Karthik Pradeep Hegadi

2KE20CS032

Assignment 19

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

Network Security

Assignment 1: Networking Security - Assignment 1 - Configure and enable Nginx to Use TLS and generate a certificate.

$~ openssl req -x509 -newkey rsa:2048 -nodes -keyout mm.pem -out mmcert.pem -sha256 -days 365

Options
req: Certificate Signing Request
X509: Certificate to be x509 format
newkey rsa:2048 : New certificate request and private key. RSA key size in bits
nodes: No DES(Data Encryption Standard). Generated private key will not be encrypted
keyout: Private key file name
out: Output file name. In this case, it is certificate

Step 1: Generate the certificate

```
lusy@localhost.localdomain /etc/nginx/certificates (32.86s)
sudo openssl req -x509 -newkey rsa:2048 -nodes -keyout mm.pem -out mmcert.pem -sha256 -days 365
..+.....+.+..+...+....+.....+.+..+.........+....+.....+.......+.....+............+.............+.....+.........++++++++++++++
++*....+...+...........+....+......+..+....+...+..+.+...+...........+.........+......+.......+.....+.++++++++++++++++++++++
...+..+.........+.+...+........+.........+..+.............................+..+.........+.........+.....+.+.....++++++++++++++
++++++
......+..+...+.......+...+...+.......................+.....+.+......+........+...+............++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+....+..+............+.++++++++++++++++++++++++++++++++++++++++
-----
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) [XX]:IN
State or Province Name (full name) []:karnataka
Locality Name (eg, city) [Default City]:hubbli
Organization Name (eg, company) [Default Company Ltd]:lusy
Organizational Unit Name (eg, section) []:lusy_c
Common Name (eg, your name or your server's hostname) []:lusy
Email Address []:lusy@server.in
```

Step 2: Verify it

```
lusy@localhost.localdomain /etc/nginx (0.021s)
cd certificates/

lusy@localhost.localdomain /etc/nginx/certificates (0.022s)
tree
.
├── mmcert.pem
└── mm.pem

0 directories, 2 files
```

Step 3: Give permission to the directory to access the folder by master process

```
lusy@localhost.localdomain /etc/nginx (0.057s)
sudo chmod 777 /etc/nginx/certificates/
```

Step 4: Make changes in config files

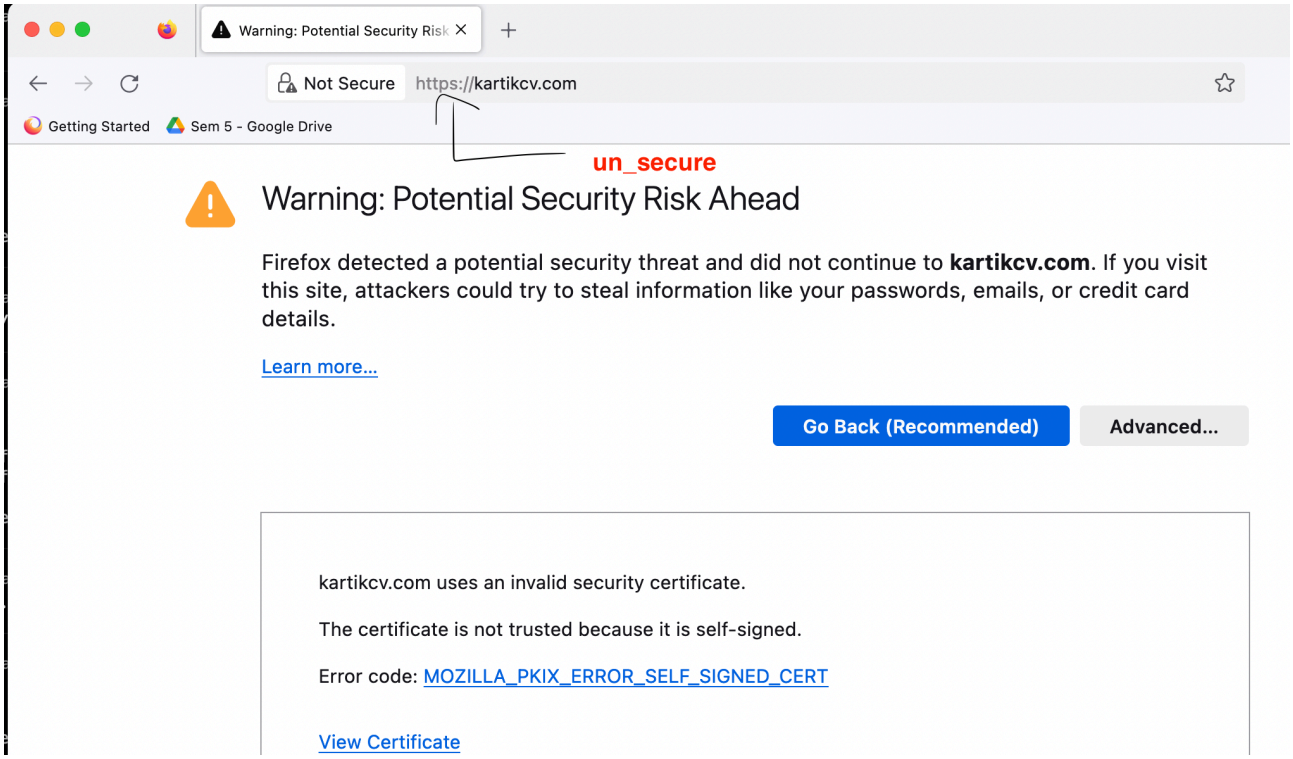
usy@localhost:/etc/nginx/certific /opt/homebrew/var/www

```
server {

        listen 80;
        server_name kartikcv.com;
        return 301 https://$server_name$request_uri;

}
        server{

        listen 443 ssl ;
        server_name kartikcv.com;

         ssl_certificate /etc/nginx/certificates/mmcert.pem;
         ssl_certificate_key /etc/nginx/certificates/mm.pem;

        location / {
        root /usr/share/nginx/mycv;
        index index.html;
        }
}
~
```

Step 5: Verify using the curl

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.034s)
curl kartikcv.com

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>

lusy@localhost.localdomain /etc/nginx/conf.d
```

Step 6 Thus we can see her "The s is added to HTTP" which shows that the connection is secure



Step 7: Just click on advance and view the generated certification.

Certificate

lusy

Subject Name

Country	IN
State/Province	karnataka
Locality	hubbli
Organization	lusy
Organizational Unit	lusy_c
Common Name	lusy
Email Address	lusy@server.in

Issuer Name

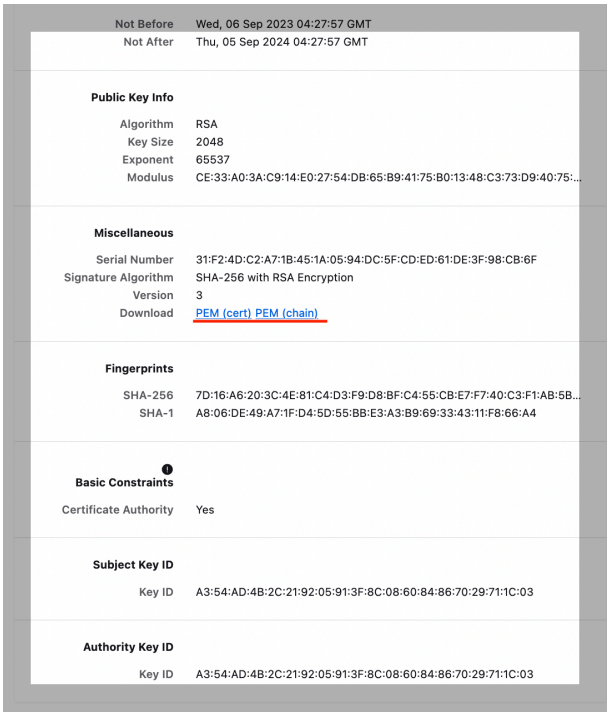
Country	IN
State/Province	karnataka
Locality	hubbli
Organization	lusy
Organizational Unit	lusy_c
Common Name	lusy
Email Address	lusy@server.in

Validity

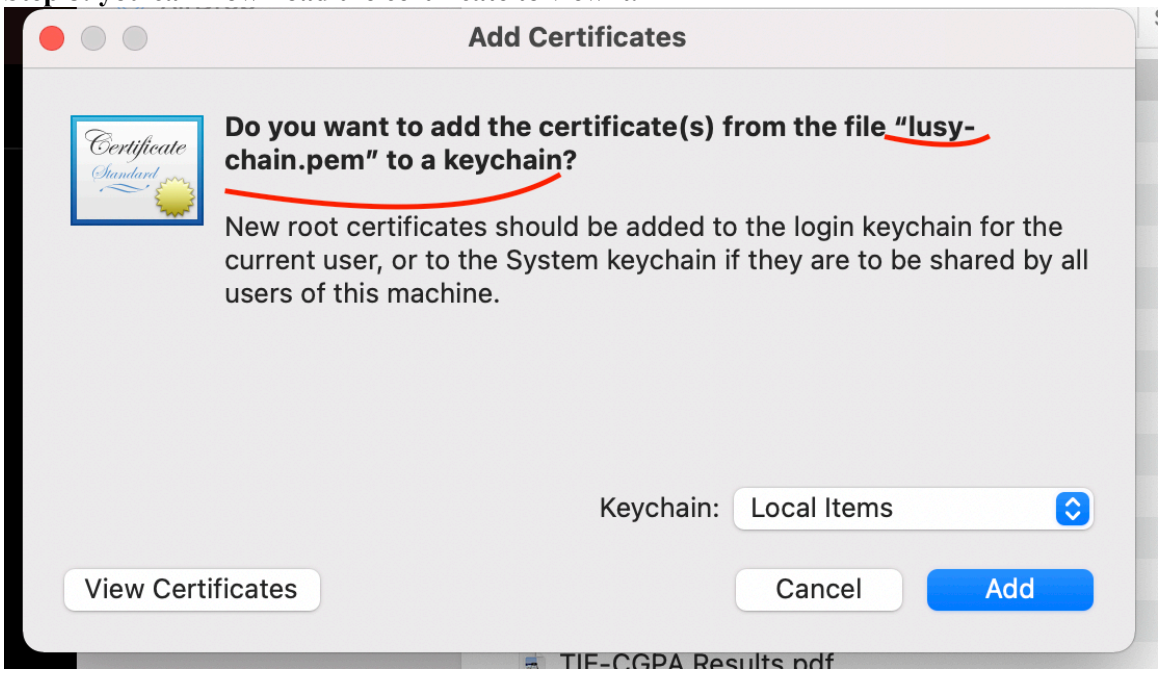
Not Before	Wed, 06 Sep 2023 04:27:57 GMT
Not After	Thu, 05 Sep 2024 04:27:57 GMT

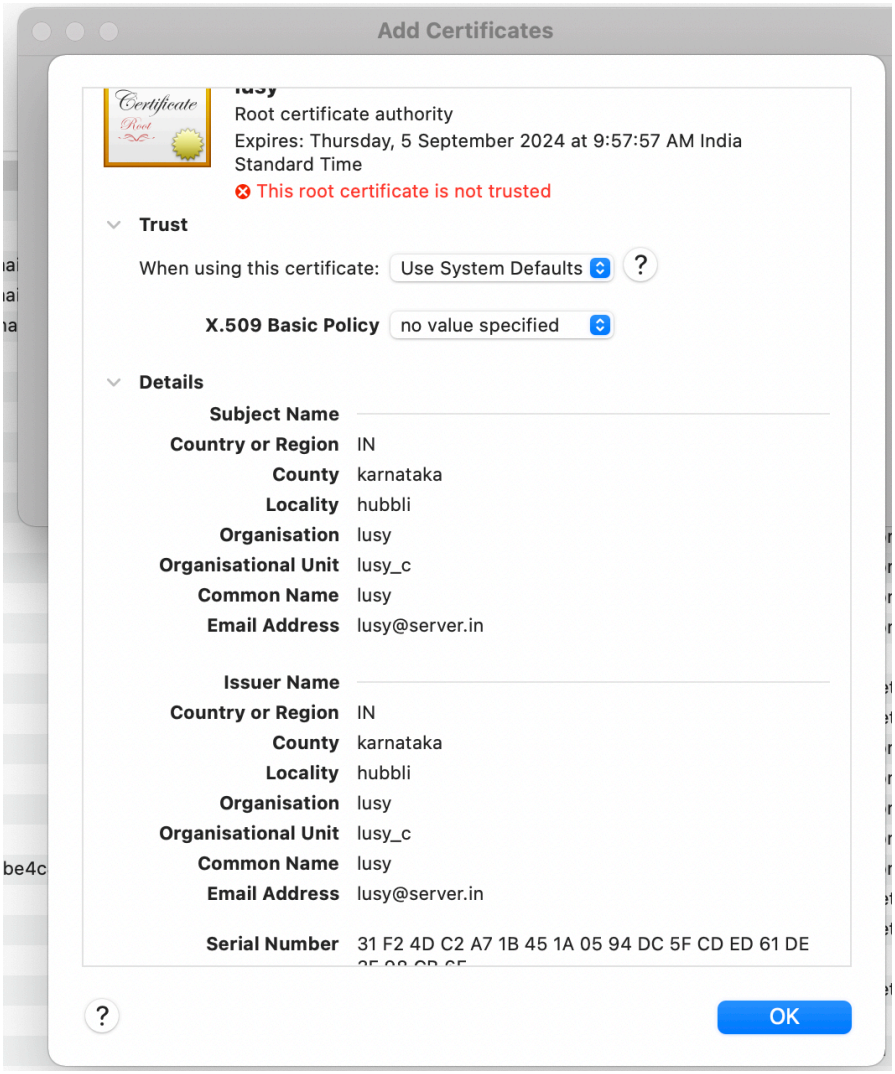
Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CE:33:A0:3A:C9:14:E0:27:54:DB:65:B9:41:75:B0:13:48:C3:73:D9:40:75:...

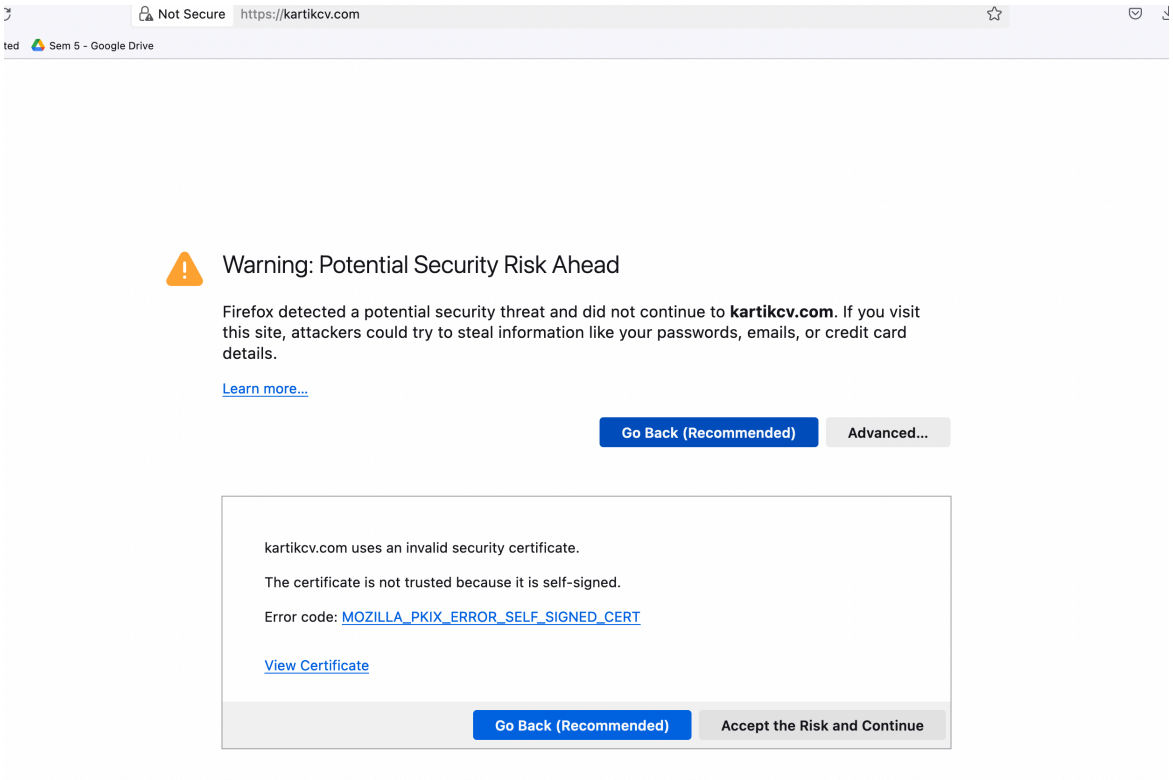


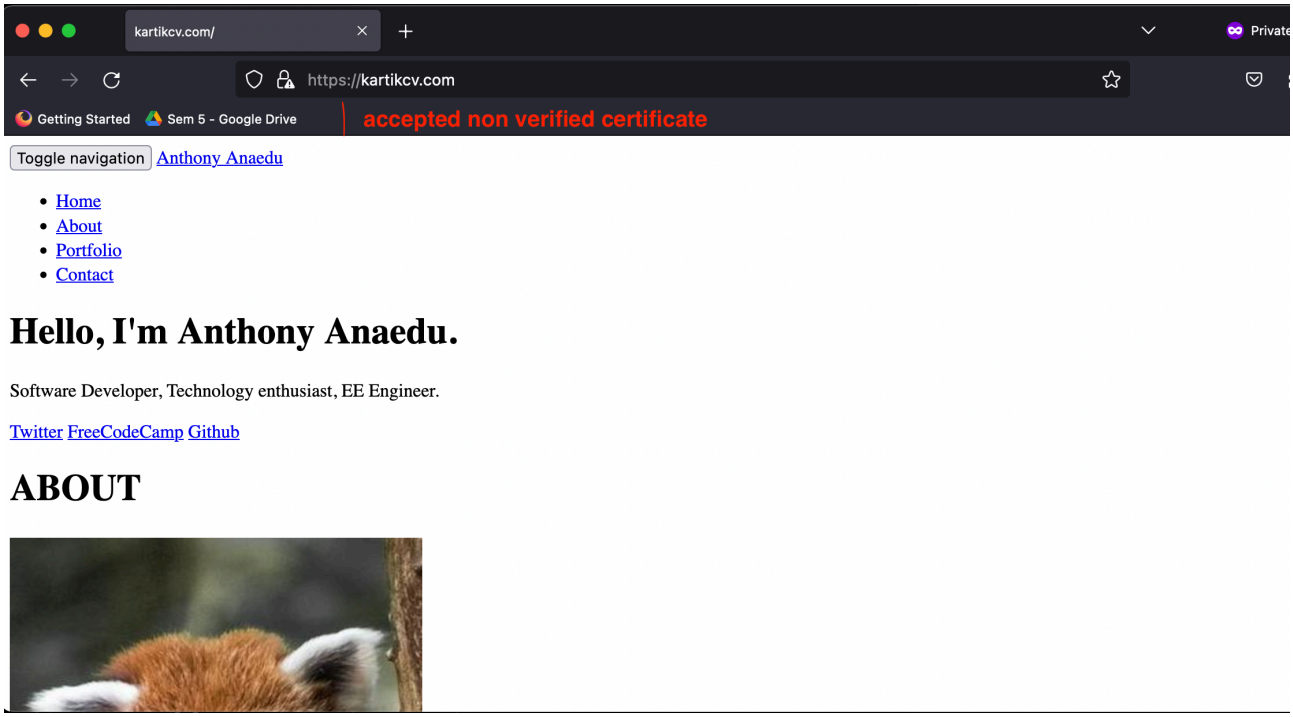
Step 8: you can Download the certificate to view it.



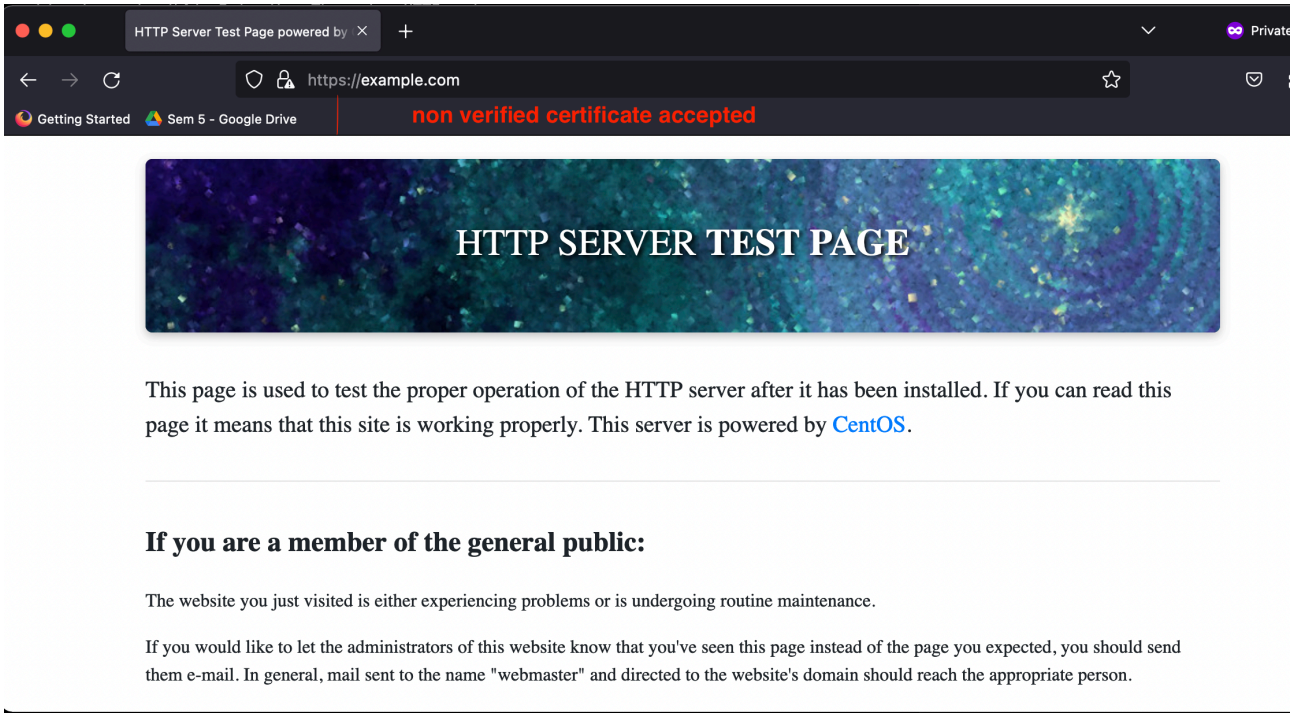


Step 9: accept and continue then you can see your page.





—TRY
(I have used another test page) just for check it.



Assignment 2 : Configure Firewall rules to prevent remote access.

1: Install the firewall into your terminal, run these commands in your terminal sudo yum install -y epel-release

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.628s)
sudo yum install -y epel-release
Last metadata expiration check: 2:30:45 ago on Wed 06 Sep 2023 10:28:16 AM IST.
Package epel-release-9-7.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

2.sudo yum install -y ufw

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.479s)
sudo yum install -y ufw
Last metadata expiration check: 2:31:20 ago on Wed 06 Sep 2023 10:28:16 AM IST.
Package ufw-0.35-24.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

3.Check the status of ufw using "sudo ufw status" (Inactive)

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.131s)
sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
SSH                        ALLOW       Anywhere
224.0.0.251 mDNS           ALLOW       Anywhere
SSH (v6)                   ALLOW       Anywhere (v6)
ff02::fb mDNS              ALLOW       Anywhere (v6)
```

4.Enable the ufw using the command "sudo ufw enable"

```
lusy@localhost.localdomain /etc/nginx/conf.d (3.888s)
sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

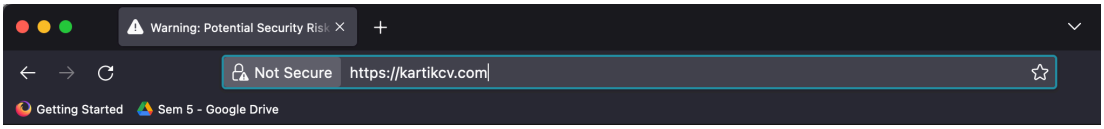
5.Check the status of ufw using "sudo ufw status" (Active)

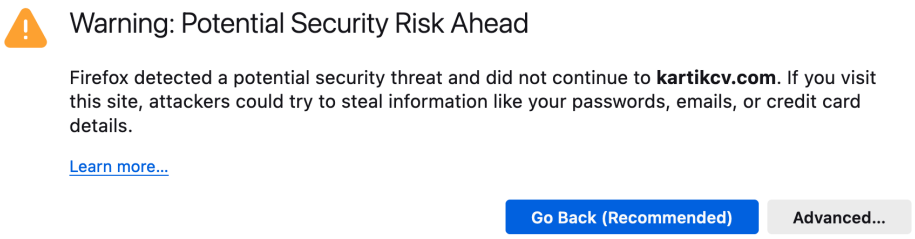
```
lusy@localhost.localdomain /etc/nginx/conf.d (0.296s)
sudo ufw deny from 192.168.43.23
Rule added

lusy@localhost.localdomain /etc/nginx/conf.d (0.272s)
sudo ufw deny 80
Rule added
Rule added (v6)
```

6. (Try to access your server (nginx) from the machine where the Ip address is blocked the site can't be reached error should display

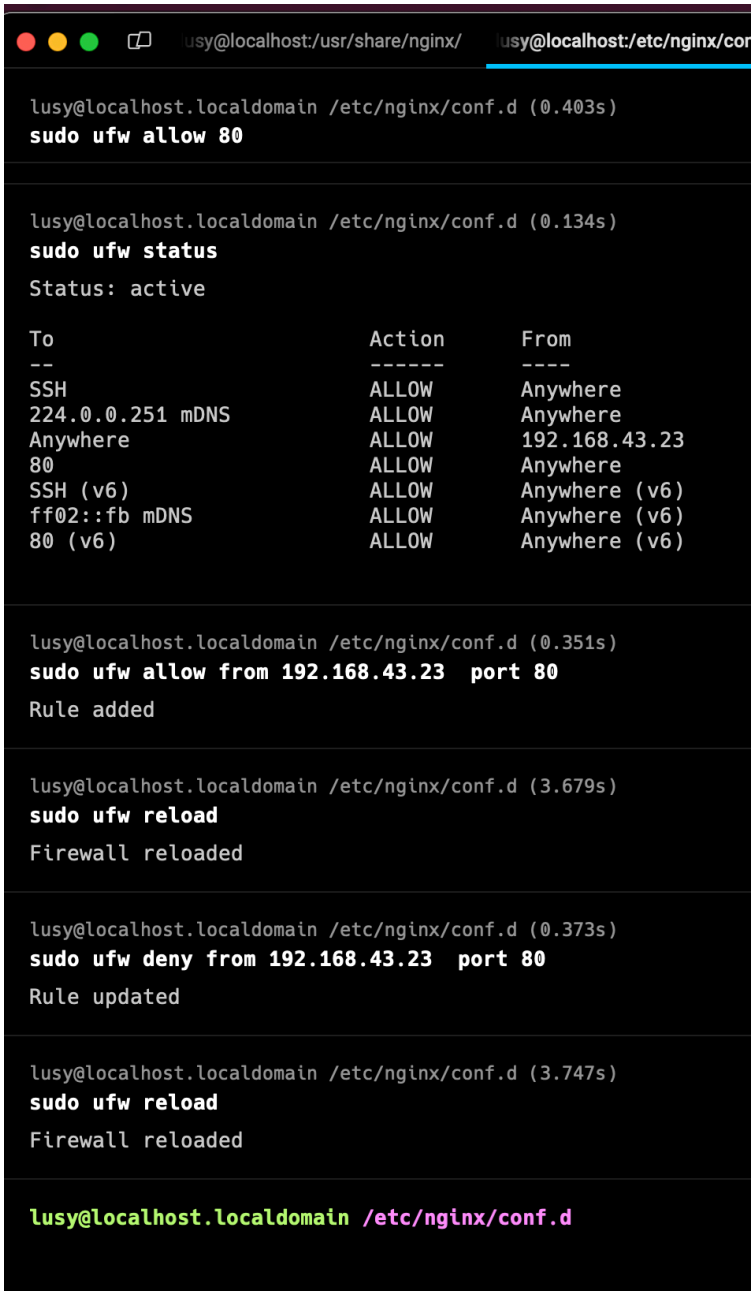
```
lusy@localhost.localdomain /etc/nginx/conf.d (0.296s)
sudo ufw deny from 192.168.43.23
Rule added

lusy@localhost.localdomain /etc/nginx/conf.d (0.272s)
sudo ufw deny 80
Rule added
Rule added (v6)
```

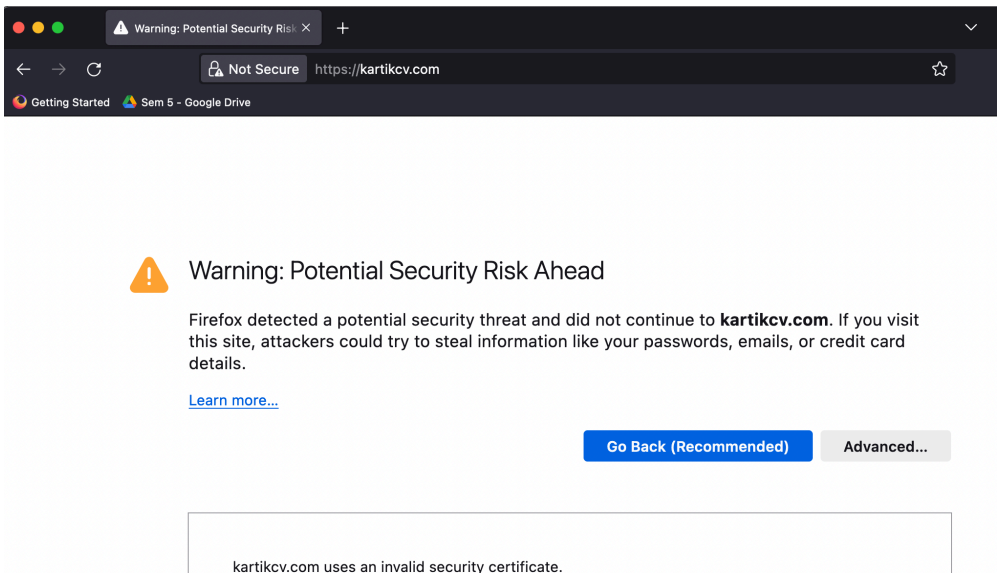
7.(Now if you try to access the server it should allow)





8.Deny a port number using command " sudo ufw deny portnumber" (rule added (Try to access the port from outside it should be blocked)




Warning: Potential Security Risk
Not Secure
https://kartikcv.com
Getting Started
Sem 5 - Google Drive
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to kartikcv.com. 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...
kartikcv.com uses an invalid security certificate.