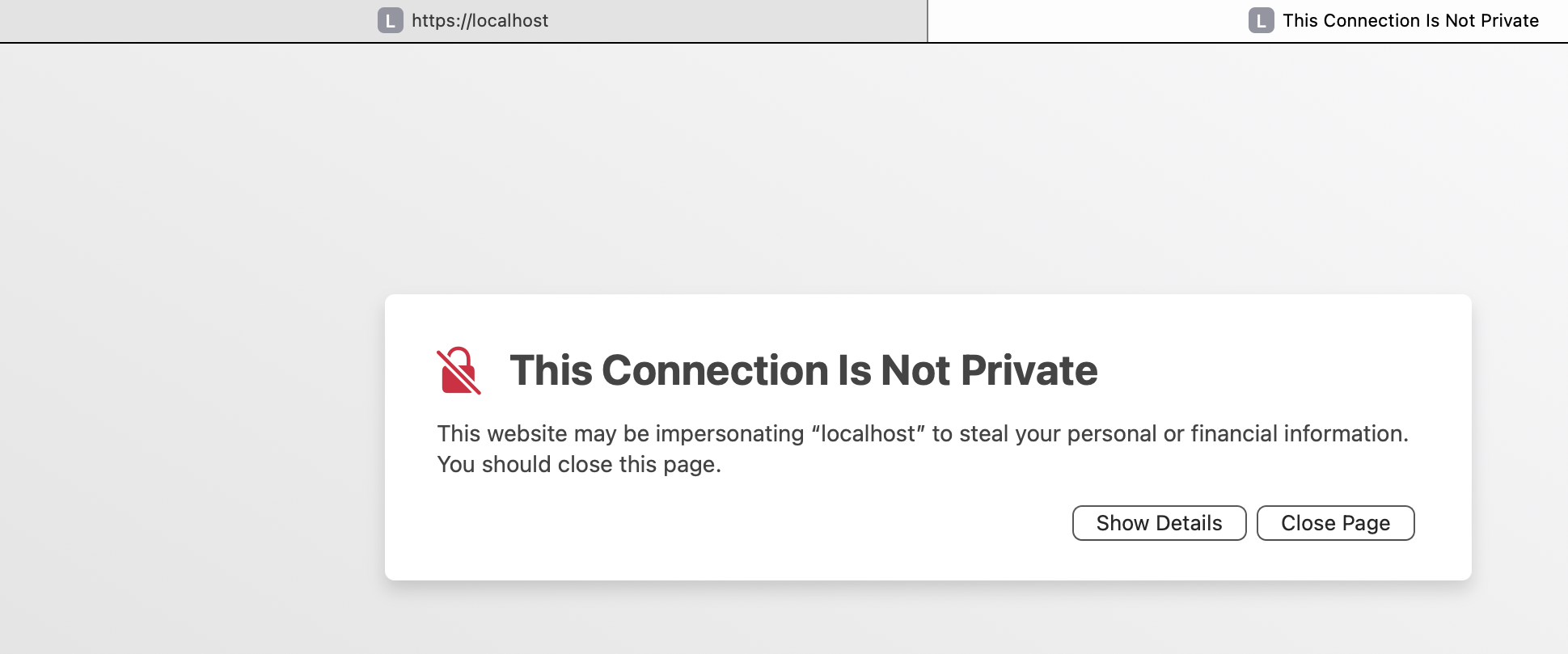
/etc/private/apache2/server.crt



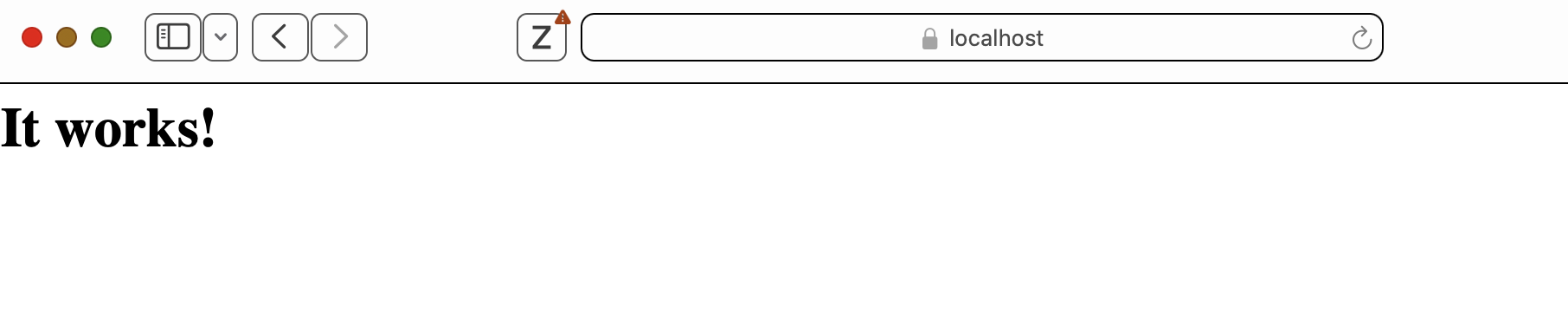
1. Browse to your Apache web server using the browser that is appropriate for your operating system (Windows: Edge; Mac: Safari; Linux: Chrome or Chromium) and using an SSL connection.

[**https://localhost:44**](https://localhost:443)

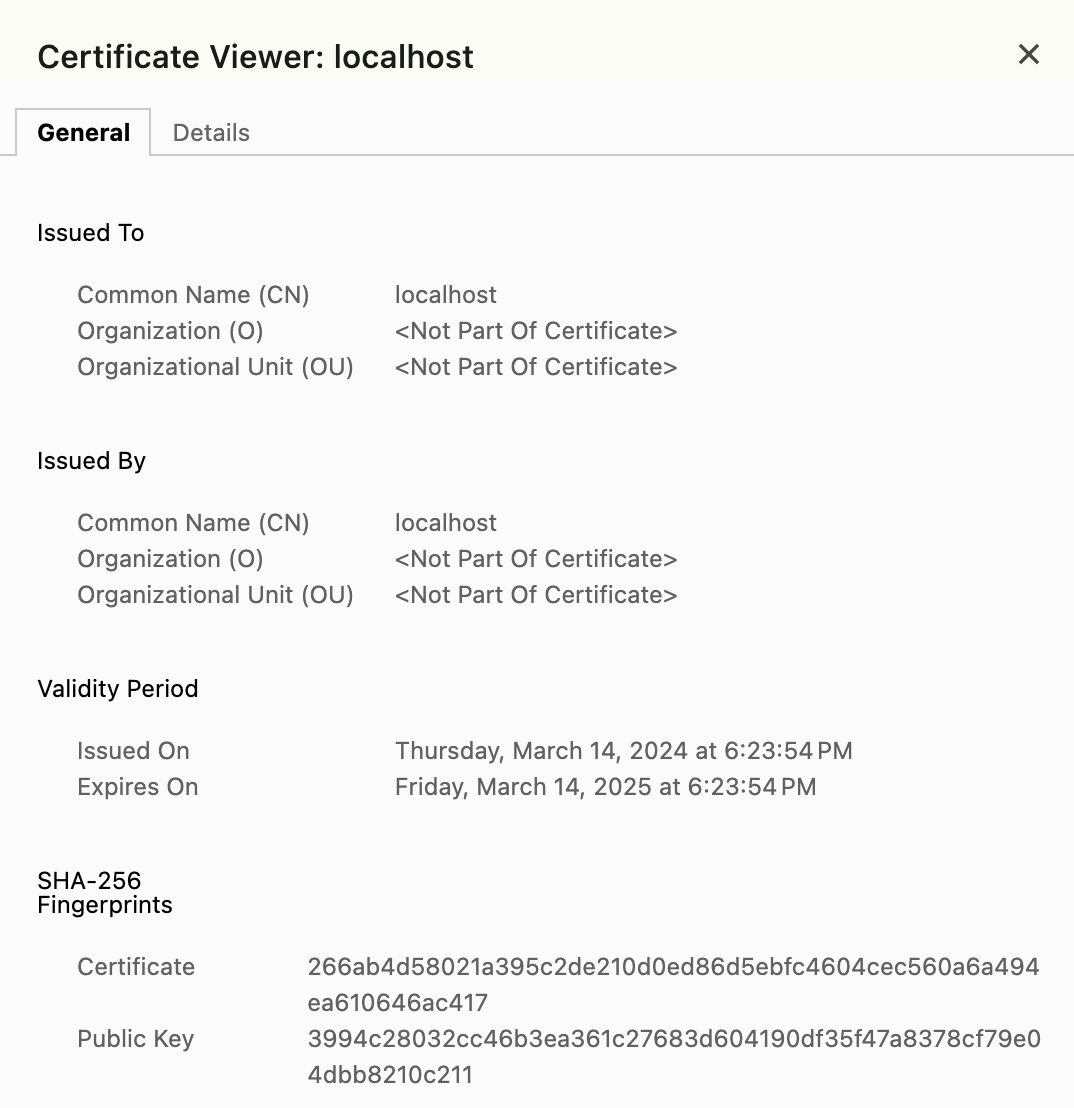
Do you receive a warning message? If so, take a screenshot and paste it into the server\_hardening Google doc.



1. 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.



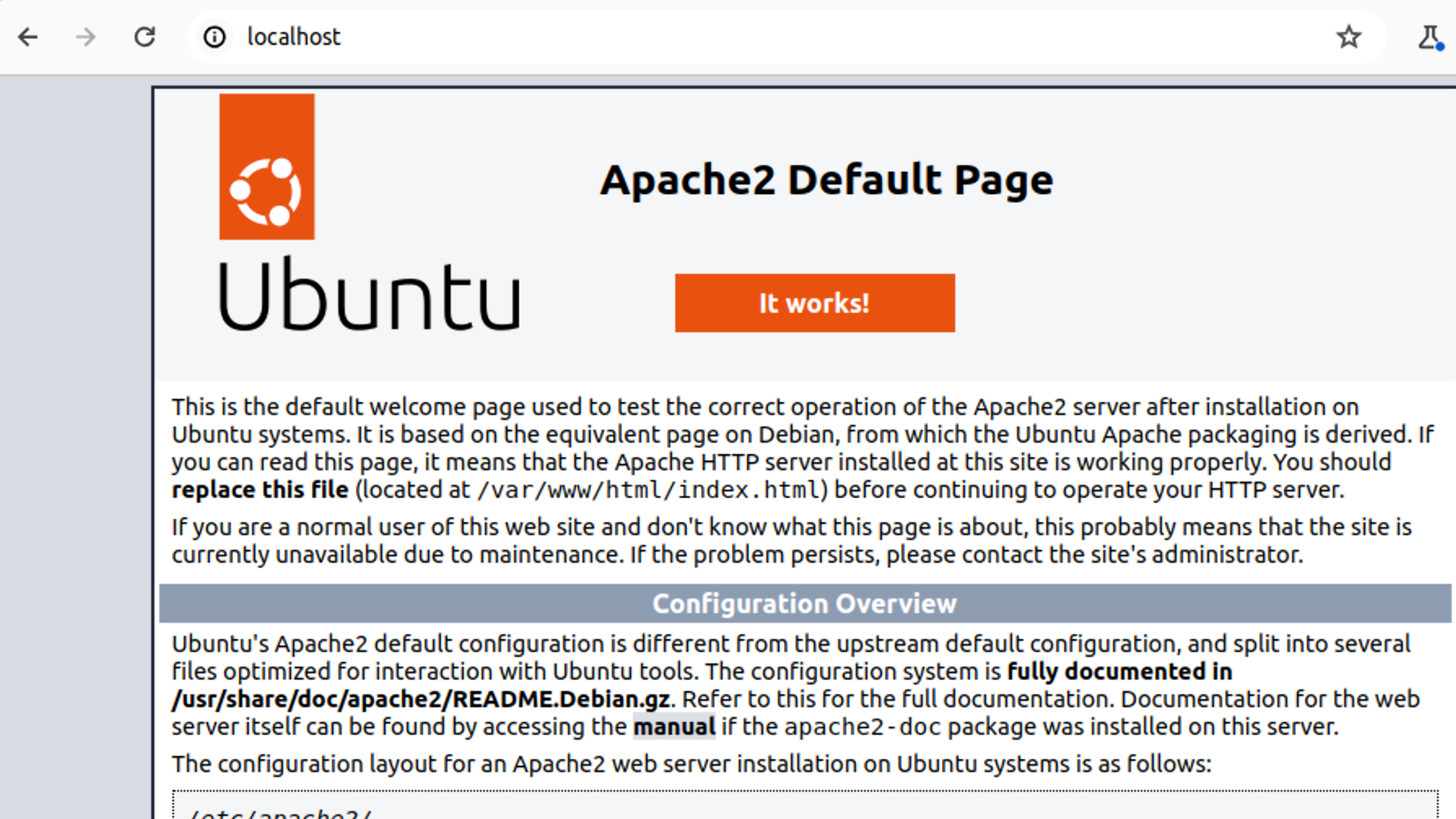
1. The certificate name is set at the time of the CA private key creation, using ‘CN=localhost’ Certificate expiration will vary based on when the certificate was created and what value was given for the ‘-days’ parameter when the certificate was created.



## 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.



1. Create a CA. Paste the content of this file into the **server\_hardening** Google doc. Type out its contents.

/etc/apache2/server.key



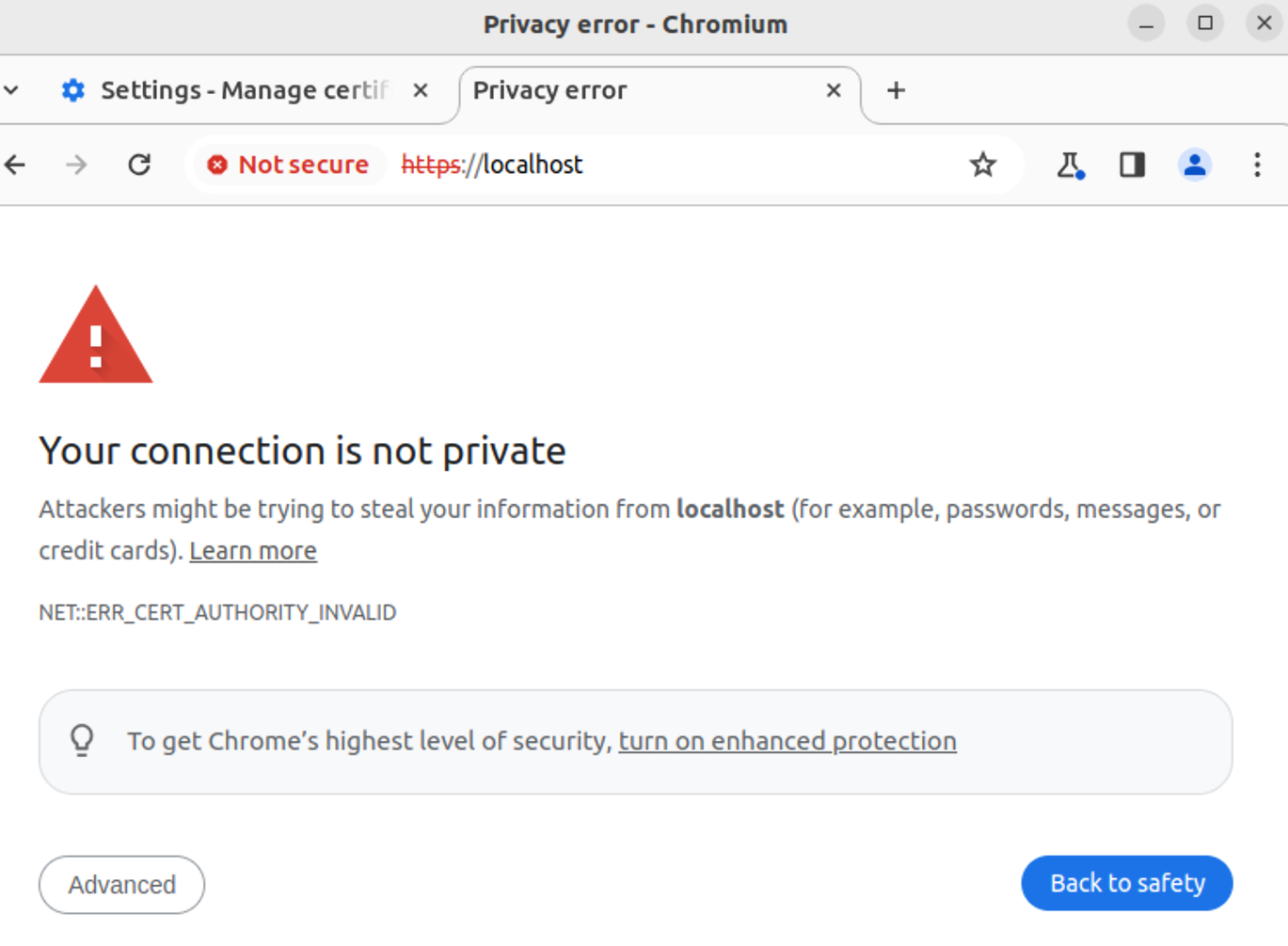
1. Secure the Apache server. Paste the content of this file into the **server\_hardening** Google doc.

/etc/apache2/server.crt

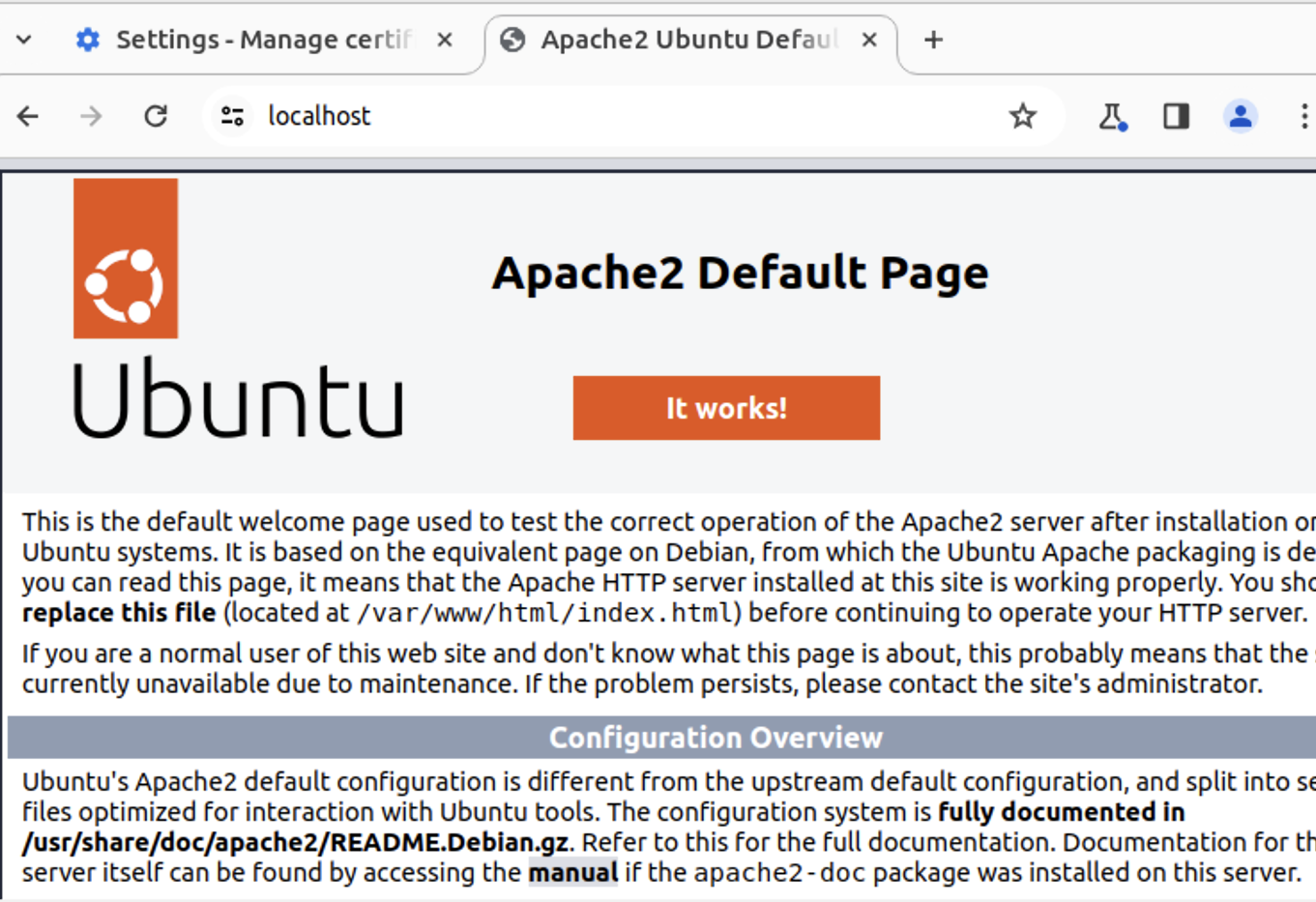


1. Browse to your Apache web server using the browser that is appropriate for your operating system (Windows: Edge; Mac: Safari; Linux: Chrome or Chromium) and using an SSL connection.

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



1. 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.



1. 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:

