Creating a Self-signed Certificate for a private IP (example https://192.168.0.1) :

1. You need OpenSSL installed. For example, on Ubuntu, you could install it by: `sudo apt-get install openssl` (It may already be installed. Type "openssl version" to find out) For Windows, you could try this: https://slproweb.com/products/Win32OpenSSL.html
2. Once OpenSSL is installed, go to OpenSSL prompt by entering 'openssl' on the console (LINUX), or the cmd prompt (WINDOWS).

   $ openssl

   OpenSSL>
3. Now do the following steps to create: Private key, Certificate Request, Self-signing the certificate, and putting it all together, by using the below commands:

i) Create KEY called mydomain.key:

```
OpenSSL> genrsa -out mydomain.key 2048
```

ii) Use the key to create a Certificate request called mydomain.csr You could accept the default options, or specify your own information:

```
OpenSSL> req -new -key mydomain.key -out mydomain.csr
```

iii) use the above to create a certificate:

```
OpenSSL> x509 -req -days 1825 -in mydomain.csr -signkey mydomain.key -out mydomain.crt
```

iv) Put all the above to create a PEM certificate: exit OpenSSL (OpenSSL> q) and go to certificate location and do:

```
$ sudo cat mydomain.key mydomain.crt >> mylabs.com.pem
```

mylabs.com.pem is your self-signed certificate. You can use this in requests like https://192.168.0.1 if your server supports https. Remember to check the port number for https(443).