PKI Lab

CSE644

Internet Security

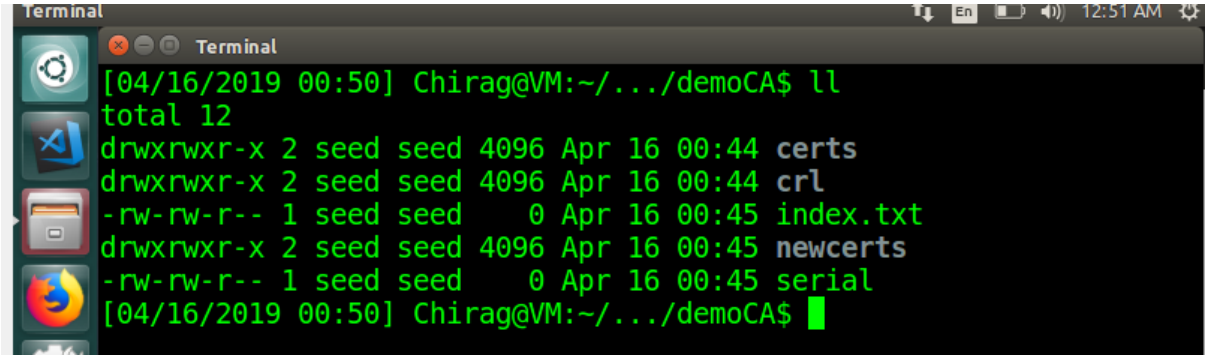
Chirag Sachdev

680231131

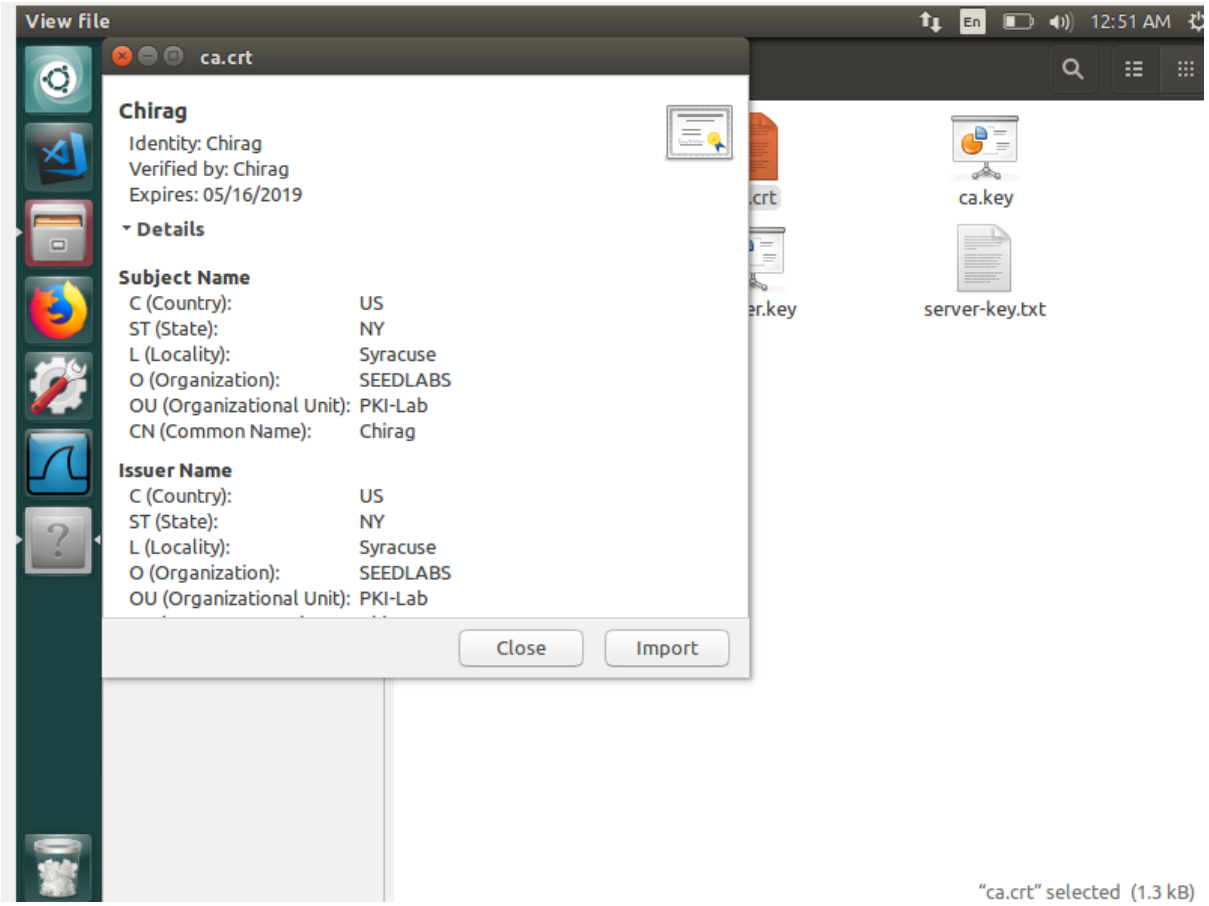
Task 1

Creating a ca.crt file by becoming a CA.

Setting up the directories

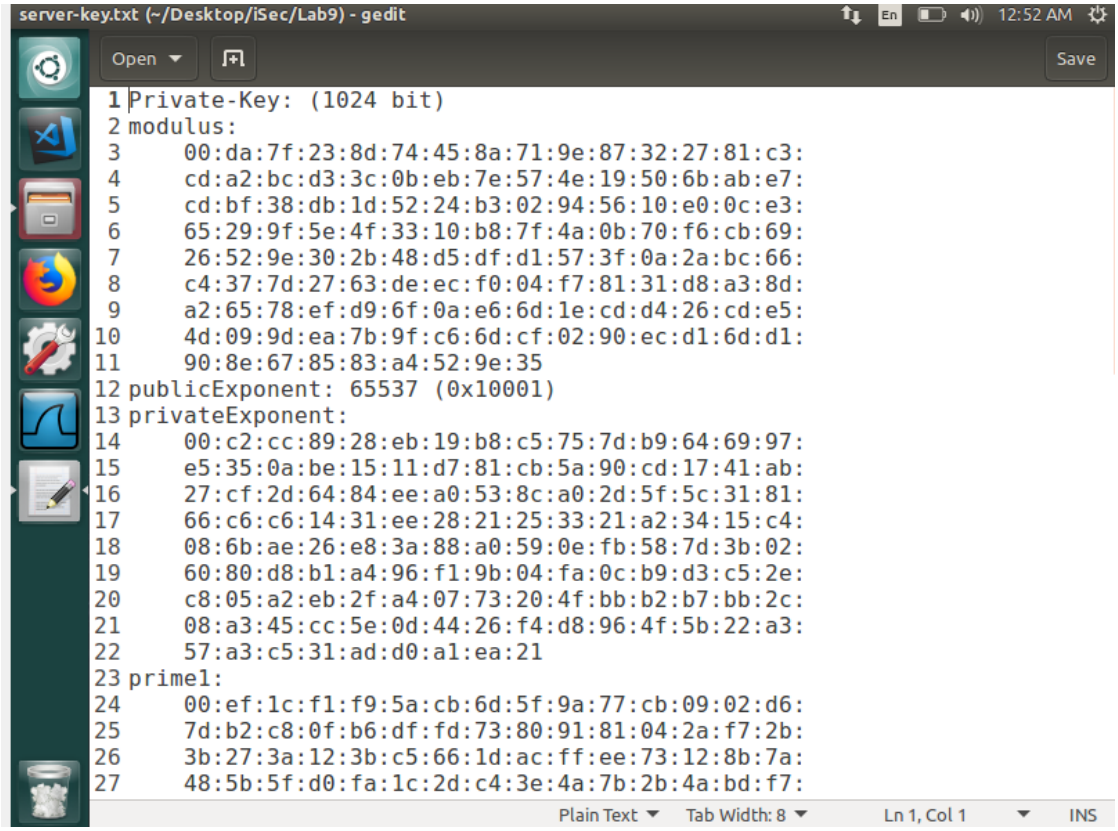


The certificate created:

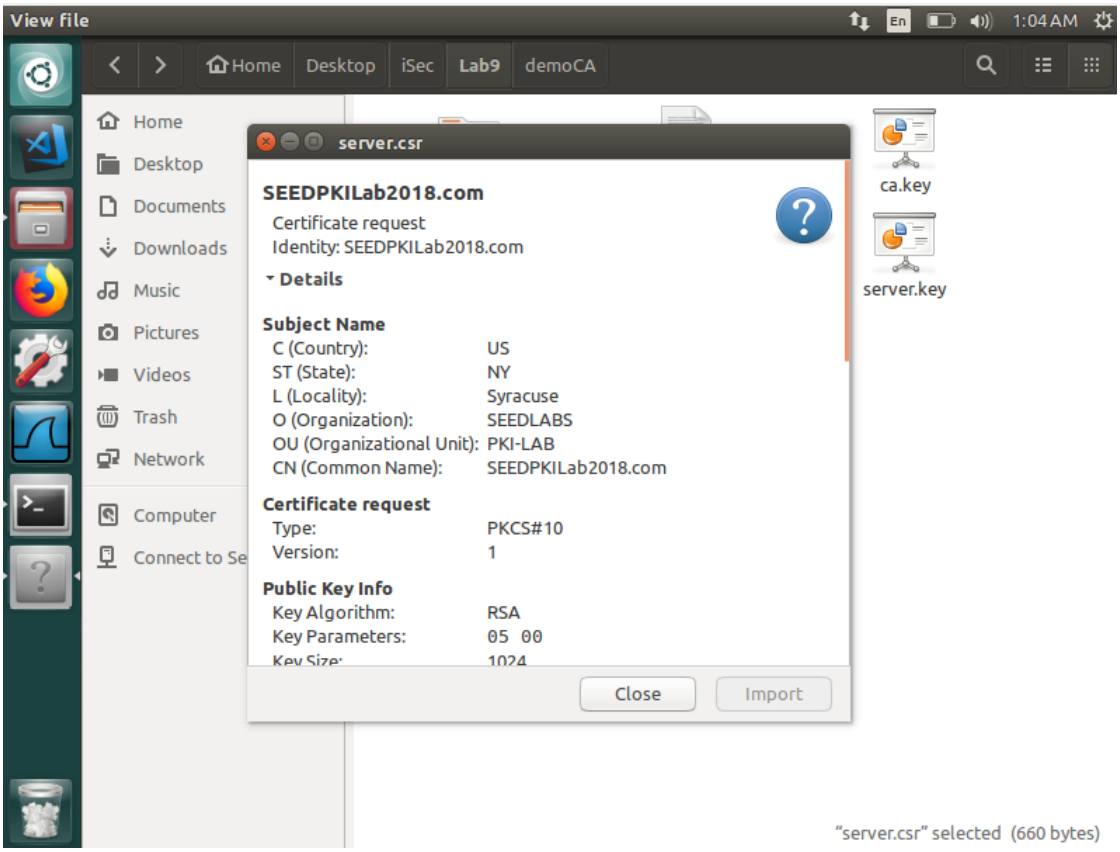


Task 2

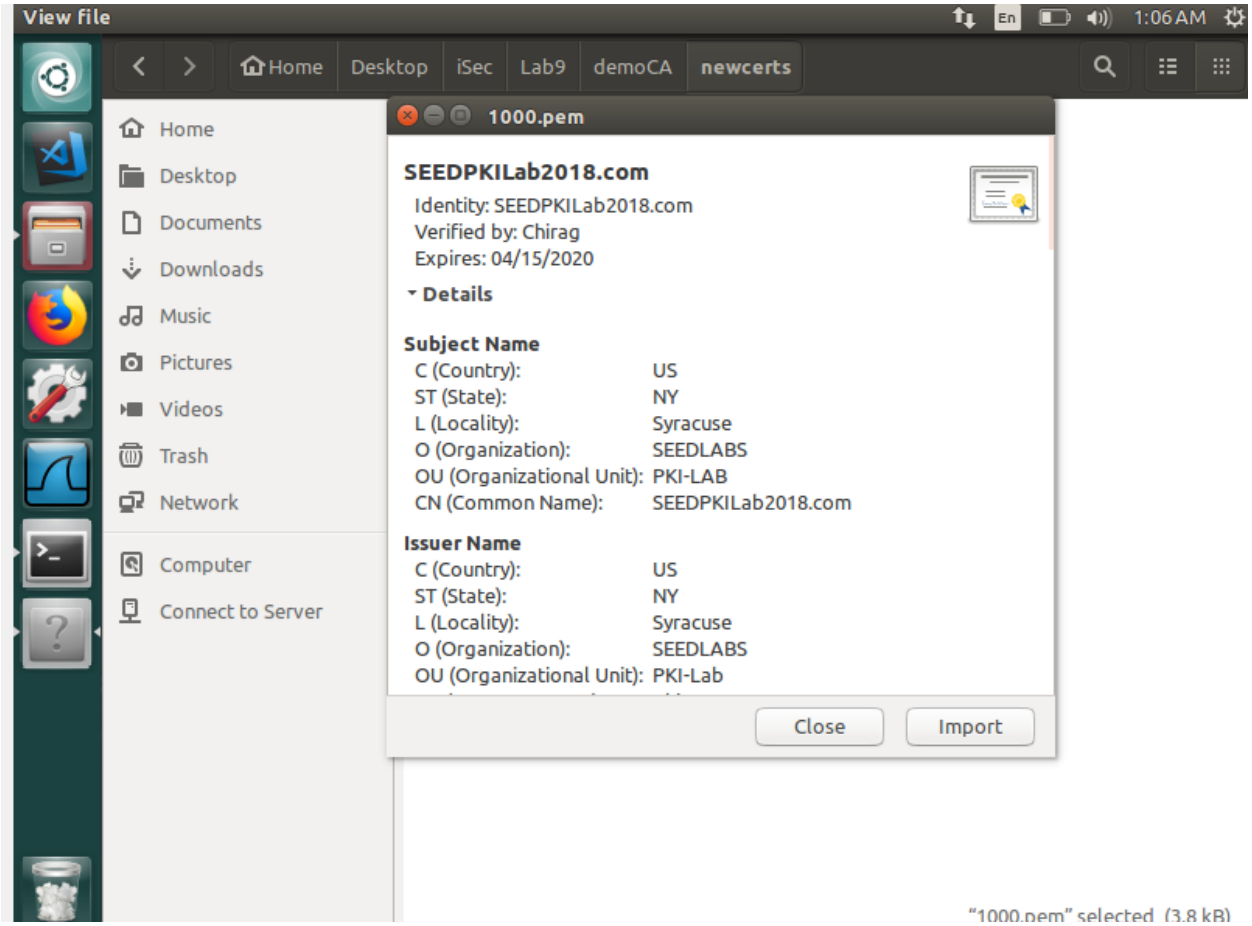
Generating public/private key pair



Generating the server signing request.

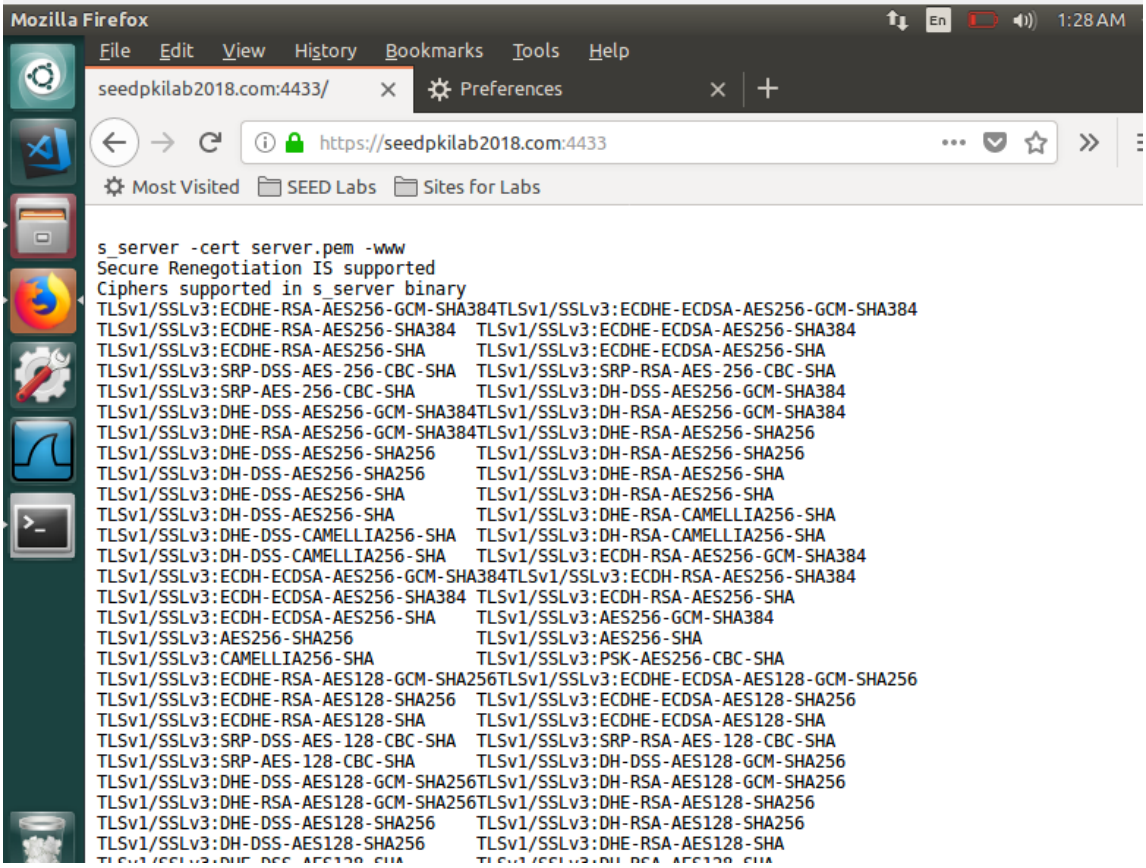


Generating the server from the request



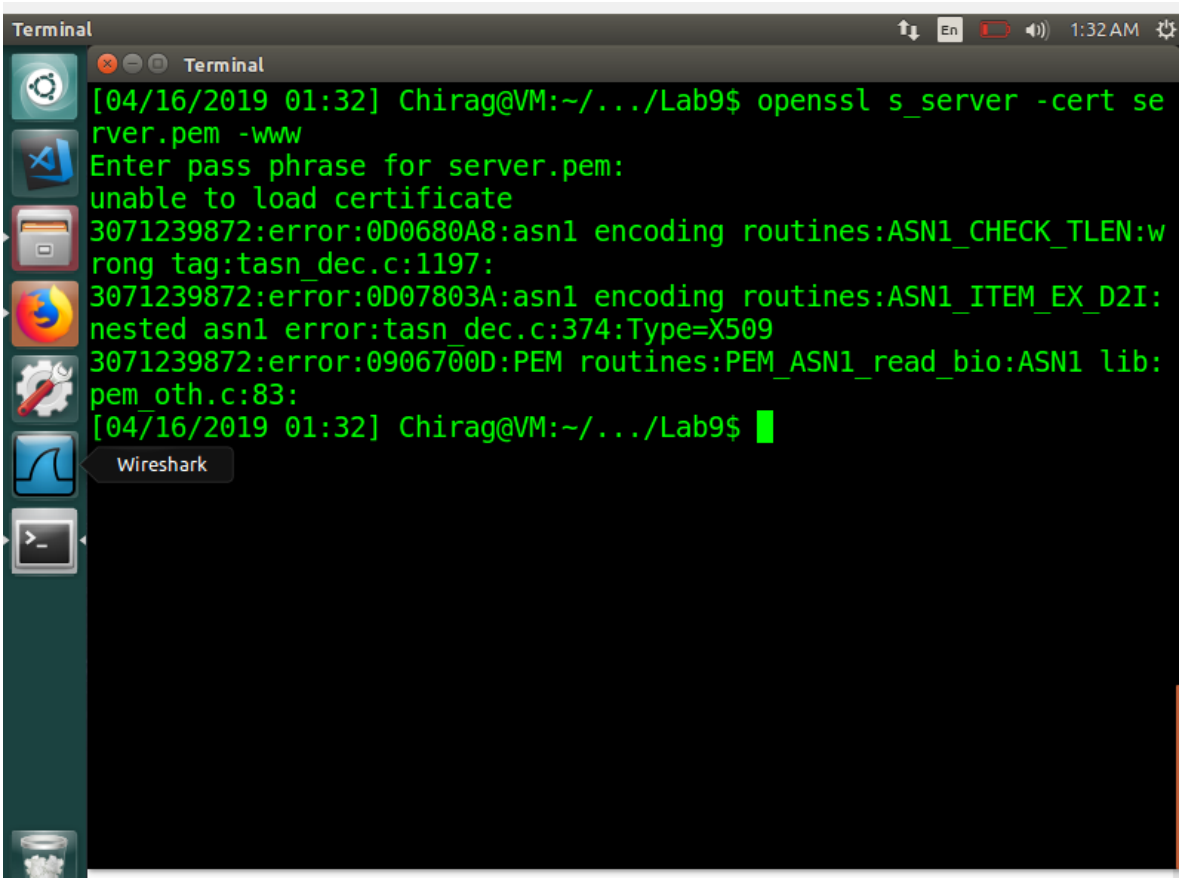
Task 3

Deploying the website from the openssl server.

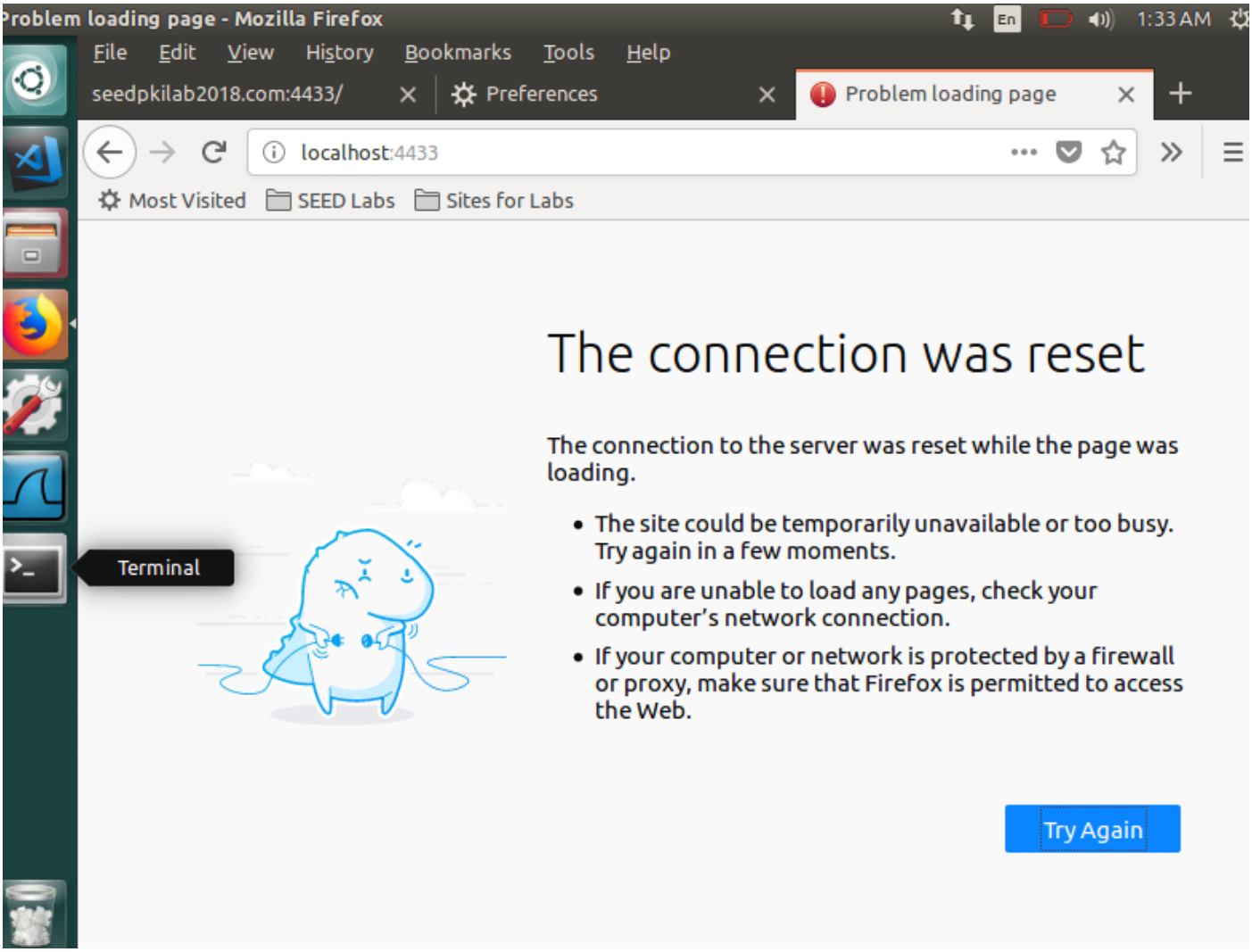


Modifying 1 single byte anywhere in the server.pem file except the encrypted certificate yields no change,

If I made a change in the encrypted certificate area, I get this response.



Connecting via localhost.



The connection isn't successful as the certificate for this site is registered as seedpkilab2018.com, hence accessing the website via the localhost would not work.

Task 4

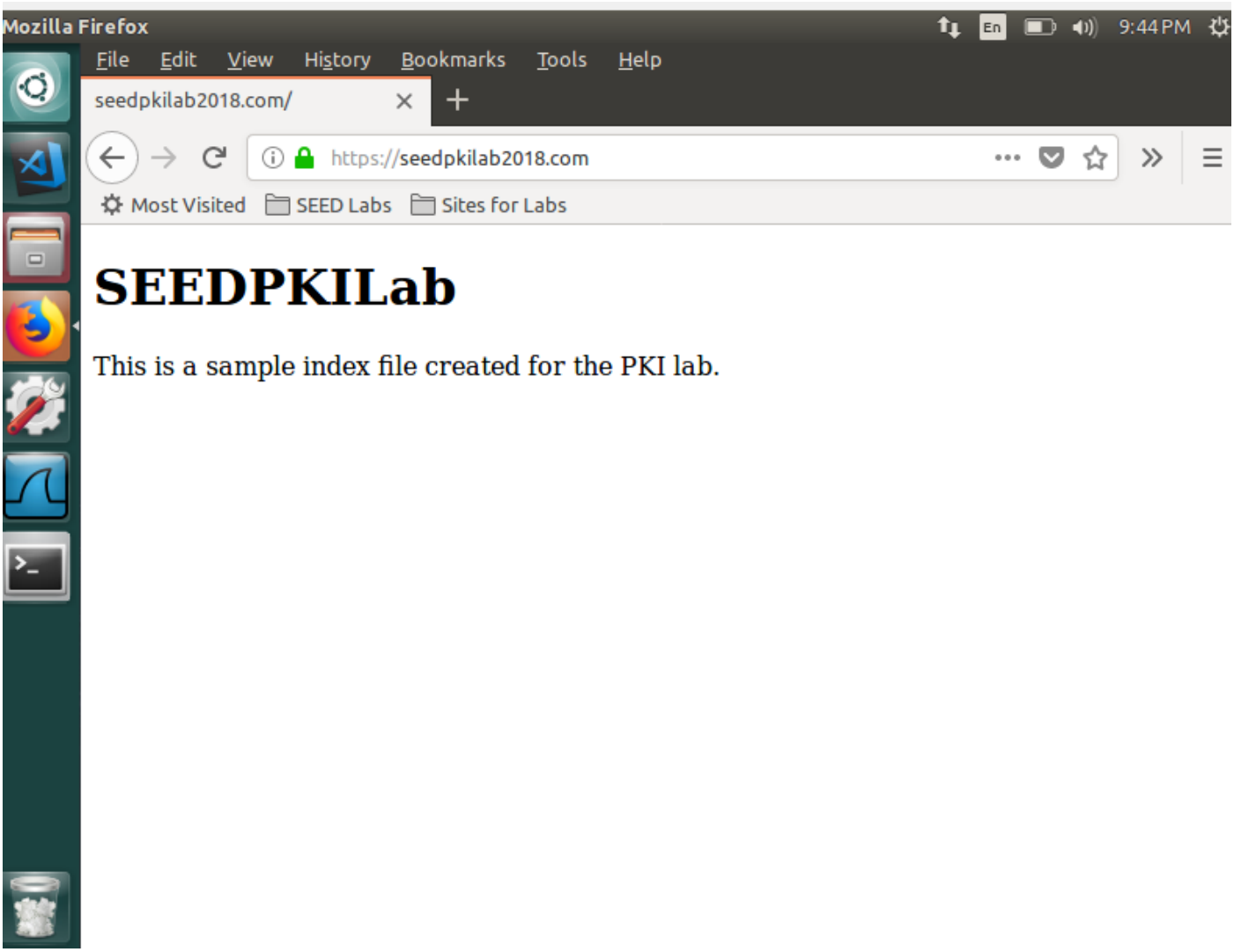
Launching the website on an apache Server

Configuring the default enabled sites

Adding a virtual host to the configuration files.

```
132
133     <VirtualHost *:443>
134         ServerName SEEDPKILab2018.com
135         DocumentRoot /var/www/SEEDPKILab
136         DirectoryIndex index.html
                Wireshark
138         SSLEngine On
139         SSLCertificateFile /home/seed/Desktop/iSec/Lab9/server.pem
140         SSLCertificateKeyFile /home/seed/Desktop/iSec/Lab9/server-
    key.pem
141     </VirtualHost>
```

After modifying the configuration files and enabling the site added, we visit the website.



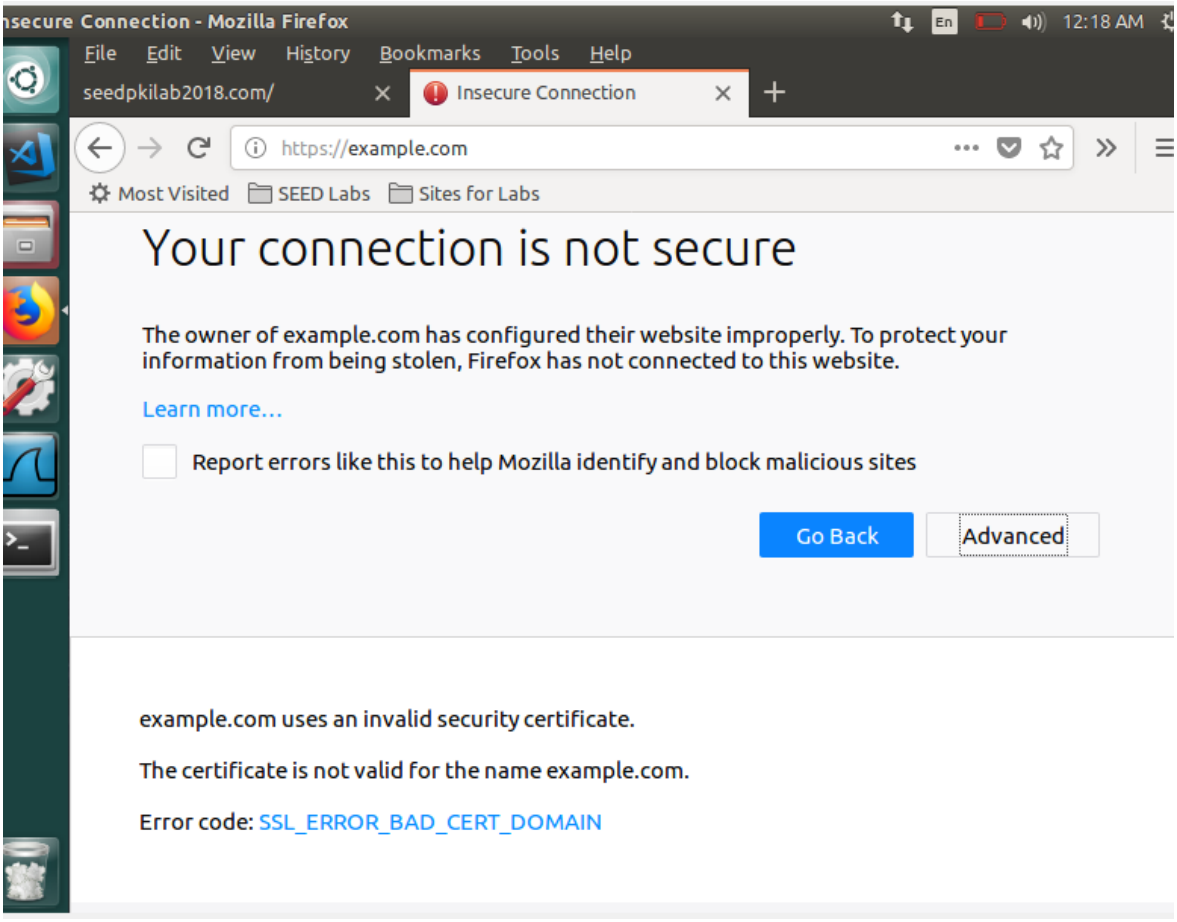
We can successfully browse the website.

Task 5

Man in the middle attack

Adding a website for example.com in the configuration files for apache

```
142
143     <VirtualHost *:443>
144         ServerName example.com
145         DocumentRoot /var/www/SEEDPKILab
146         DirectoryIndex index.html
147
148         SSLEngine On
149         SSLCertificateFile /home/seed/Desktop/iSec/Lab9/server-
    example.pem
150         SSLCertificateKeyFile /home/seed/Desktop/iSec/Lab9/server-
    key.pem
151     </VirtualHost>
152
```



The attack is not successful as the certificate used for example.com was issues for Seedpkilab2018.com, hence the browser recognizes this and flags the connection as insecure.

Task 6

Launching the man in the middle attack with the compromised ca.

We issue a fake certificate for example.com pointing it to our malicious website,

The browser recognizes the ca and hence believes that this is the actual certificate for example.com