

CMSC 626 Principles of Computer Security

Project 2

Exercise 8

Faisal Rasheed Khan

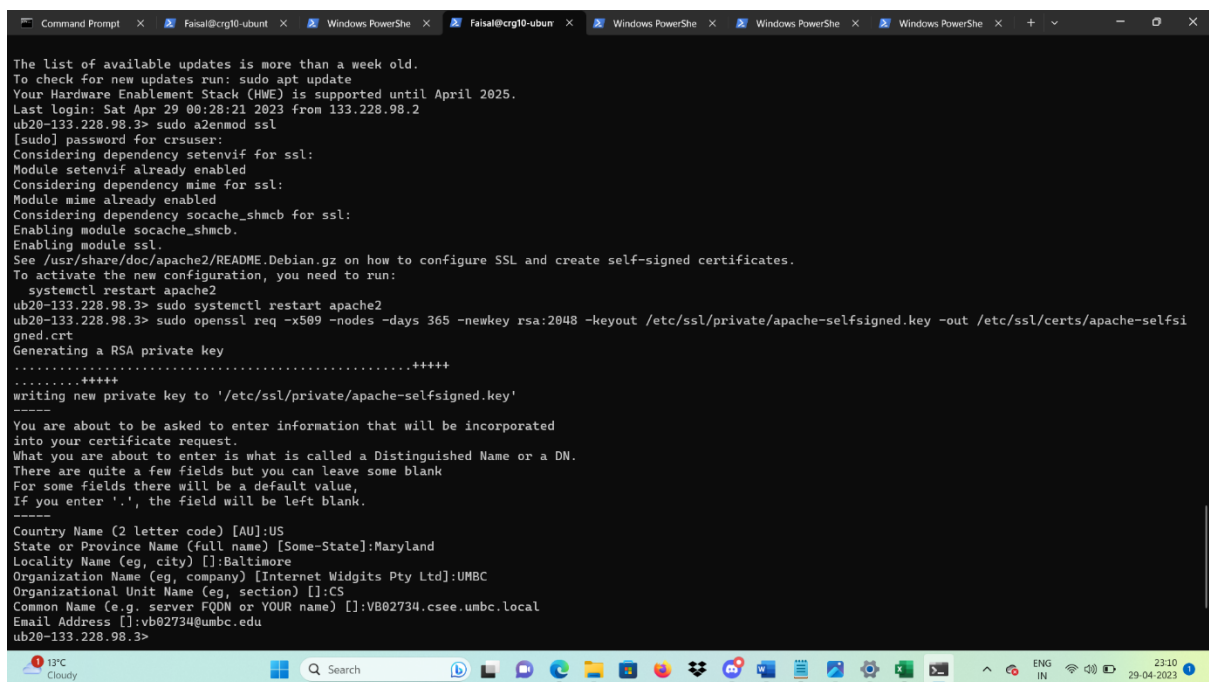
VB02734

vb02734@umbc.edu

Shrenik PolySetty

AZ61492

Output Images:



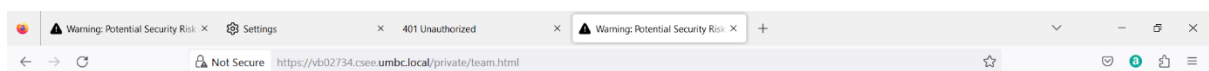
```
Command Prompt x Faisal@crg10-ubunt x Windows PowerShell x Faisal@crg10-ubunt x Windows PowerShell x Windows PowerShell x Windows PowerShell x + - _ X


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Apr 29 00:28:21 2023 from 133.228.98.2
ub20-133.228.98.3> sudo apt-get install ssl
[sudo] password for crsuser:
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
ub20-133.228.98.3> sudo systemctl restart apache2
ub20-133.228.98.3> sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
Generating a RSA private key
.....+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Baltimore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UMBC
Organizational Unit Name (eg, section) []:CS
Common Name (e.g. server FQDN or YOUR name) []:VB02734.csee.umbc.local
Email Address []:vb02734@umbc.edu
ub20-133.228.98.3>
```

```
Command Prompt x Faisal@crg10-ubunt x Windows PowerShe x Faisal@crg10-ubun x Windows PowerShe x Windows PowerShe x Windows PowerShe x + - _ x
GNU nano 4.8 /etc/apache2/sites-available/vb02734.csee.umbc.local.conf
<VirtualHost *:443>
  ServerName vb02734.csee.umbc.local
  DocumentRoot /var/www/vb02734.csee.umbc.local

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
  SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>
```

HTTPS:



 **Warning: Potential Security Risk Ahead**

Firefox detected a potential security threat and did not continue to **vb02734.csee.umbc.local**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#) [Advanced...](#)

vb02734.csee.umbc.local uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

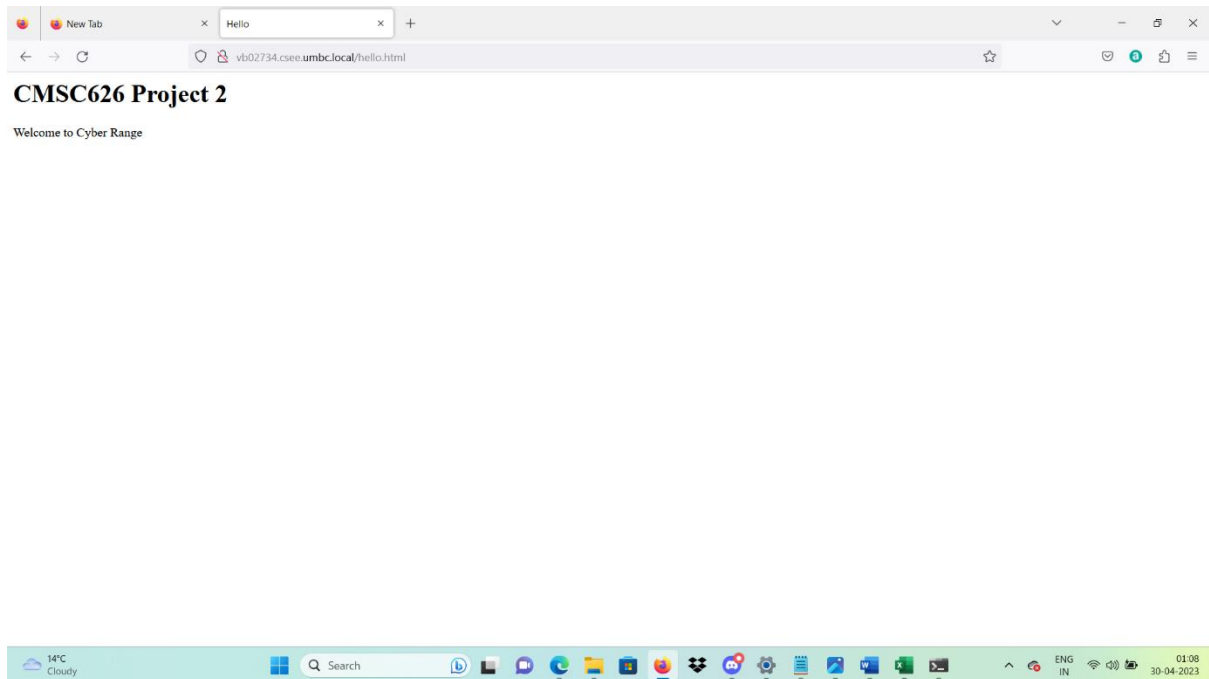
Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[View Certificate](#)

[Go Back \(Recommended\)](#) [Accept the Risk and Continue](#)



Checking if the setup is right or not:



HTTPS:

