

PKI Lab

CSE644

Internet Security

Chirag Sachdev

680231131

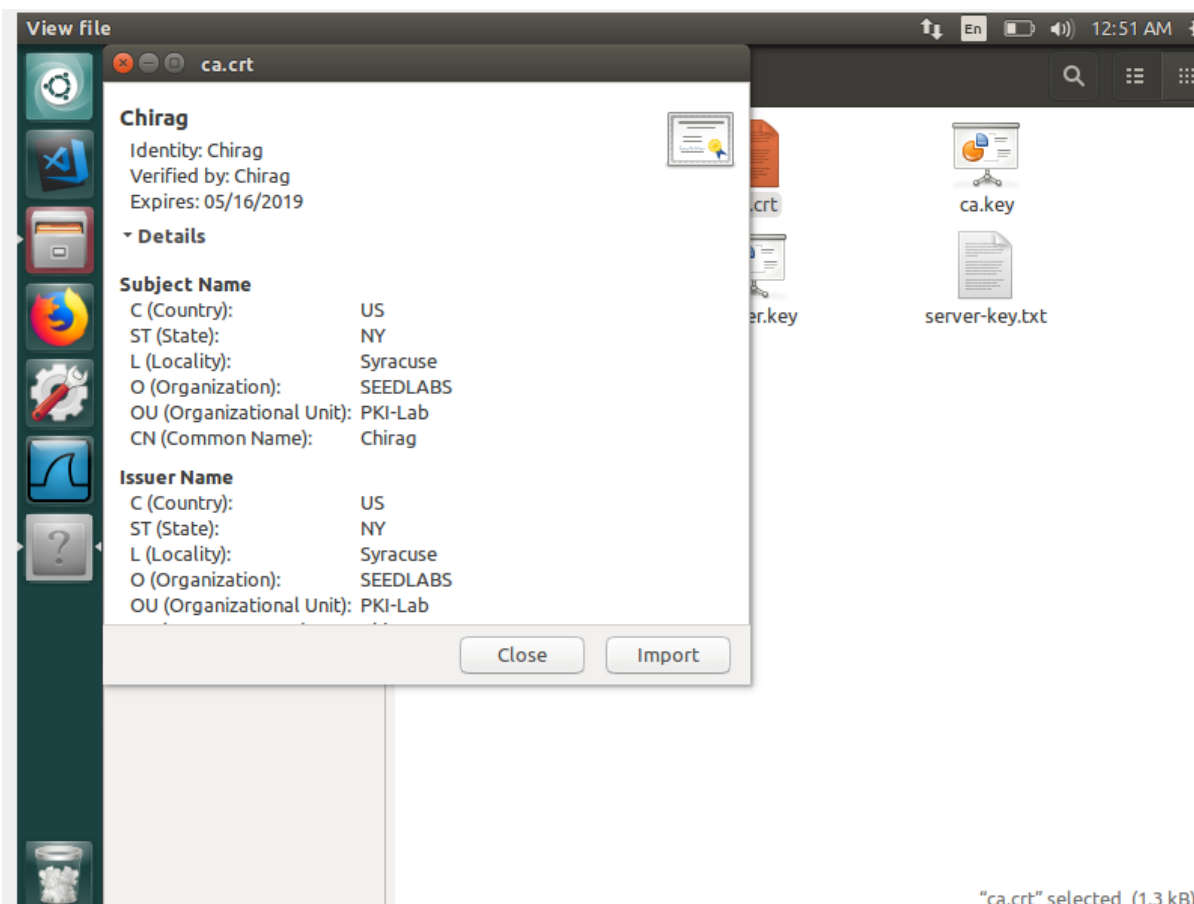
## Task 1

Creating a ca.crt file by becoming a CA.

Setting up the directories

```
Terminal
[04/16/2019 00:50] Chirag@VM:~/../demoCA$ ll
total 12
drwxrwxr-x 2 seed seed 4096 Apr 16 00:44 certs
drwxrwxr-x 2 seed seed 4096 Apr 16 00:44 crl
-rw-rw-r-- 1 seed seed   0 Apr 16 00:45 index.txt
drwxrwxr-x 2 seed seed 4096 Apr 16 00:45 newcerts
-rw-rw-r-- 1 seed seed   0 Apr 16 00:45 serial
[04/16/2019 00:50] Chirag@VM:~/../demoCA$
```

The certificate created:



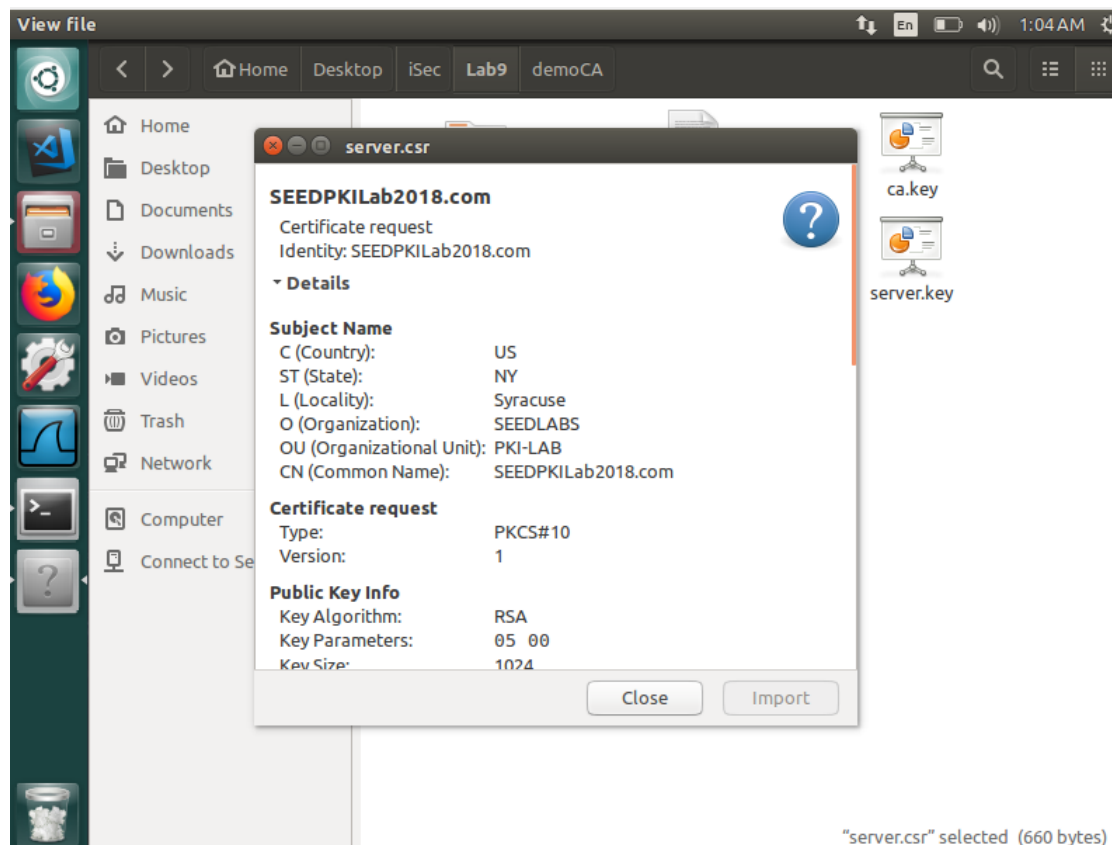
"ca.crt" selected (1.3 kB)

## Task 2

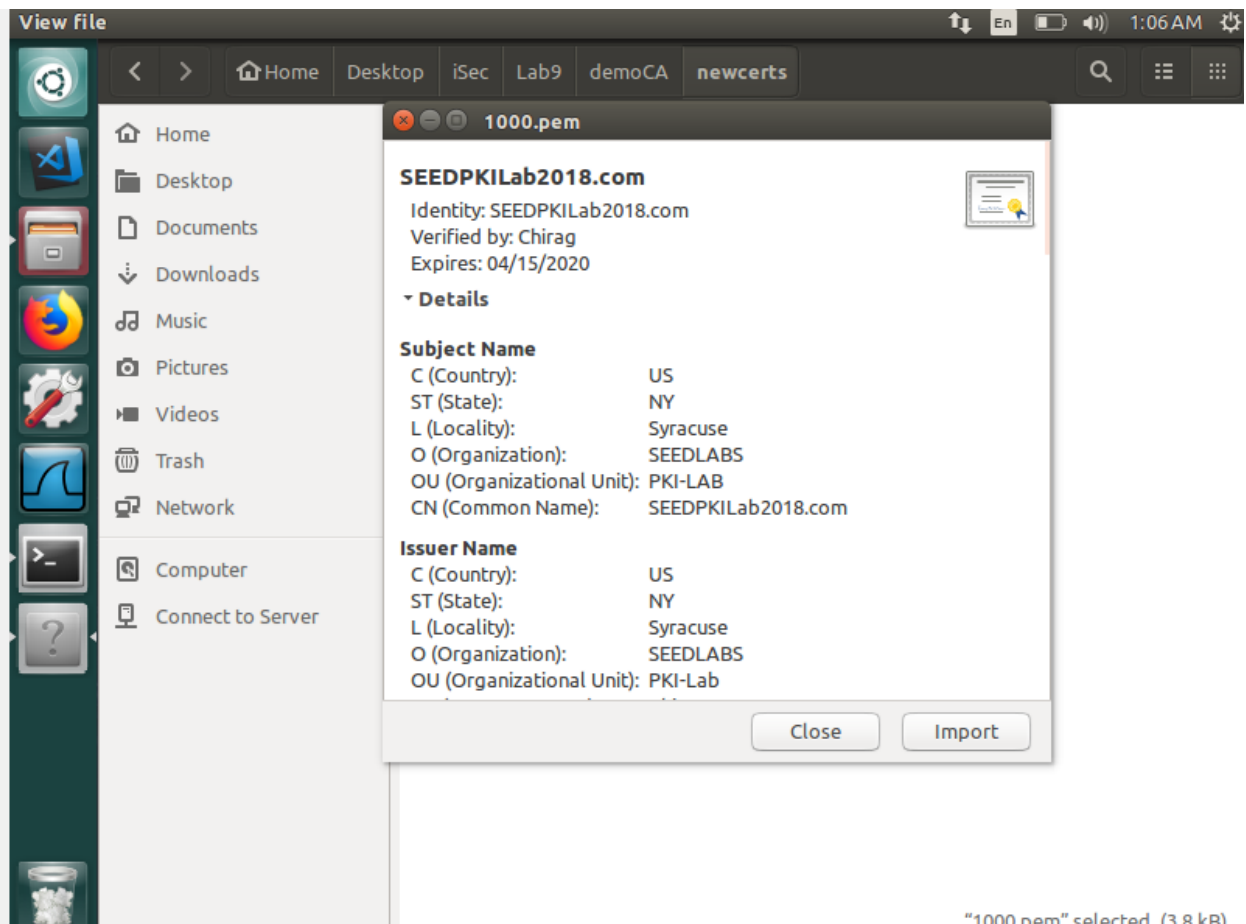
### Generating public/private key pair

```
server-key.txt (~/Desktop/iSec/Lab9) - gedit
1 Private-Key: (1024 bit)
2 modulus:
3 00:da:7f:23:8d:74:45:8a:71:9e:87:32:27:81:c3:
4 cd:a2:bc:d3:3c:0b:eb:7e:57:4e:19:50:6b:ab:e7:
5 cd:bf:38:db:1d:52:24:b3:02:94:56:10:e0:0c:e3:
6 65:29:9f:5e:4f:33:10:b8:7f:4a:0b:70:f6:cb:69:
7 26:52:9e:30:2b:48:d5:df:d1:57:3f:0a:2a:bc:66:
8 c4:37:7d:27:63:de:ec:f0:04:f7:81:31:d8:a3:8d:
9 a2:65:78:ef:d9:6f:0a:e6:6d:1e:cd:d4:26:cd:e5:
10 4d:09:9d:ea:7b:9f:c6:6d:cf:02:90:ec:d1:6d:d1:
11 90:8e:67:85:83:a4:52:9e:35
12 publicExponent: 65537 (0x10001)
13 privateExponent:
14 00:c2:cc:89:28:eb:19:b8:c5:75:7d:b9:64:69:97:
15 e5:35:0a:be:15:11:d7:81:cb:5a:90:cd:17:41:ab:
16 27:cf:2d:64:84:ee:a0:53:8c:a0:2d:5f:5c:31:81:
17 66:c6:c6:14:31:ee:28:21:25:33:21:a2:34:15:c4:
18 08:6b:ae:26:e8:3a:88:a0:59:0e:fb:58:7d:3b:02:
19 60:80:d8:b1:a4:96:f1:9b:04:fa:0c:b9:d3:c5:2e:
20 c8:05:a2:eb:2f:a4:07:73:20:4f:bb:b2:b7:bb:2c:
21 08:a3:45:cc:5e:0d:44:26:f4:d8:96:4f:5b:22:a3:
22 57:a3:c5:31:ad:d0:a1:ea:21
23 prime1:
24 00:ef:1c:f1:f9:5a:cb:6d:5f:9a:77:cb:09:02:d6:
25 7d:b2:c8:0f:b6:df:fd:73:80:91:81:04:2a:f7:2b:
26 3b:27:3a:12:3b:c5:66:1d:ac:ff:ee:73:12:8b:7a:
27 48:5b:5f:d0:fa:1c:2d:c4:3e:4a:7b:2b:4a:bd:f7:
```

### Generating the server signing request.

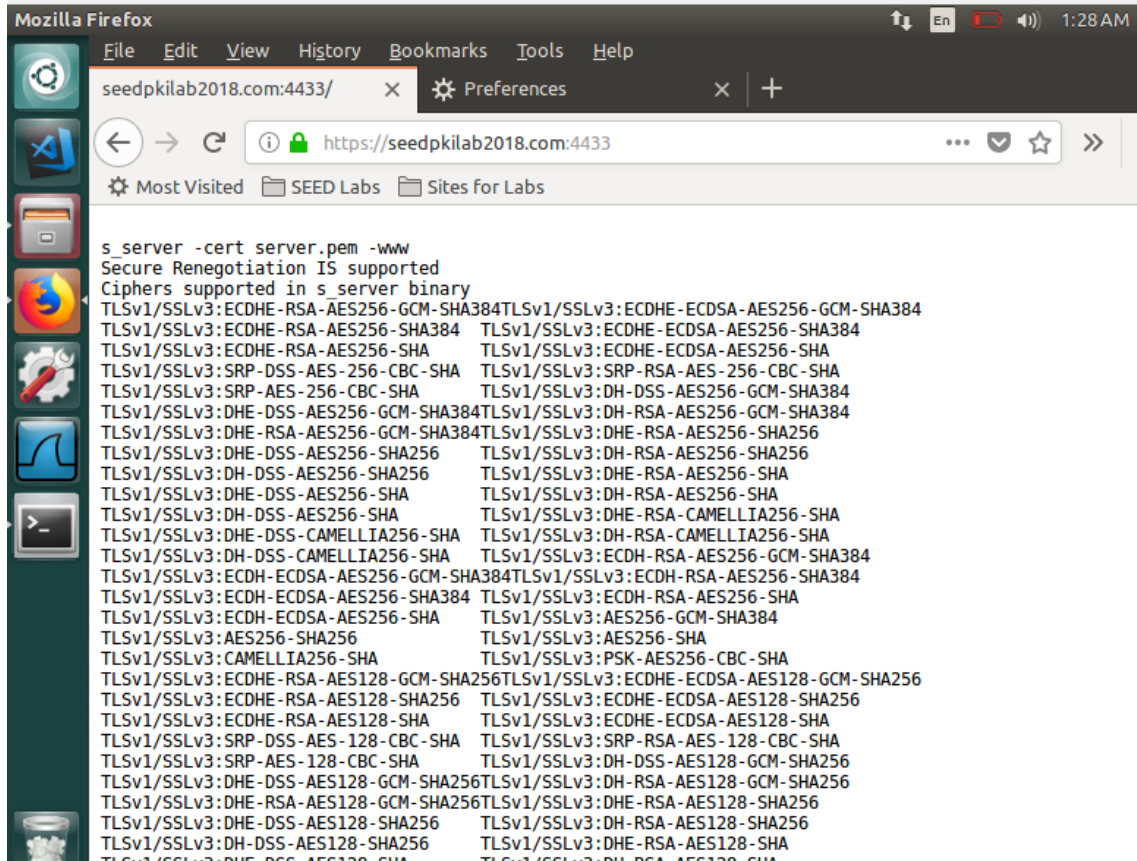


## Generating the server from the request



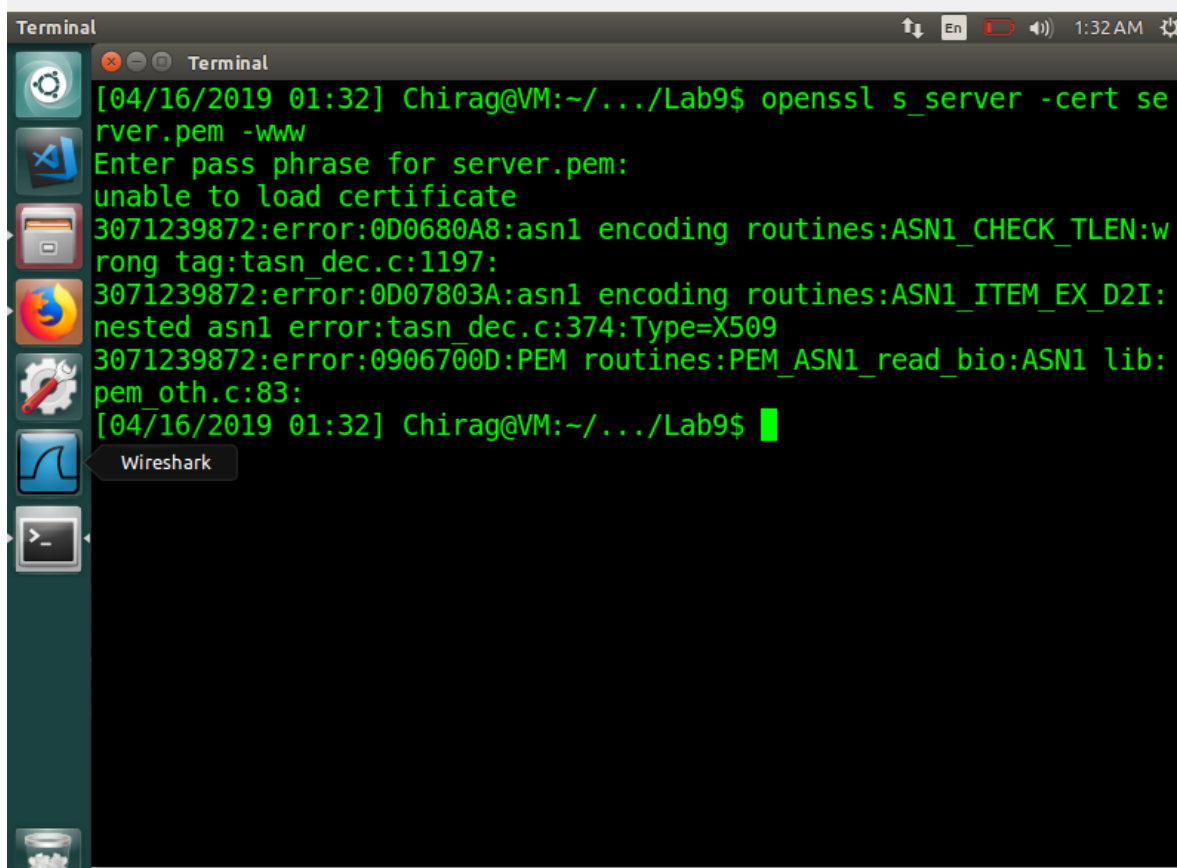
### Task 3

Deploying the website from the openssl server.

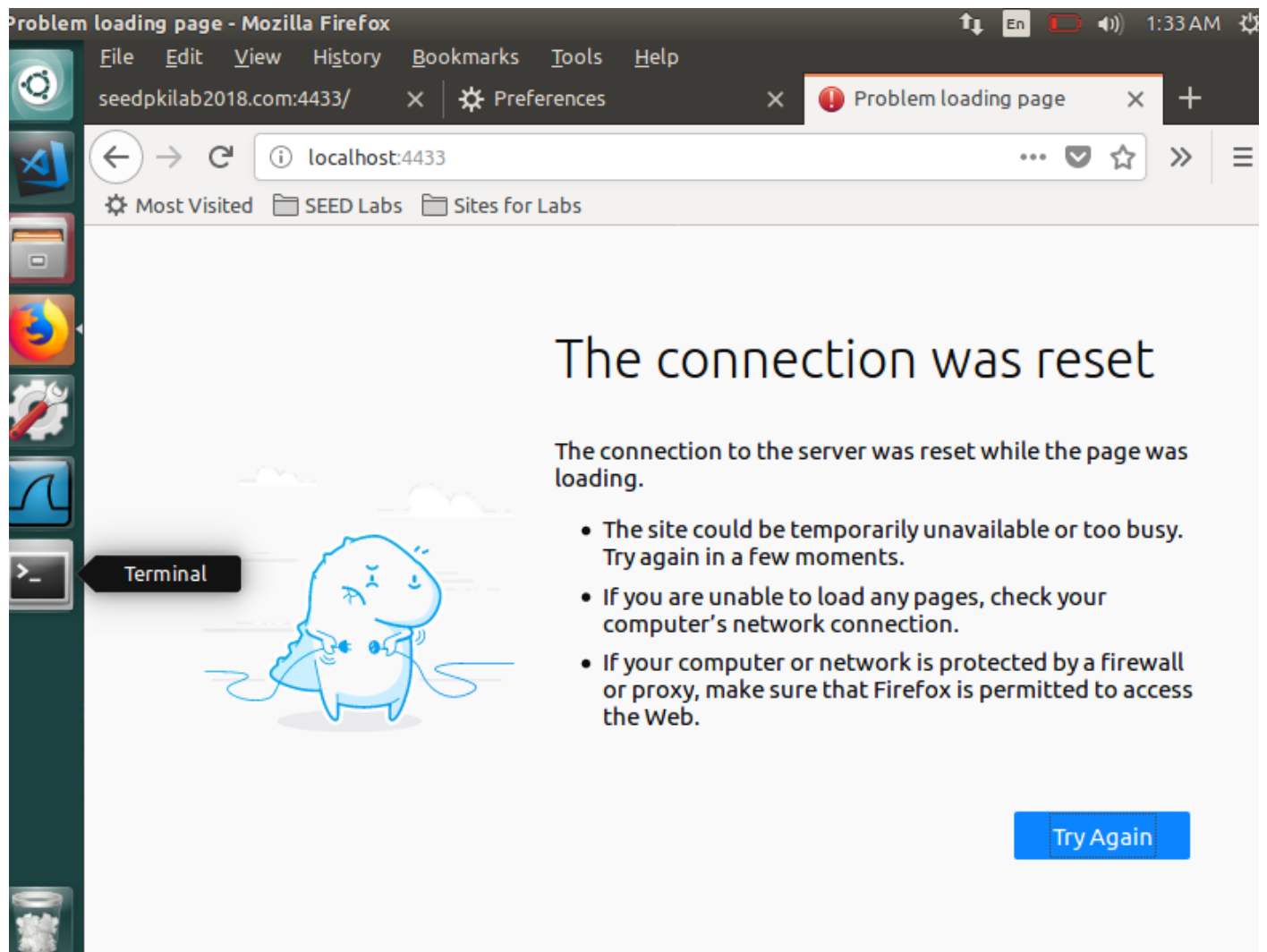


Modifying 1 single byte anywhere in the server.pem file except the encrypted certificate yields no change,

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

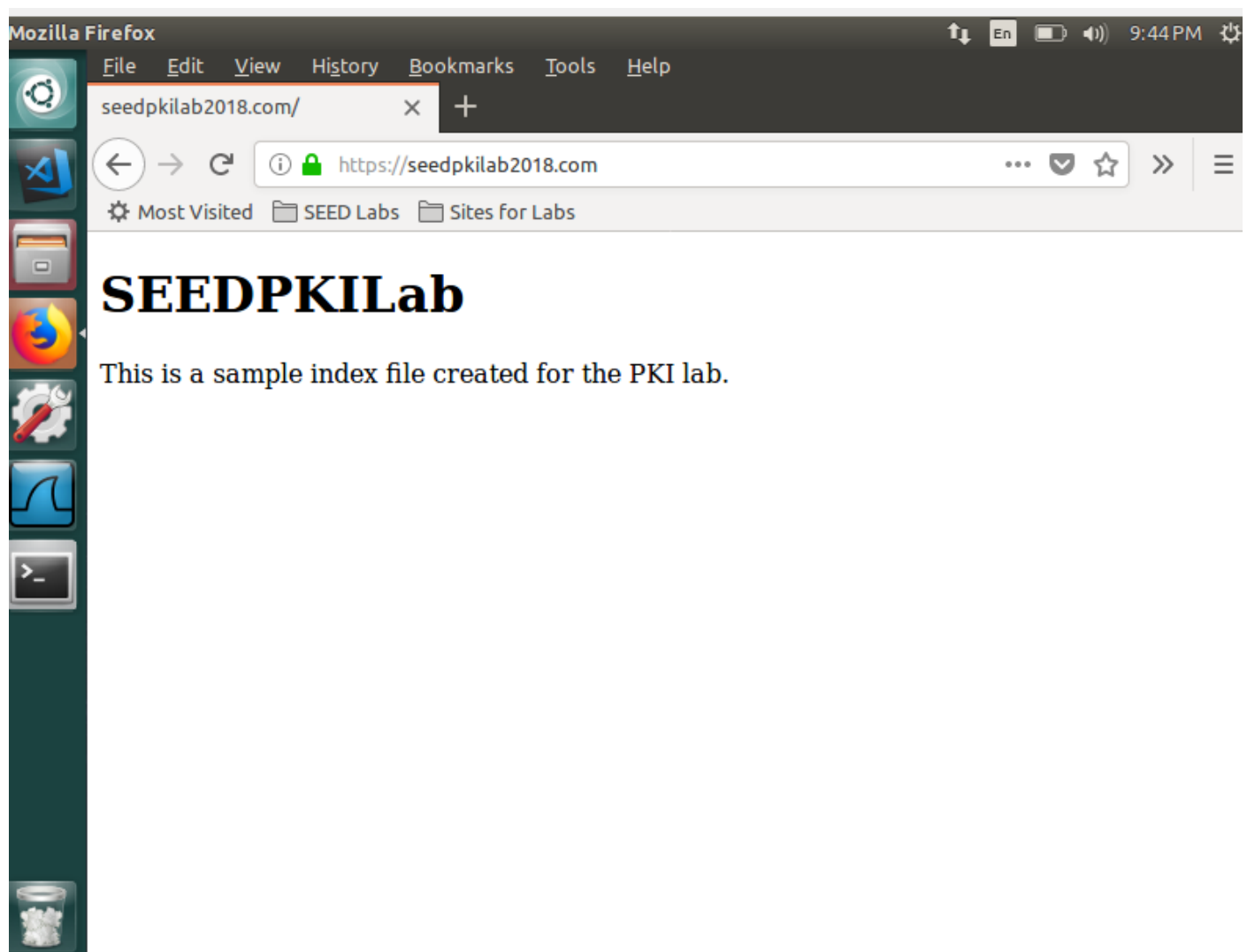
Launching the website on an apache Server

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
137
138         SSLEngine On
139         SSLCertificateFile /home/seed/Desktop/iSec/Lab9/server.pem
140         SSLCertificateKeyFile /home/seed/Desktop/iSec/Lab9/server-
141         key.pem
142     </VirtualHost>
```

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



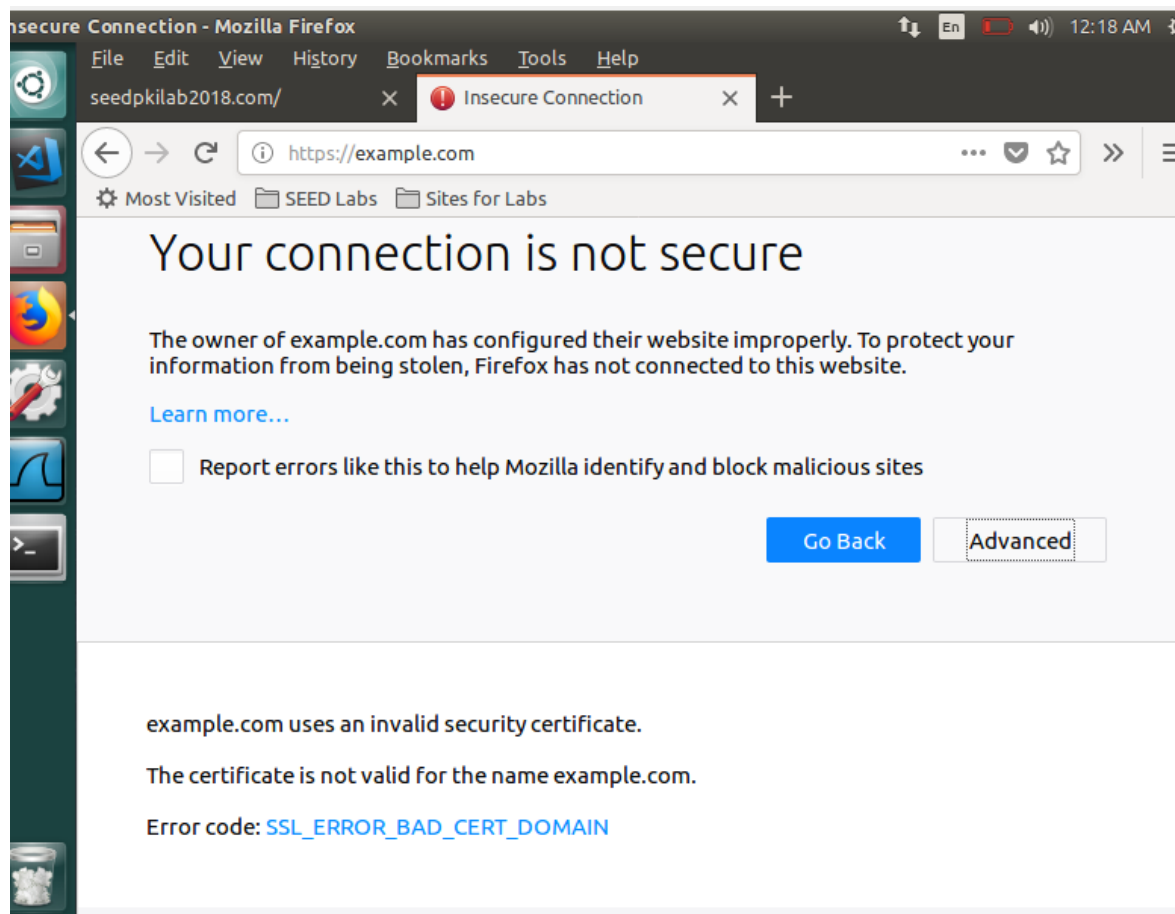
We can successfully browse the website.

## 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 issued 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

