1-Configure SSL (https) site in apache2

- To configure apache for SSL

1-Generate key pairs (public, private)

- Generate private key

  $ openssl genrsa -out mykey.priv 2048

- Generate public key

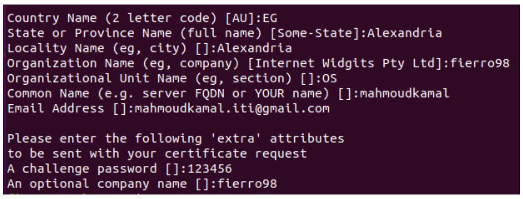
  $ openssl rsa -in mykey.priv -pubout > mykey.pub

- Secure private key

  $ chmod o-r mykey.priv

2-Generate CSR

$ openssl req -new -key mykey.priv -out mycsr.csr



```
Country Name (2 letter code) [AU]:EG
State or Province Name (full name) [Some-State]:Alexandria
Locality Name (eg, city) []:Alexandria
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fierro98
Organizational Unit Name (eg, section) []:OS
Common Name (e.g. server FQDN or YOUR name) []:mahmoudkamal
Email Address []:mahmoudkamal.iti@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:fierro98
```

3-Pay for the certificate or use self-signed certificate

$ openssl x509 -req -days 365 -in mycsr.csr -signkey mykey.priv -sha256 -out mycert.crt

4-Configure apache2 for SSL

- Enable apache for ssl

  $ sudo a2enmod ssl

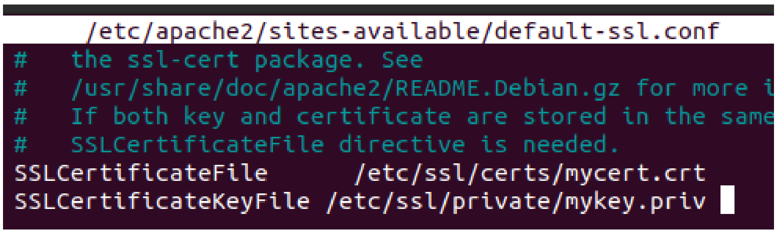
- Configure the SSL virtualhost /etc/apache2/sites-available/default-ssl.conf

  Change certifictes paths SSLCertificateFile,SSLCertificateKeyFile

  $ sudo cp mycert.crt /etc/ssl/certs

  $ sudo cp mykey.priv /etc/ssl/private

  $ sudo nano /etc/apache2/sites-available/default-ssl.conf



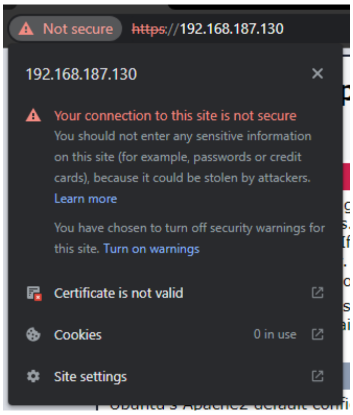
```
        /etc/apache2/sites-available/default-ssl.conf
#    the ssl-cert package. See
#    /usr/share/doc/apache2/README.Debian.gz for more i
#    If both key and certificate are stored in the same
#    SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/mycert.crt
SSLCertificateKeyFile /etc/ssl/private/mykey.priv
```

- Enable SSL Site

  $ sudo a2ensite default-ssl

- Restart

  $ sudo service apache2 restart



Not secure ~~https~~://192.168.187.130

192.168.187.130

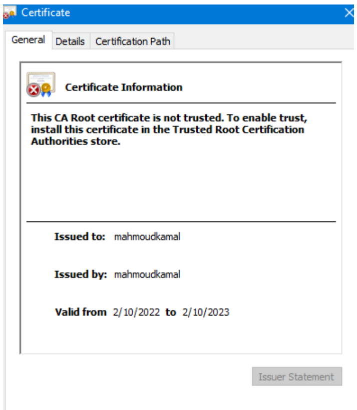
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

Certificate is not valid

Cookies 0 in use



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: mahmoudkamal

Issued by: mahmoudkamal

Valid from 2/10/2022 to 2/10/2023

2-SQL MAP to apply sql injection

Running an SQL injection attack scan with sqlmap:

```
$ sqlmap.py -u “<URL>” --batch --banner
```

A small change in the command will run the same battery of tests but by using a POST as a test method instead of a GET.

Try the following command:

```
$ sqlmap.py -u “<URL>” --data=“id=1” --banner
```

Password cracking with sqlmap

```
$ sqlmap.py -u “<URL>” --batch --password
```

Get a list of databases on your system and their tables

```
$ sqlmap.py -u “<URL>” --batch --dbs
```

References:

https://www.comparitech.com/net-admin/sqlmap-cheat-sheet/

https://cdn.comparitech.com/wp-content/uploads/2021/07/sqlmap-Cheat-Sheet.pdf

https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/