Task 1:

1. **mkdir CMSC23206Lab1**
2. **cd CMSC23206Lab1**
3. **echo "hello world" > index.html**
4. **python3 -m http.server 8080**

Task 2:

I used Wireshark and a loopback capture filter with an HTTP display filter to display the local web server's traffic.

Since my web server is unencrypted, anyone with access to the network can "sniff" the traffic using technologies like Wireshark to see the GET request for "hello world." This can become dangerous as sensitive data, like login credentials, personal information, or API tokens, can also be included in these packets and be intercepted.

Task 3:

I created the certificate for myself using **openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes** to get the cert.pem and key.pem and started the HTTPS server using them with **python3 -m http.server 8443 --bind 127.0.0.1 --directory . --certfile cert.pem --keyfile key.pem**. Since this is a local web server, a CA would need a publicly verifiable domain name, which localhost is not, so they cannot verify that I am controlling that domain.