**Applied Cryptography (UE20CS314)**

**Lab 5**

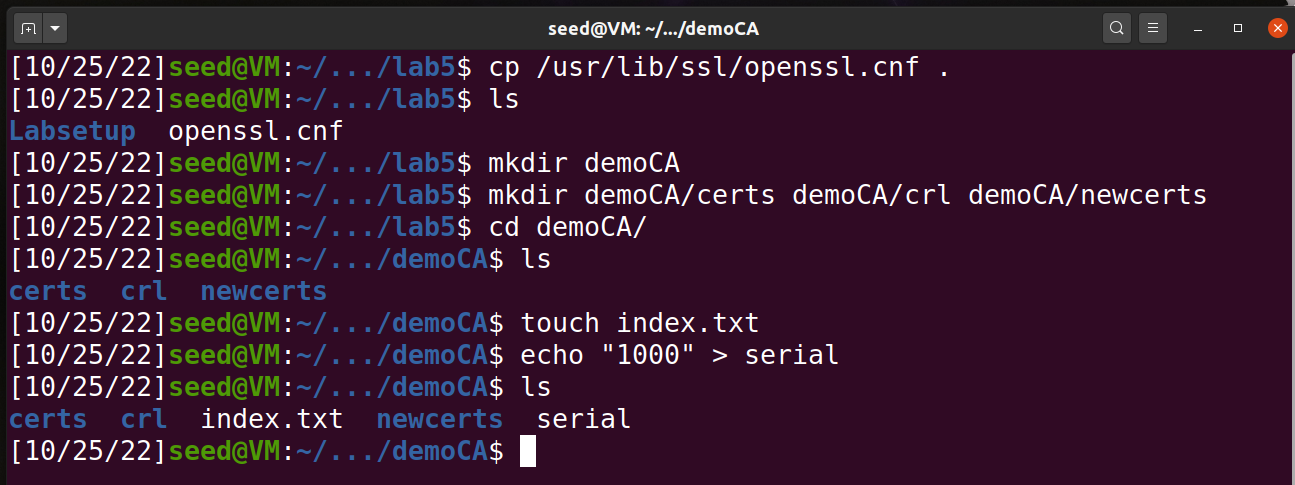
**Name: Vishwa Mehul Mehta**

**SRN: PES2UG20CS389**

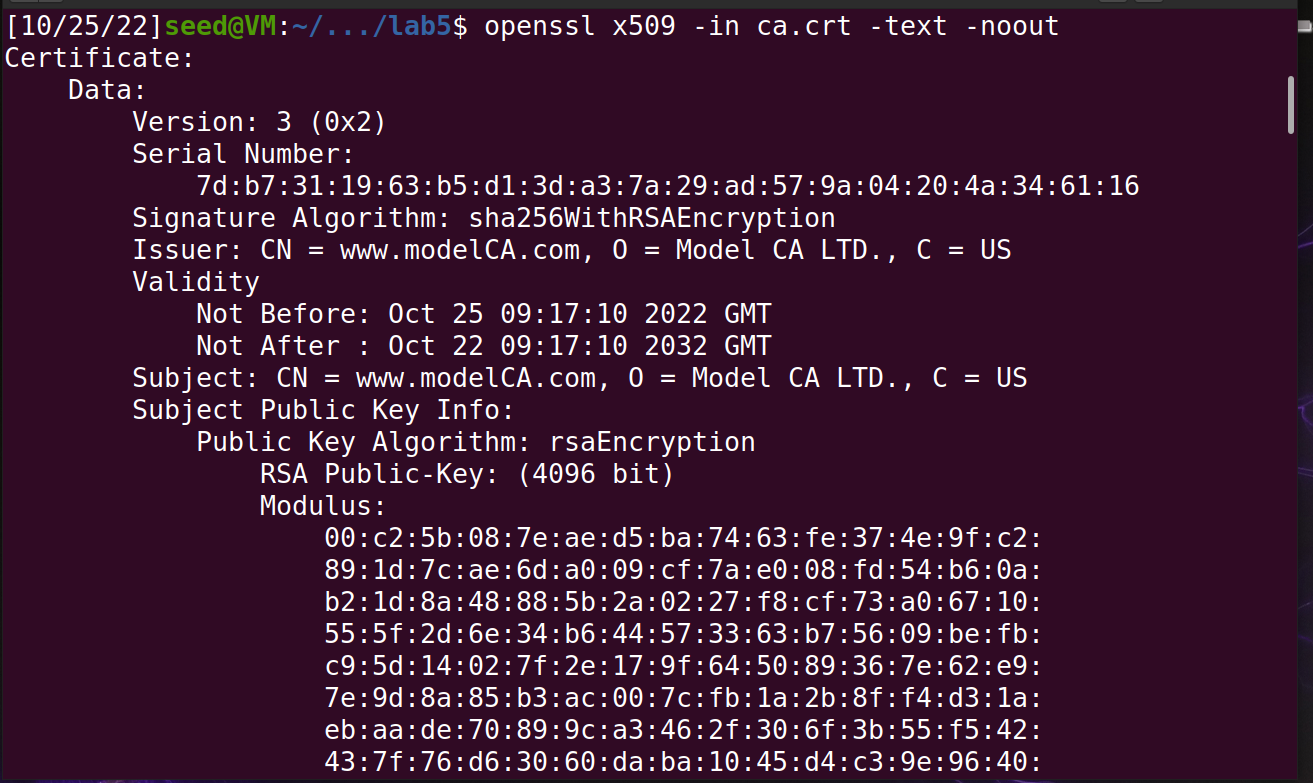
**Section: F**

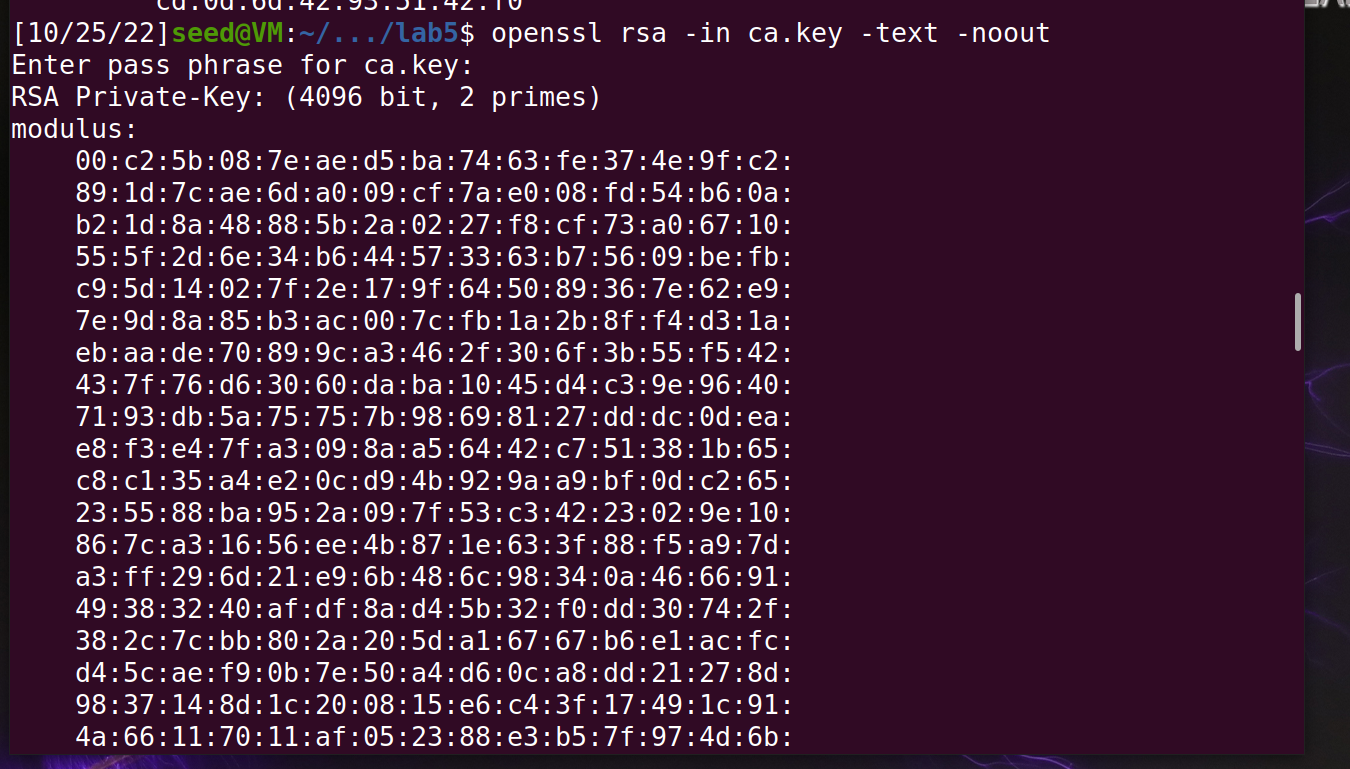
Task 1:

Screenshot:







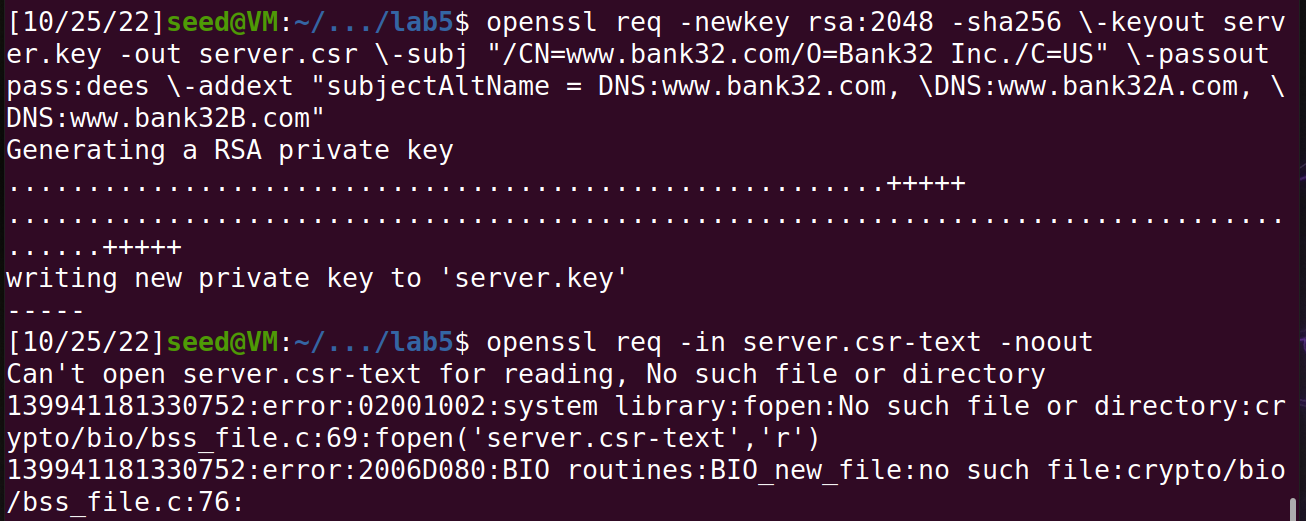


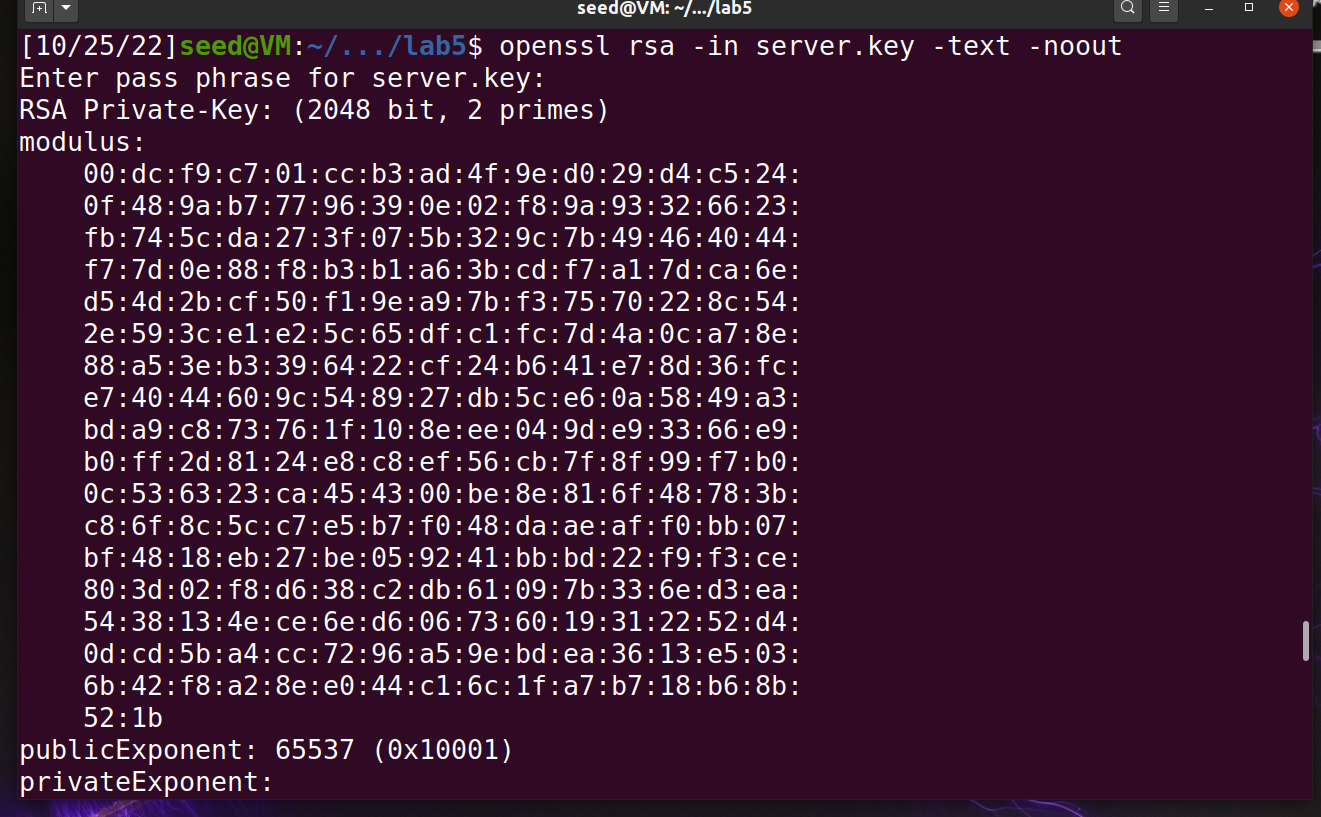
Observation:

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

Task 2:

Screenshot:



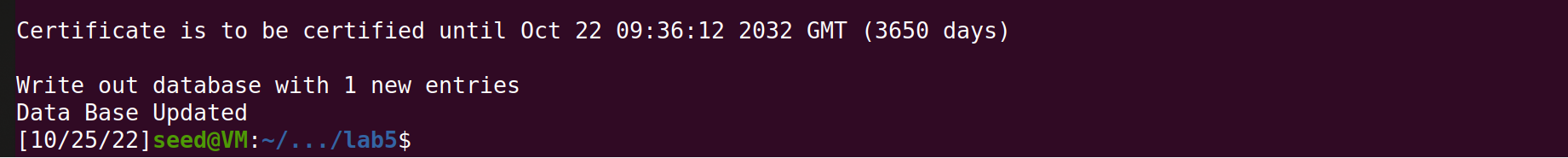


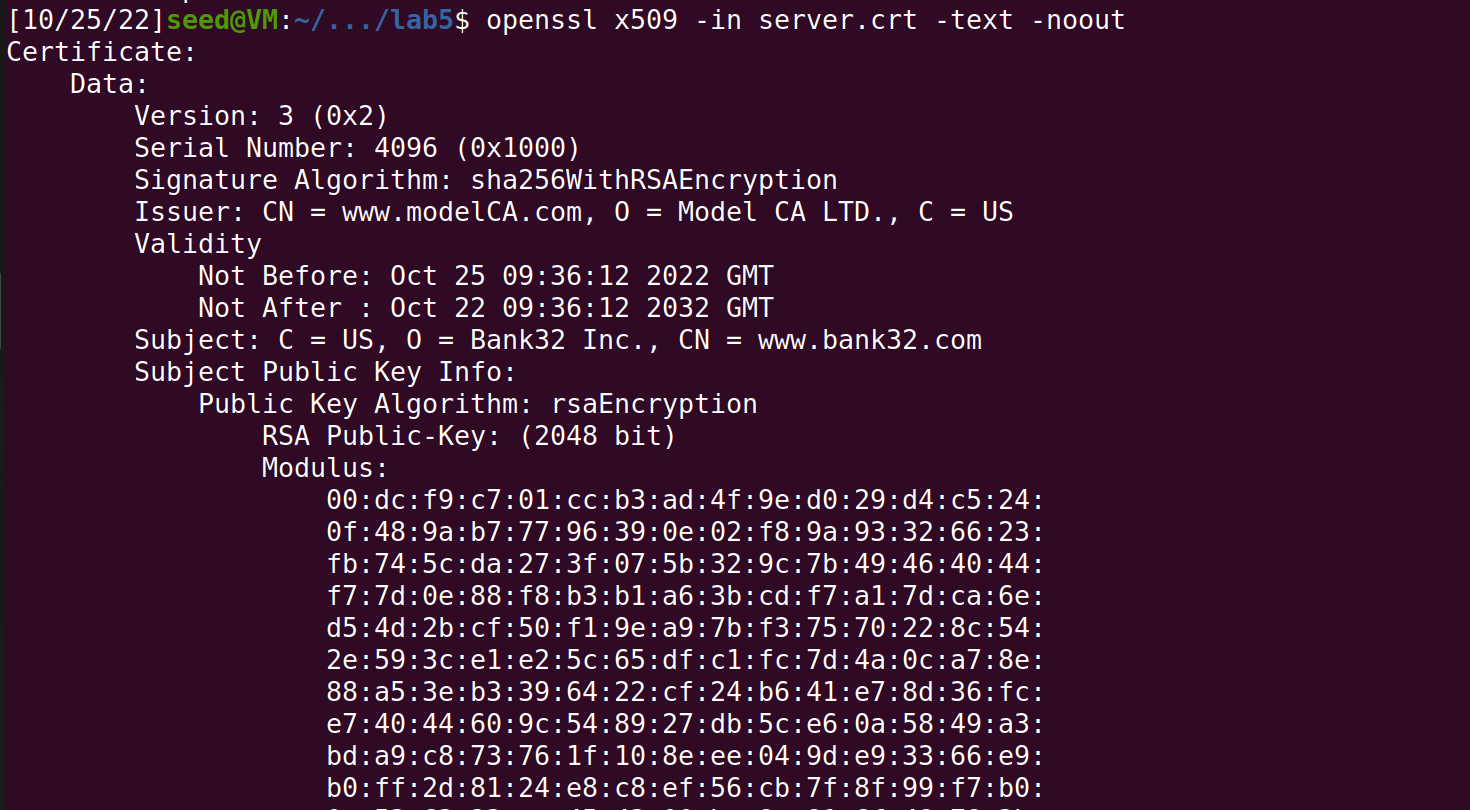
Observation:

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

Task 3:

Screenshot:



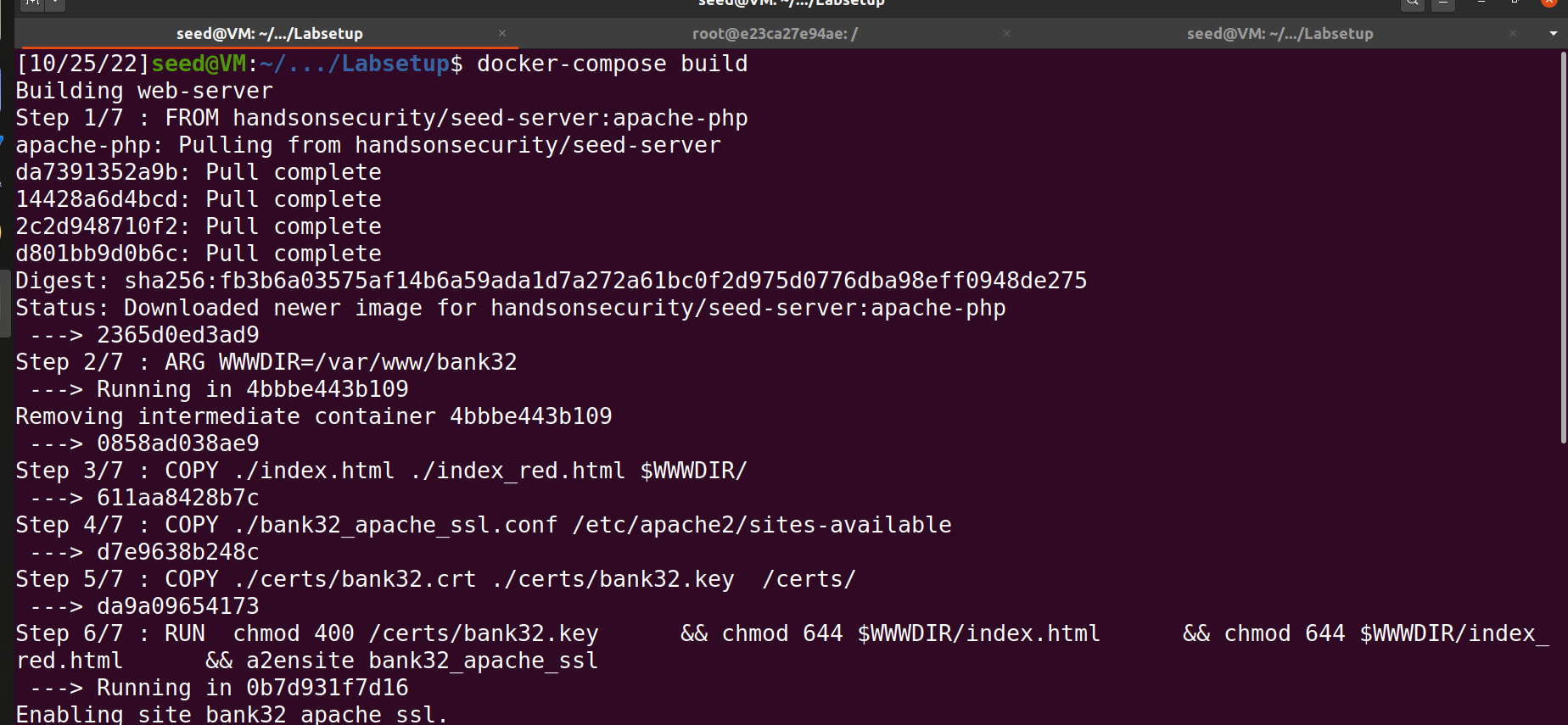


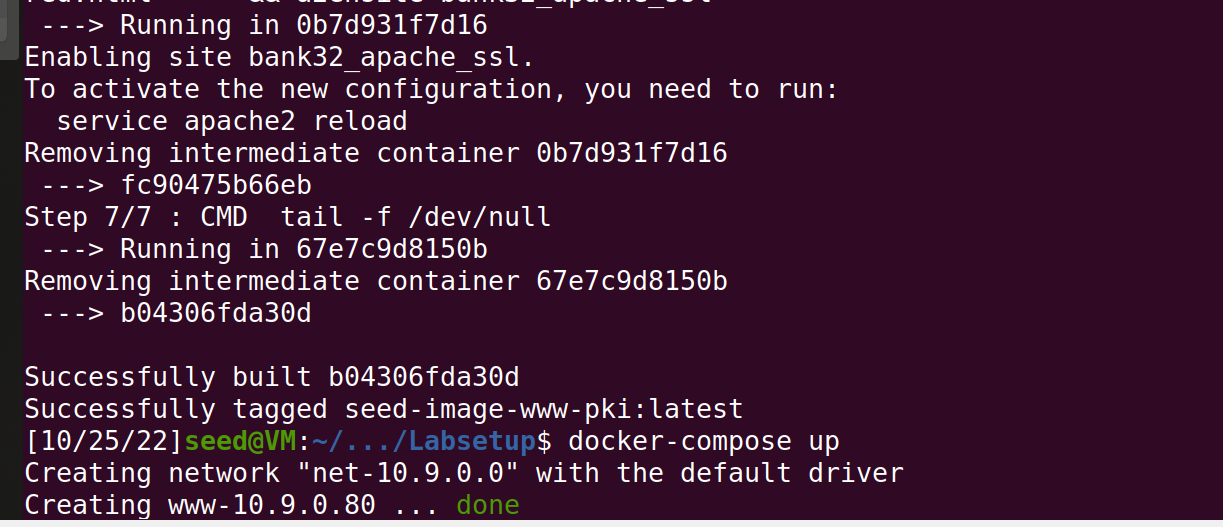
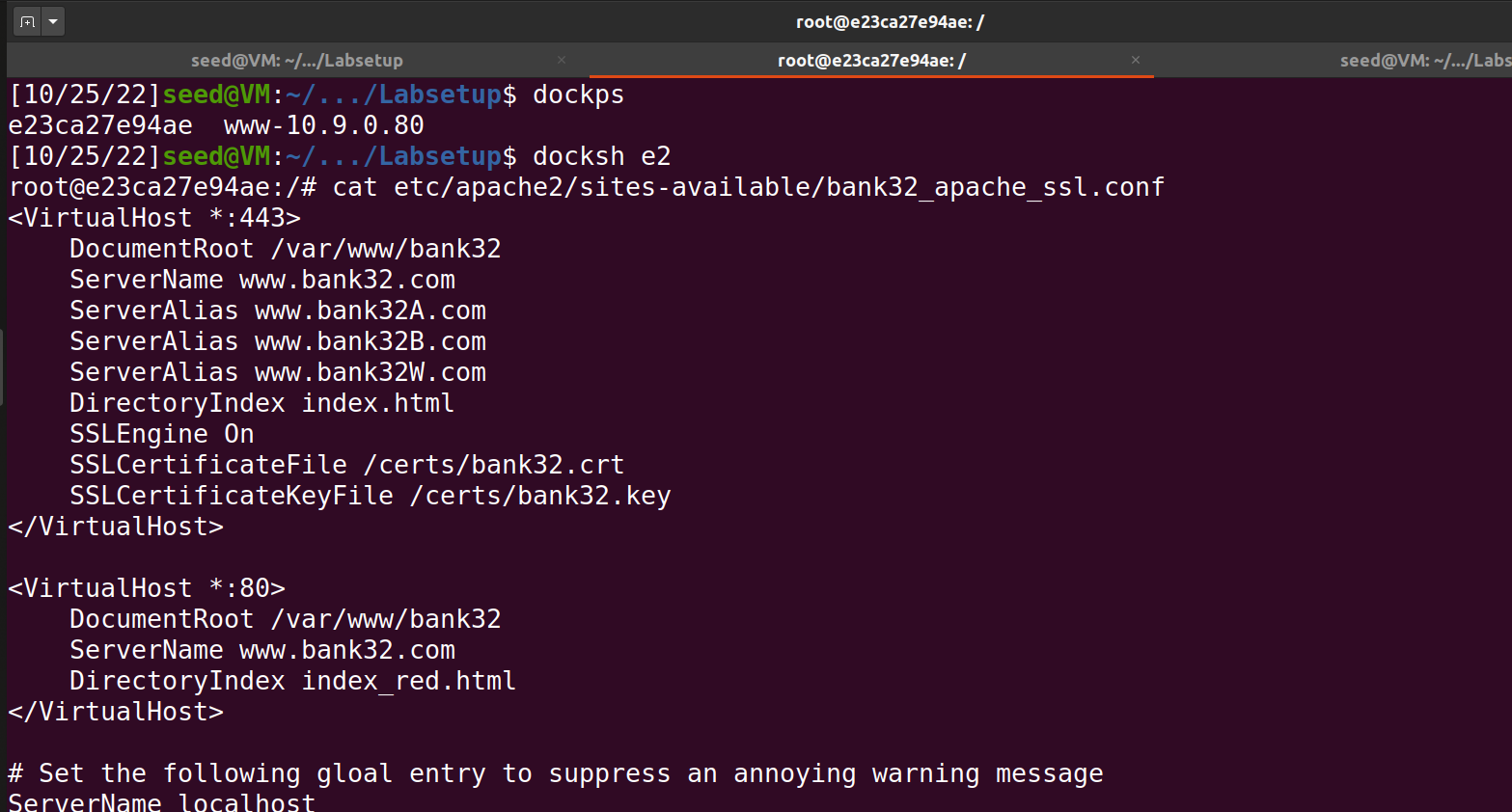
Observation:

We generate a certificate for our server here.

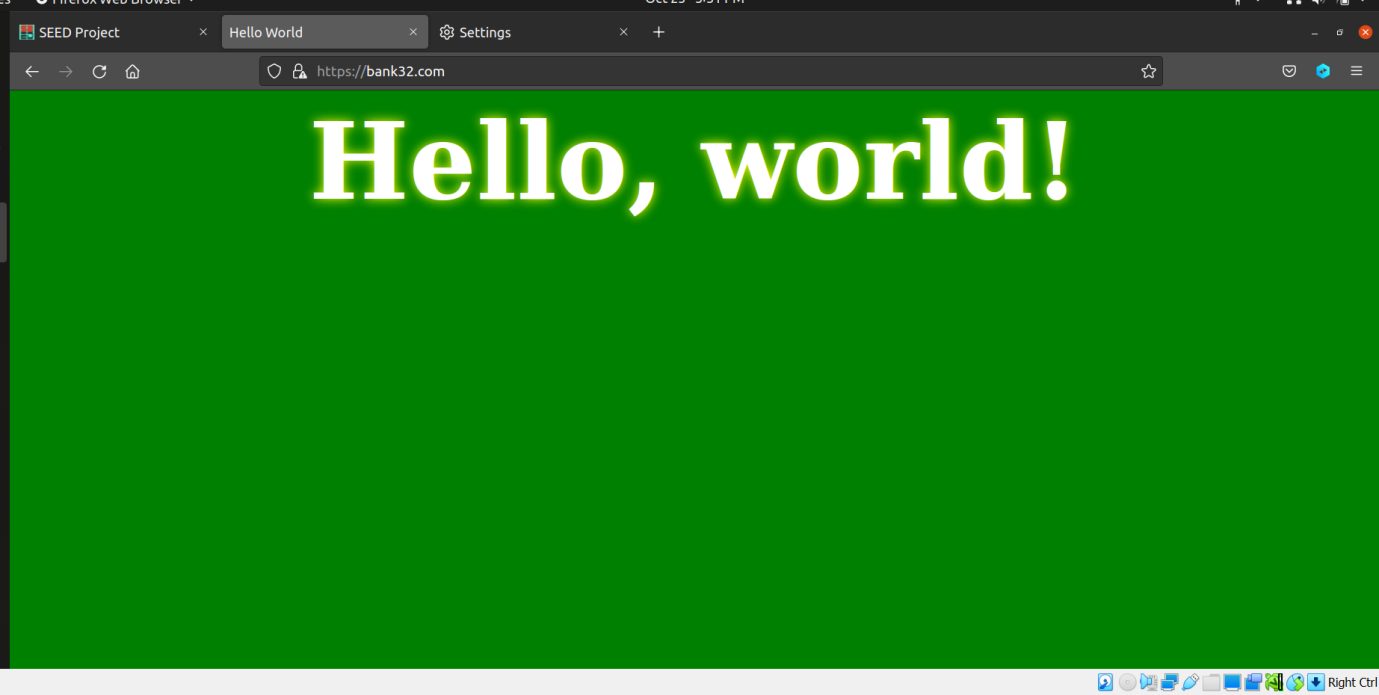
Task 4:

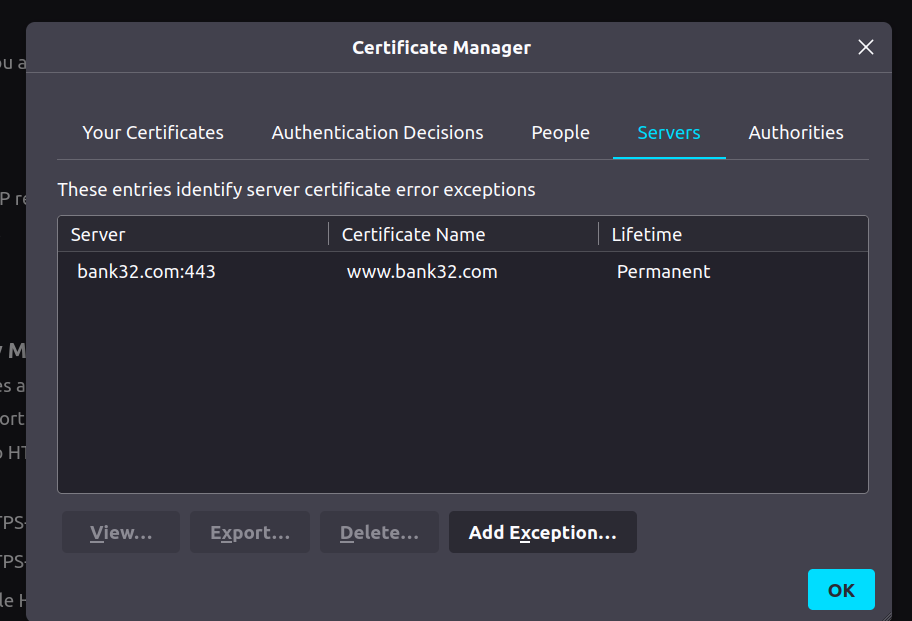
Screenshot:

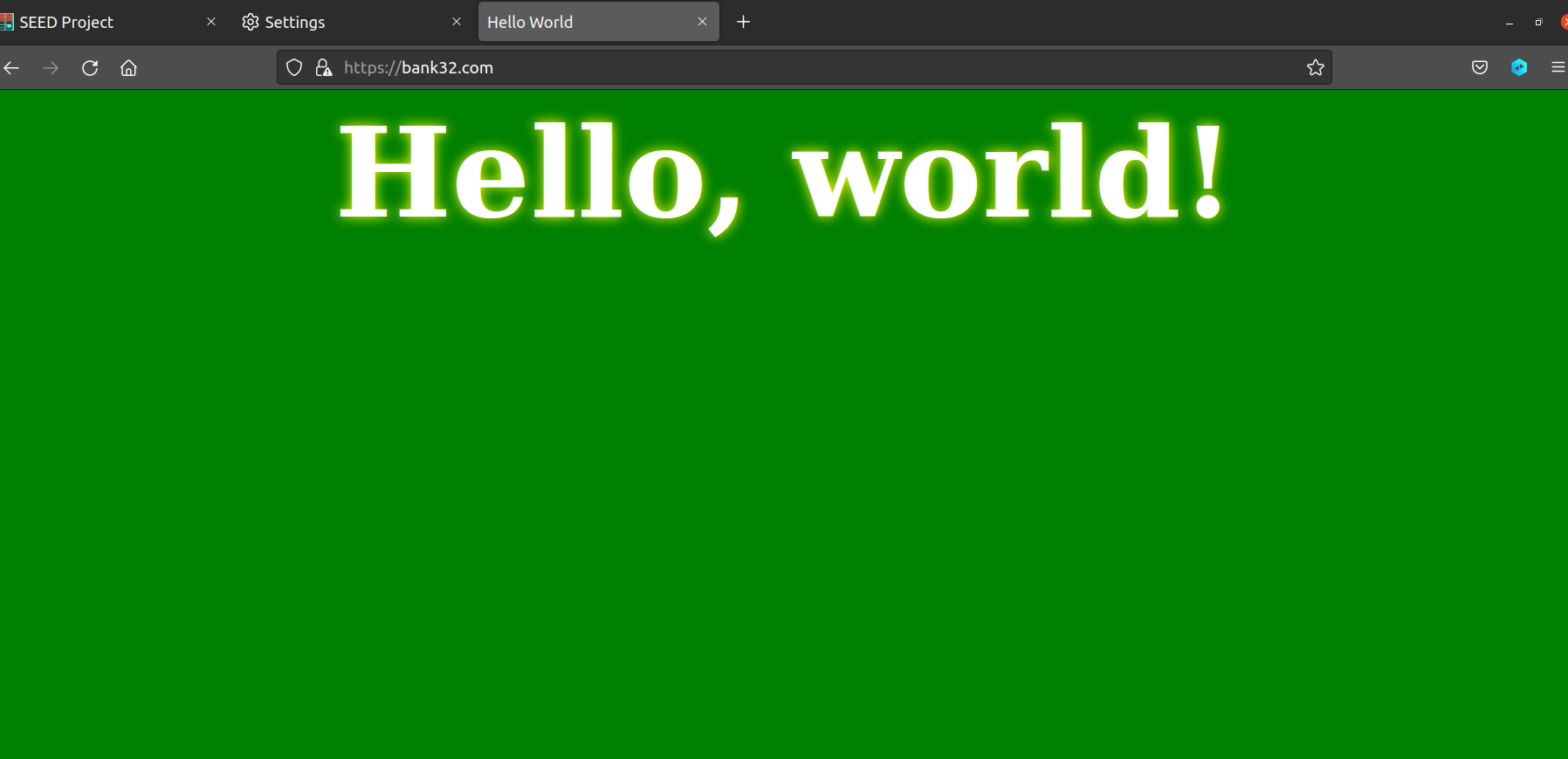


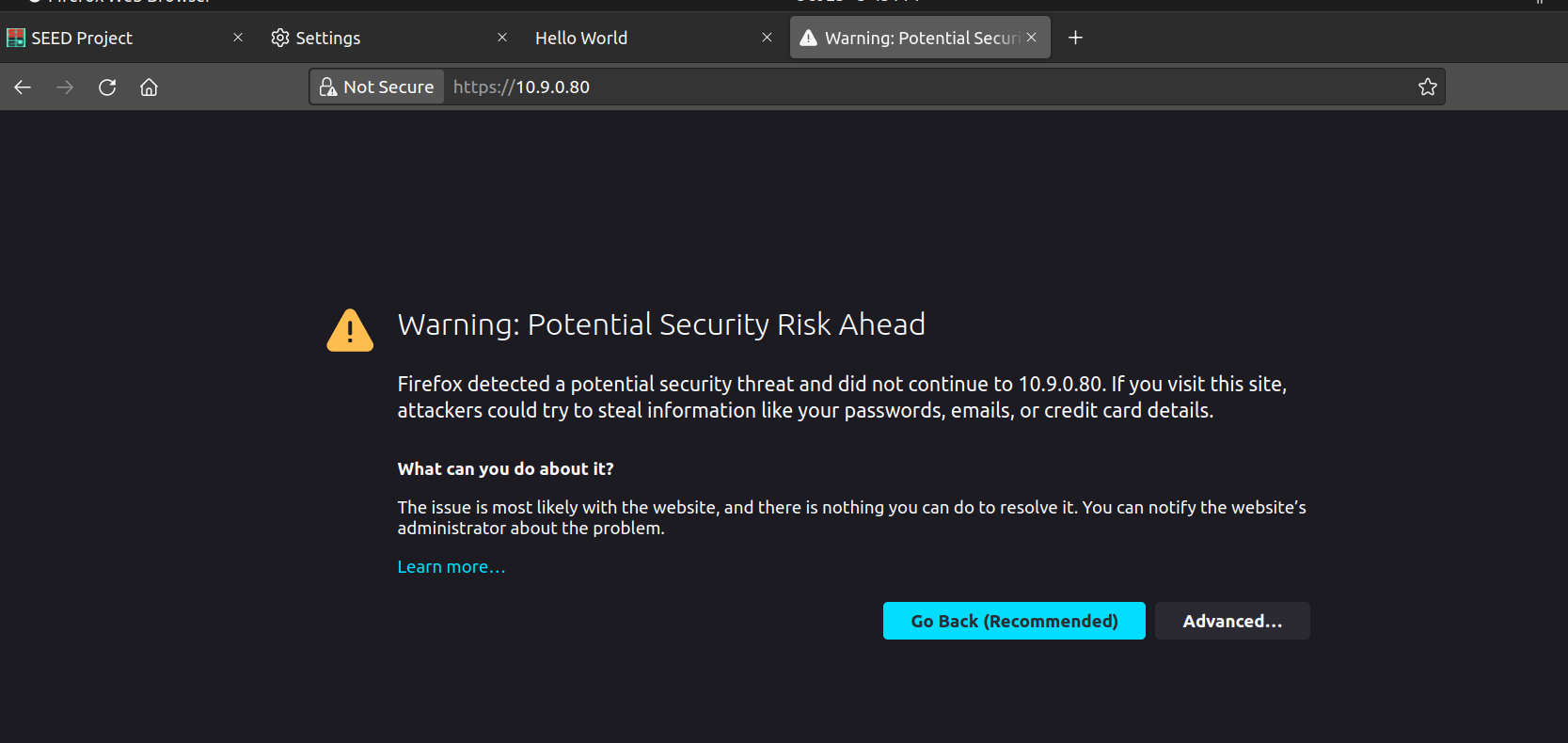
  










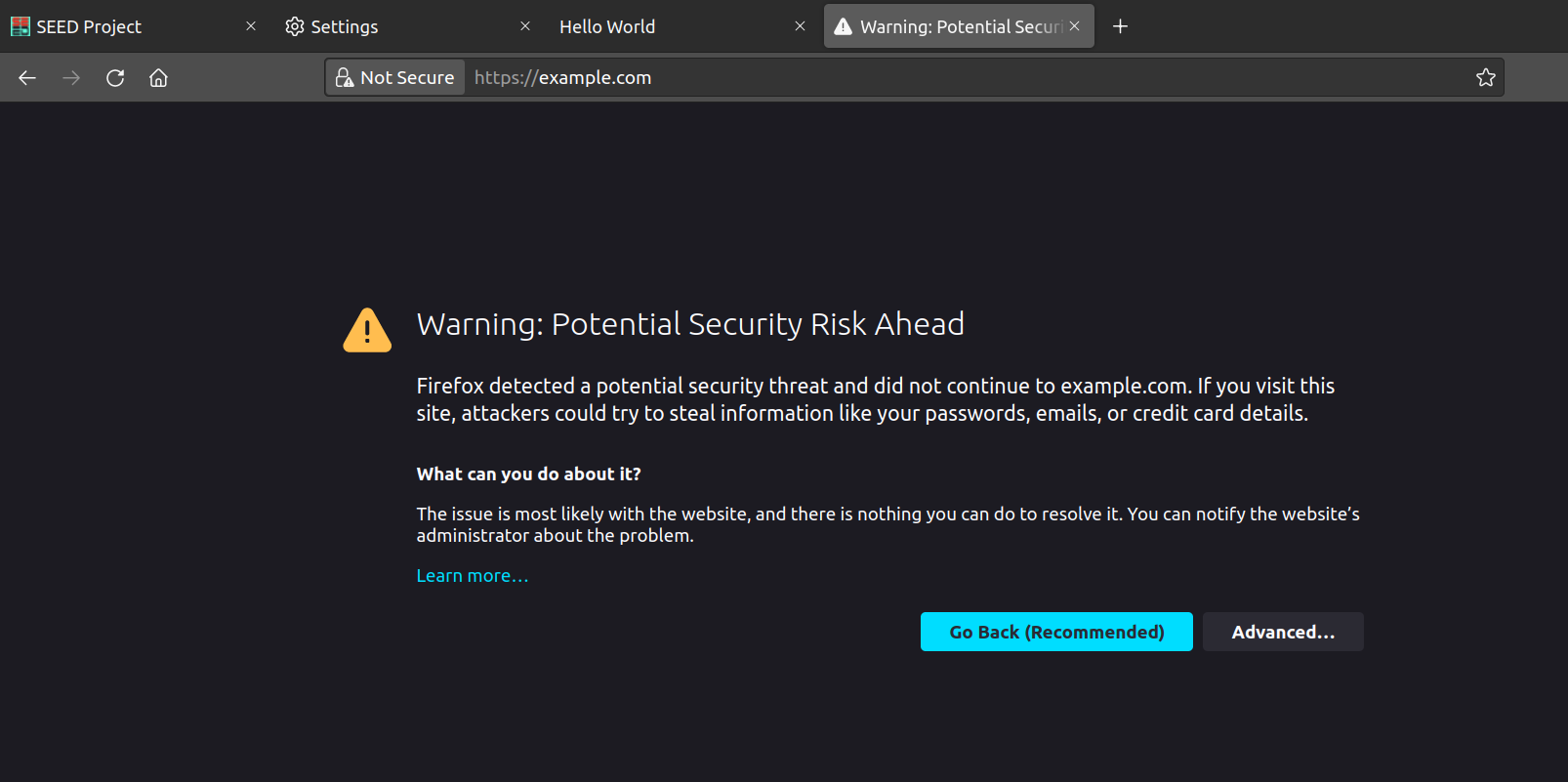


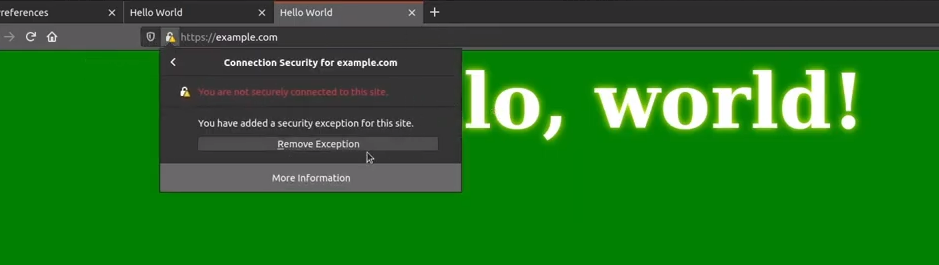
Observation:

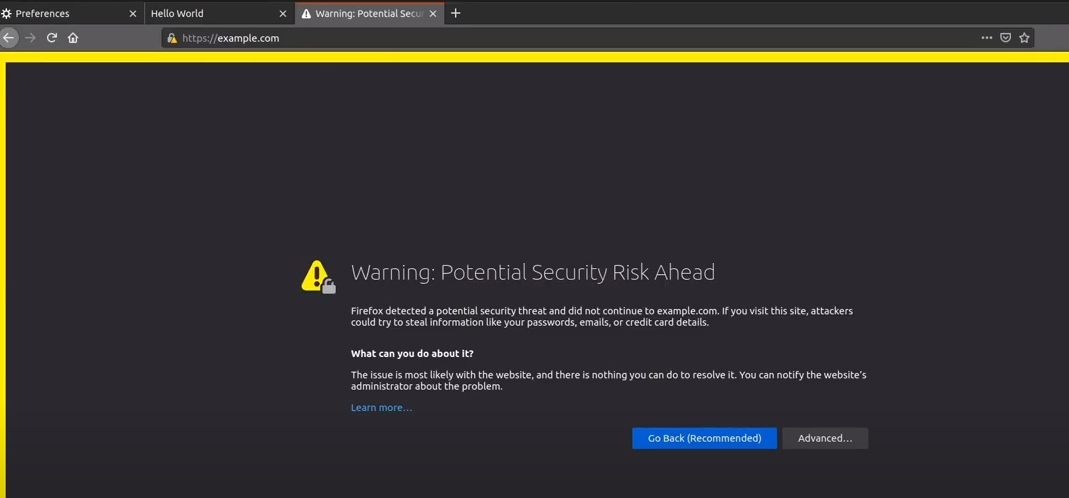
We can see the **Hello World** written when we navigate to <https://www.bank32.com>, but we see that the site is unsafe. On adding the CA to the list of certificate authorities this warning is no longer seen. We cannot use the IP address to access the website.

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.