Application Security

LAB1

Ingy Mahmoud El-Sakhawy

1- Install mod_ssl:

```
[ingy@localhost ~]$ sudo yum install mod_ssl
Updating Subscription Management repositories.
Red Hat Enterprise Linux 9 for x86_64 - BaseOS   10 kB/s | 4.1 kB     00:00
Red Hat Enterprise Linux 9 for x86_64 - BaseOS  2.7 MB/s |  18 MB     00:06
Red Hat Enterprise Linux 9 for x86_64 - AppStre 9.4 kB/s | 4.5 kB     00:00
Red Hat Enterprise Linux 9 for x86_64 - AppStre 2.8 MB/s |  29 MB     00:10
Last metadata expiration check: 0:00:03 ago on Sat 09 Mar 2024 08:03:38 PM EET.
Dependencies resolved.
```

2- Enable the SSL Module:

```
[ingy@localhost ~]$ sudo yum install httpd
Updating Subscription Management repositories.
Last metadata expiration check: 0:03:28 ago on Sat 09 Mar 2024 08:03:38 PM EET.
Dependencies resolved.
================================================================================
 Package            Arch   Version       Repository                      Size
================================================================================
Installing:
 httpd              x86_64 2.4.57-5.el9  rhel-9-for-x86_64-appstream-rpms  52 k
Installing dependencies:
 redhat-logos-httpd noarch 90.4-2.el9    rhel-9-for-x86_64-appstream-rpms  18 k
Installing weak dependencies:
 mod_http2          x86_64 1.15.19-5.el9 rhel-9-for-x86_64-appstream-rpms 152 k
 mod_lua            x86_64 2.4.57-5.el9  rhel-9-for-x86_64-appstream-rpms  62 k
```

3- Create Private Key and Certificate:

```
[ingy@localhost ~]$ sudo openssl req -new -key /etc/pki/tls/private/mypriv.key -
out /etc/pki/tls/certs/mycert.csr
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]:eg
State or Province Name (full name) []:egypt
Locality Name (eg, city) [Default City]:alexandria
Organization Name (eg, company) [Default Company Ltd]:none
Organizational Unit Name (eg, section) []:none
Common Name (eg, your name or your server's hostname) []:ingy
Email Address []:none

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0000
An optional company name []:none
```

```
[ingy@localhost certs]$ sudo cat mycert.csr
-----BEGIN CERTIFICATE-----
MIIDbzCCAlcCFGaPSV+EMfebv6MvRQ07eLU+USbTMA0GCSqGSIb3DQEBCwUAMHQx
CzAJBgNVBAYTAmVnMQ4wDAYDVQQIDAVlZ3lwdDETMBEGA1UEBwwKYWxleGFuZHJp
YTENMAsGA1UECgwEbm9uZTENMAsGA1UECwwEbm9uZTENMAsGA1UEAwwEaW5neTET
MBEGCSqGSIb3DQEJARYEbm9uZTAeFw0yNDAzMDkxODIzMzZaFw0yNTAzMDkxODIz
MzZaMHQxCzAJBgNVBAYTAmVnMQ4wDAYDVQQIDAVlZ3lwdDETMBEGA1UEBwwKYWxl
eGFuZHJpYTENMAsGA1UECgwEbm9uZTENMAsGA1UECwwEbm9uZTENMAsGA1UEAwwE
aW5neTETMBEGCSqGSIb3DQEJARYEbm9uZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMFcARyA9xuQfONbGIkiaSdEpd23voNEczEZ/0yipSKZKHi7OPM8
+CJGhI5TMqUPV1BuK6hWg8ELgyru24eTW4HFe+nPfIiPMBdnxuA8c0wCoWbD2n6I
auQAAy0DkZZWftkdZ+X5rj25FXHr1gVz6N121TPC2sIeFYGSAgktITf6F/v4hVyI
sQlthoK0x+g+vXMV+IHR6ALNvEmIHoPgKBkEbBwvPJ7kheLRHEvyxgkwfk2j+p8i
lIo30q8wzYFXWvLLy21Twl92vasBnZOb22UZoekrgomrOiq71B7kk6+1pa5eXQec
agVrabAu0WWjmqbQFUKLO/gcZq/qYDFw29ECAwEAATANBgkqhkiG9w0BAQsFAAOC
AQEAKvXt0odQi6LpqnnQtqN5wmDlClckZXZCuhs7dypbjDtx5uYYaB3cujMmPN9U
1drsqyExg9xi8Bz37pUnpGNQkk9JAeh014K2tuCECFPAqo2lnCTPWL4C8zMs98Q4
jhnxRMfbsNnkMcII3tpXQ6N8kFUuv26lRgNZNKHUEgTBDVALhYRzW6CRUd1o2mhe
5+3iydrPf1ePaxfvMKh/SDRBL5LfU73NyXFAe9cB1FwhhruslYYvDMyLmZB9nN1q
NlFfGBy6JmOE2NNYhb4cMyoyghI7+Wj4ZeSFqJUMDOOYvtlQ40m2hz0NaBKhG5hq
iC0GuCXZ0MeNphKeCXXKW0utHw==
-----END CERTIFICATE-----
```

4- Generate a private key

successfully generated and the self-signed certificate mycert.crt

```
[ingy@localhost ~]$ sudo openssl x509 -req -days 365 -in /etc/pki/tls/certs/myce
rt.csr -signkey /etc/pki/tls/private/mypriv.key -out /etc/pki/tls/certs/mycert.c
rt
Certificate request self-signature ok
subject=C = eg, ST = egypt, L = alexandria, O = none, OU = none, CN = ingy, emai
lAddress = none
```

5- Configure SSL Certificate and Key:

```
SSLCertificateFile /etc/pki/tls/certs/mycert.crt

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#   ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile /etc/pki/tls/private/mypriv.key
```

6- Restarted the apache:

```
[ingy@localhost ~]$ sudo systemctl restart httpd
[ingy@localhost ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: di
     Active: active (running) since Sat 2024-03-09 20:48:01 EET; 1min 15s ago
```

```
[ingy@localhost ~]$ sudo systemctl enable httpd
[ingy@localhost ~]$ sudo systemctl restart httpd
```

7- test my Apache server's HTTPS configuration