https.ext - Notepad

File Edit Format View Help

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = localhost
DNS.2 = informatika.dev
```

C:\Windows\system32\cmd.exe

```
E:\laragon\etc\ssl>openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
..............+++++
.........+++++
e is 65537 (0x010001)

E:\laragon\etc\ssl>openssl req -new -key server.key -out server.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) [AU]:
```

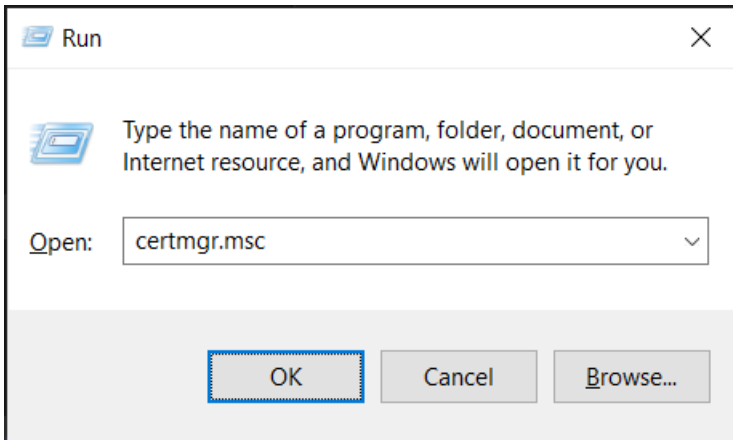
E:\laragon\etc\ssl\makecert.bat - Notepad++

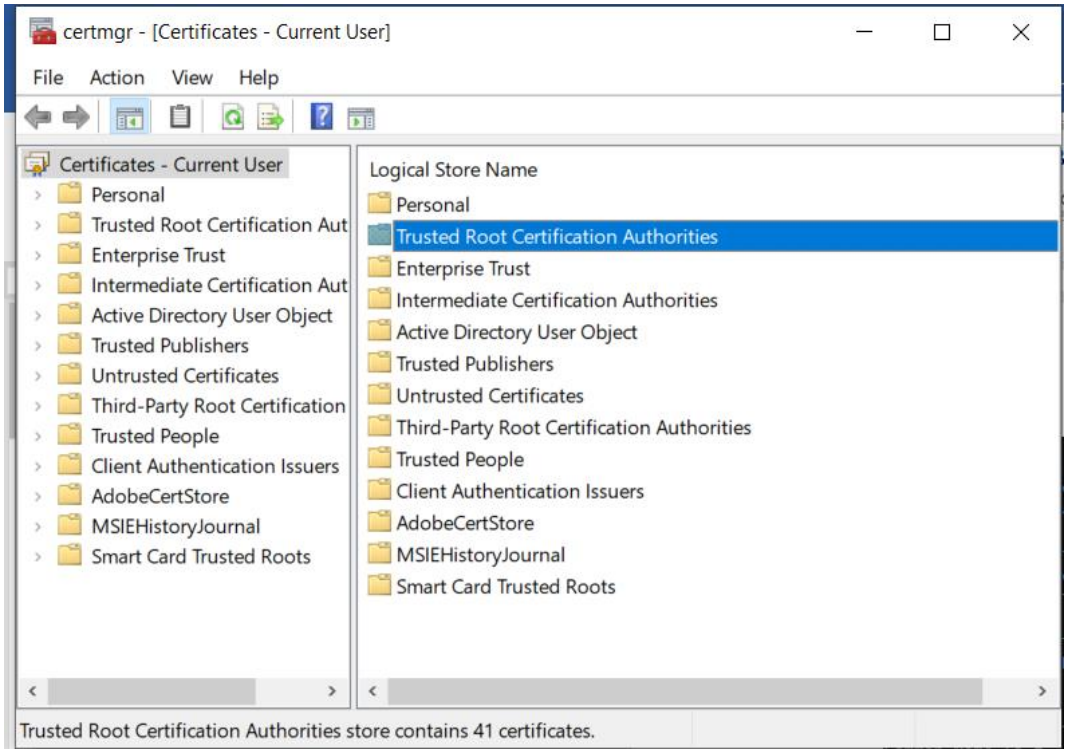
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X

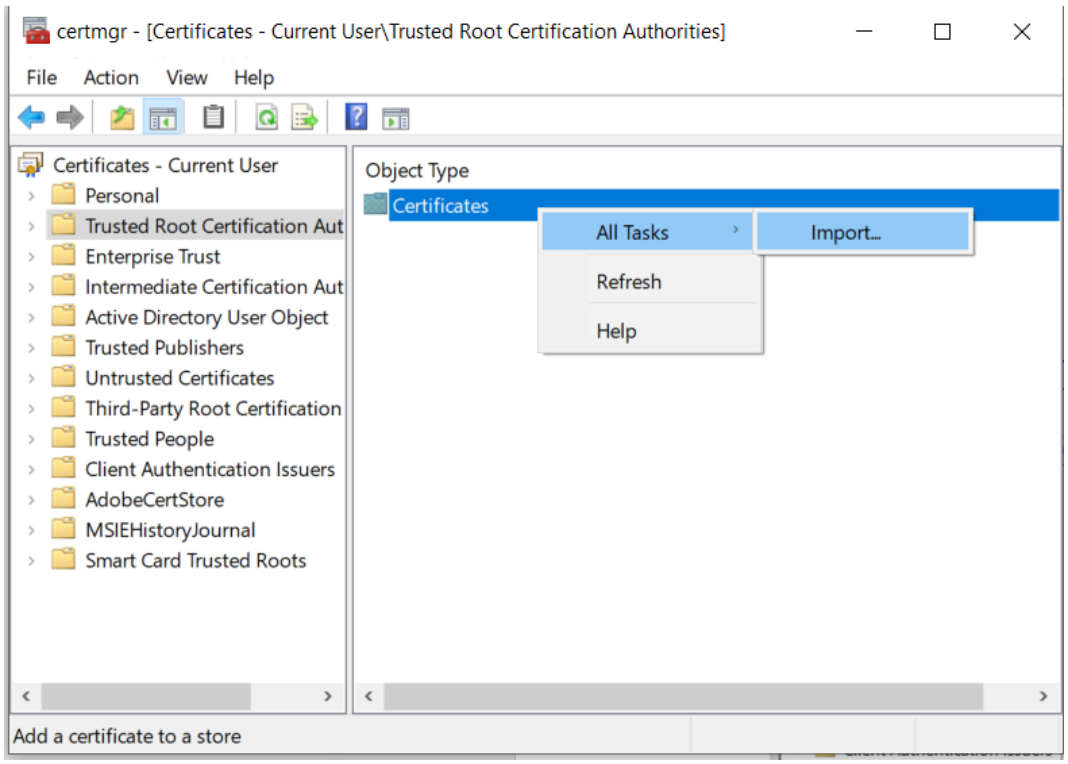
php.ini | makecert.bat

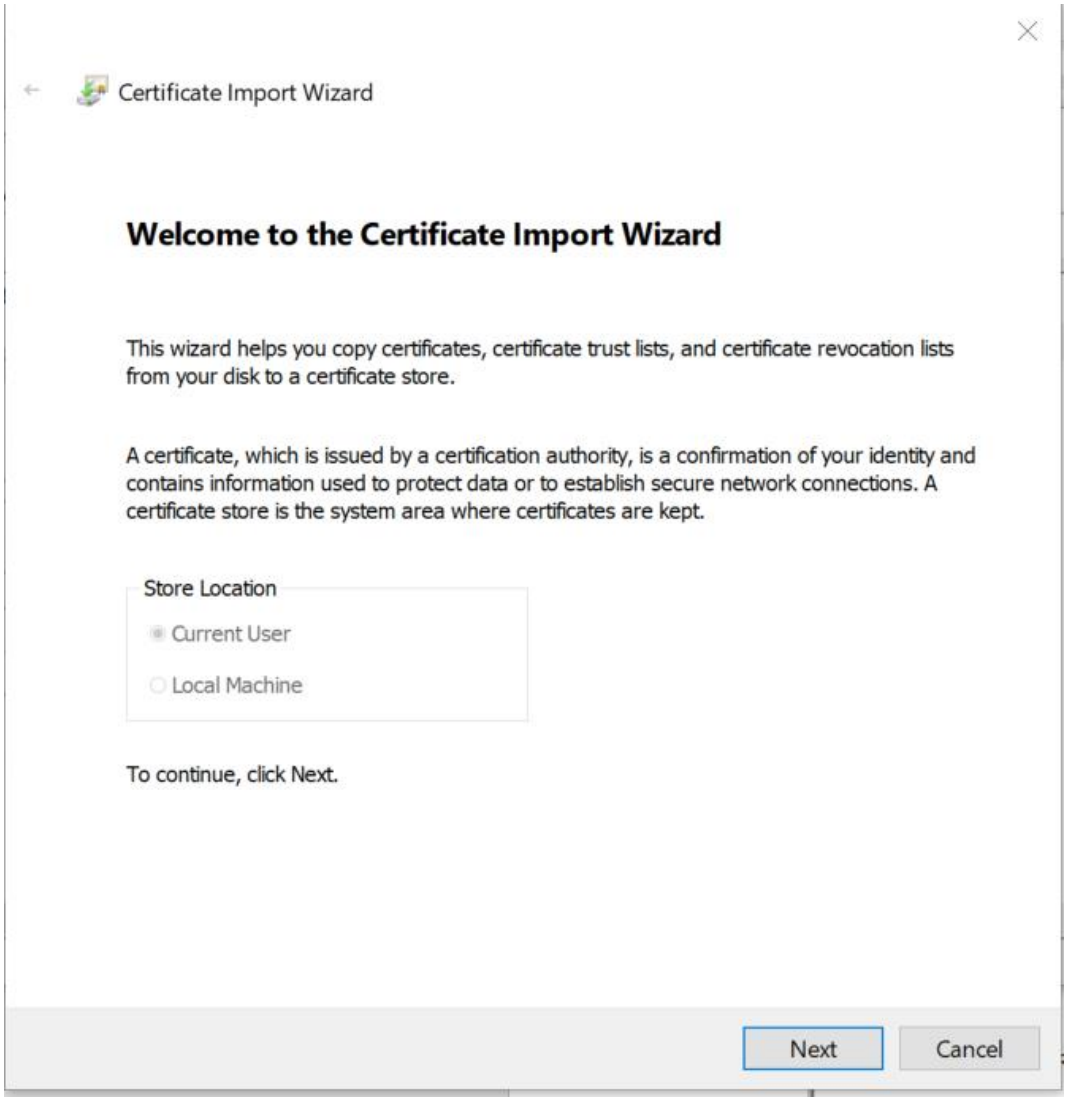
```
1  openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 500
   -sha256 -extfile https.ext
```

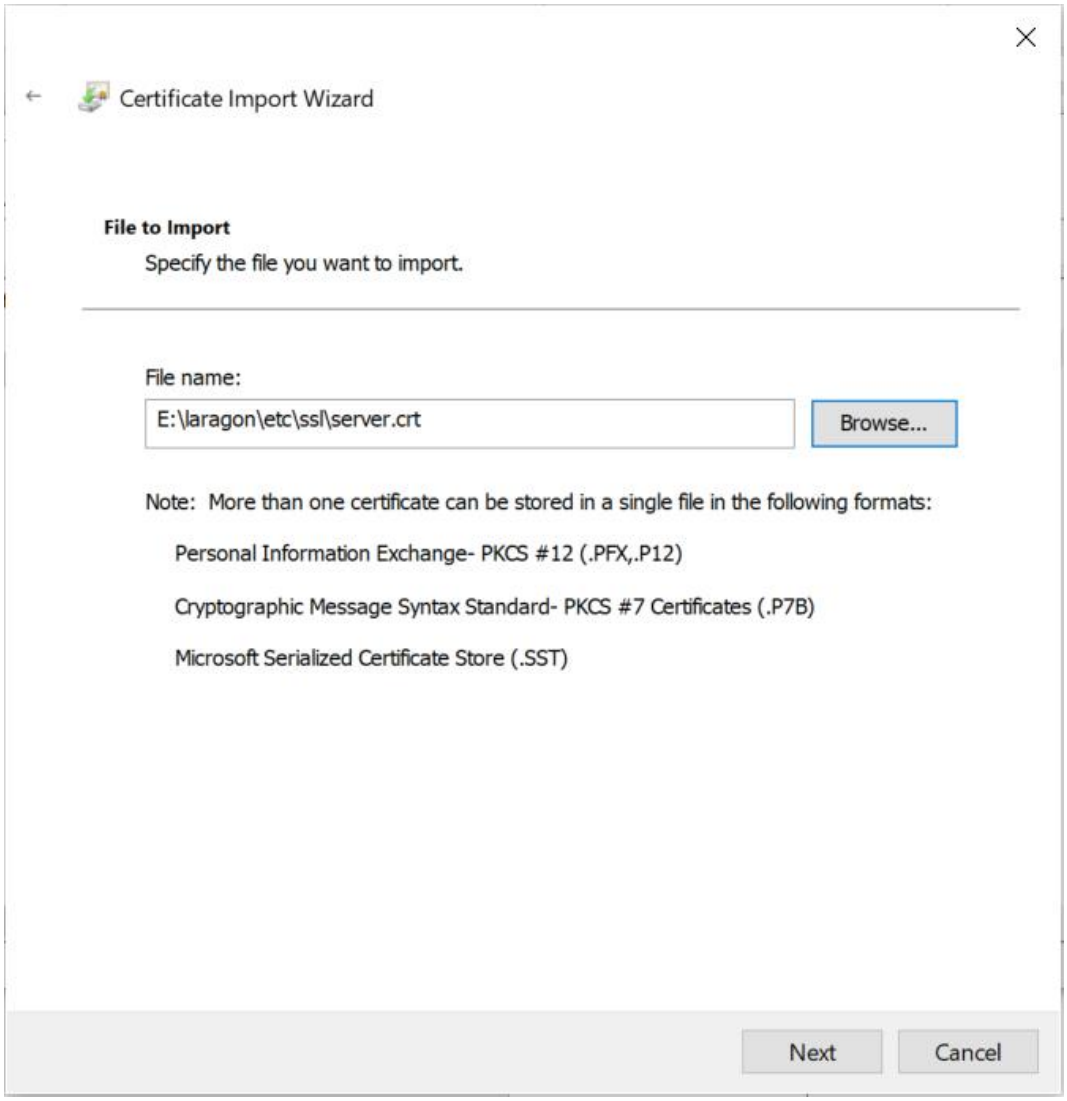
```
E:\laragon\etc\ssl>openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Pontianak
Locality Name (eg, city) []:Kalimantan Barat
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Politeknik Negeri Pontianak
Organizational Unit Name (eg, section) []:Informatika
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:orminela@gmail.com

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

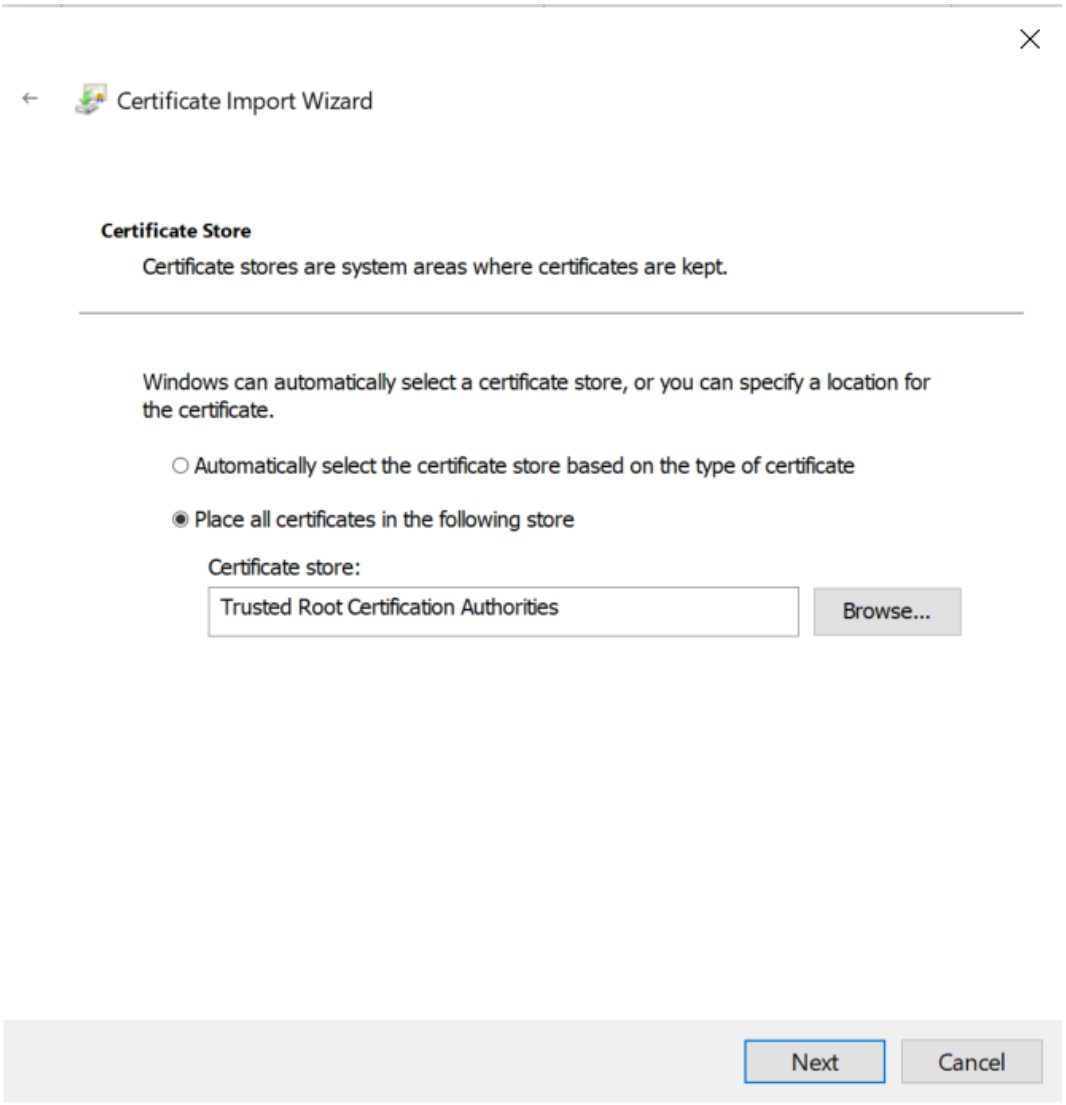


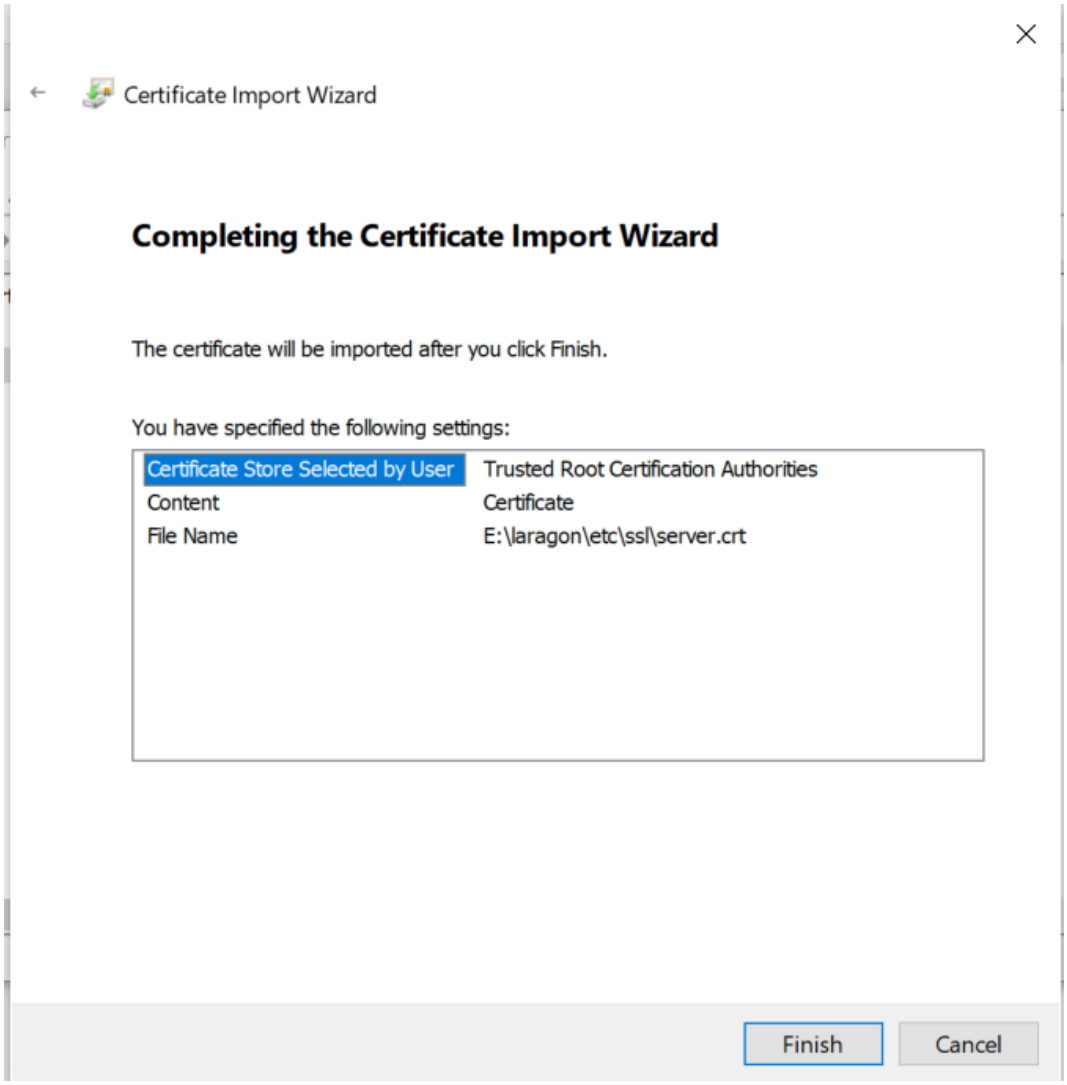

certmgr - [Certificates - Current User]
File Action View Help
Certificates - Current User
Personal
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Aut
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
AdobeCertStore
MSIEHistoryJournal
Smart Card Trusted Roots
Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
AdobeCertStore
MSIEHistoryJournal
Smart Card Trusted Roots
Trusted Root Certification Authorities store contains 41 certificates.

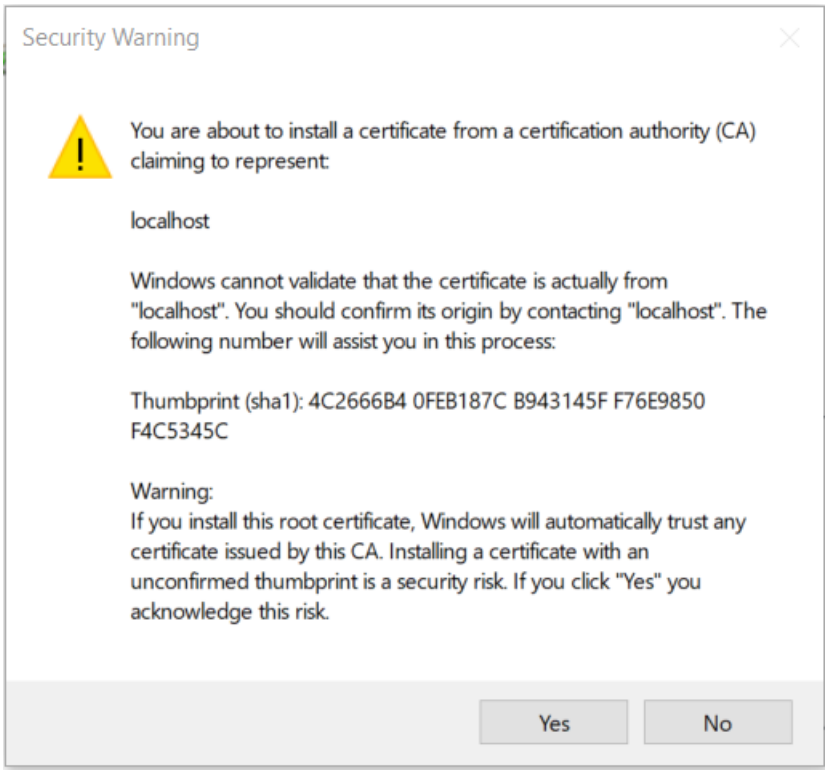

certmgr - [Certificates - Current User\Trusted Root Certification Authorities]
File Action View Help
Certificates - Current User
Personal
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Aut
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
AdobeCertStore
MSIEHistoryJournal
Smart Card Trusted Roots
Object Type
Certificates
All Tasks
Import...
Refresh
Help
Add a certificate to a store

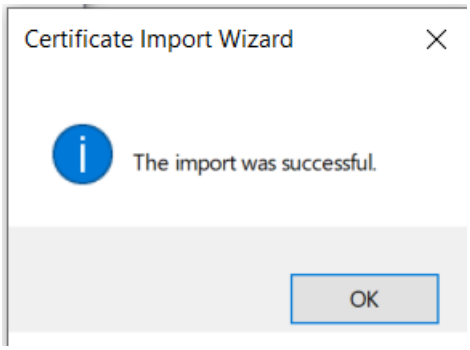

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
E:\laragon\etc\ssl\server.crt
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
File Name
E:\laragon\etc\ssl\server.crt
Finish
Cancel


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
localhost
Windows cannot validate that the certificate is actually from "localhost". You should confirm its origin by contacting "localhost". The following number will assist you in this process:
Thumbprint (sha1): 4C2666B4 0FEB187C B943145F F76E9850 F4C5345C
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Yes
No


Certificate Import Wizard
The import was successful.
OK

E:\laragon\etc\apache2\sites-enabled\00-default.conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

php.ini | makecert.bat | server.key | 00-default.conf

```
24  # match a ServerName or ServerAlias in any <VirtualHost> block.CRLF
25  #CRLF
26  CRLF
27  # First Virtual Host must be a shallow duplicate of the main hostCRLF
28  # in httpd.confCRLF
29  <VirtualHost 127.0.0.1:80>CRLF
30      <Directory "E:/laragon/www/public">CRLF
31          ServerName informatika.devCRLF
32      ServerAlias www.informatika.devCRLF
33      </Directory>CRLF
34  </VirtualHost>CRLF
35  CRLF
36  CRLF
37  <VirtualHost 127.0.0.1:443>CRLF
38      DocumentRoot "C:/xampp/htdocs/private"CRLF
39      ServerName informatika.devCRLF
40      ServerAlias www.informatika.devCRLF
41      SSLEngine onCRLF
42      SSLCertificateFile "C:/xampp/apache/conf/ssl.crt/server.crt"CRLF
43      SSLCertificateKeyFile "C:/xampp/apache/conf/ssl.key/server.key"CRLF
44      <Directory "C:/xampp/htdocs/private">CRLF
45          Options AllCRLF
46          AllowOverride AllCRLF
47          Require all grantedCRLF
48      </Directory>CRLF
49  </VirtualHost>
```

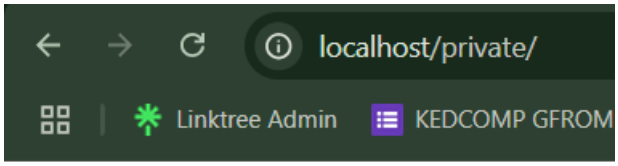
length : 1.510 lines : 49 | Ln : 27 Col : 66 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS

E: > laragon > www > private > index.php

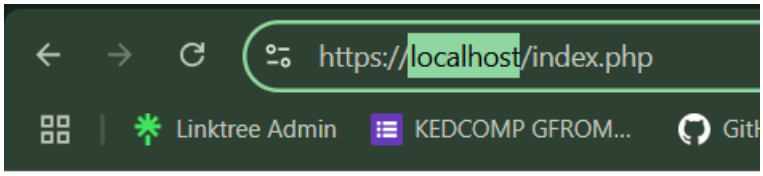
```
1  <?php
2      echo "Akses 127.0.0.1:443"."</br>";;
3      echo "Folder: private";
4  ?>
```

E: > laragon > www > public > index.php

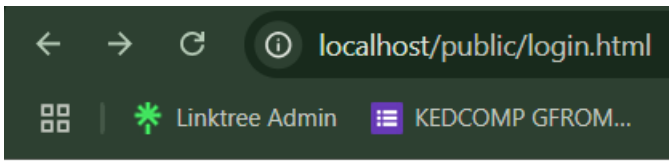
```
1  <?php
2      echo "Akses 127.0.0.1:80"."</br>";
3      echo "Folder: Publik";
4  ?>
```



Akses 127.0.0.1:443
Folder: private



Akses 127.0.0.1:443
Folder: private

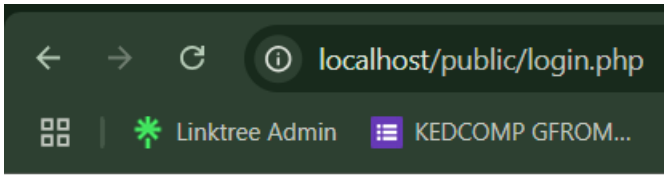


Login Page Public

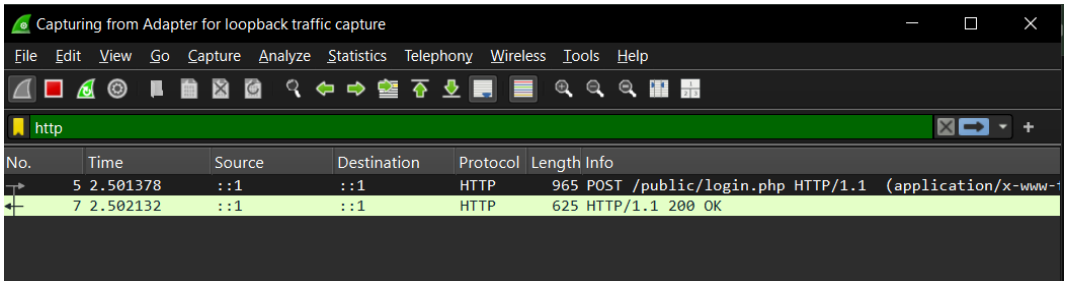
Username:
3202216065

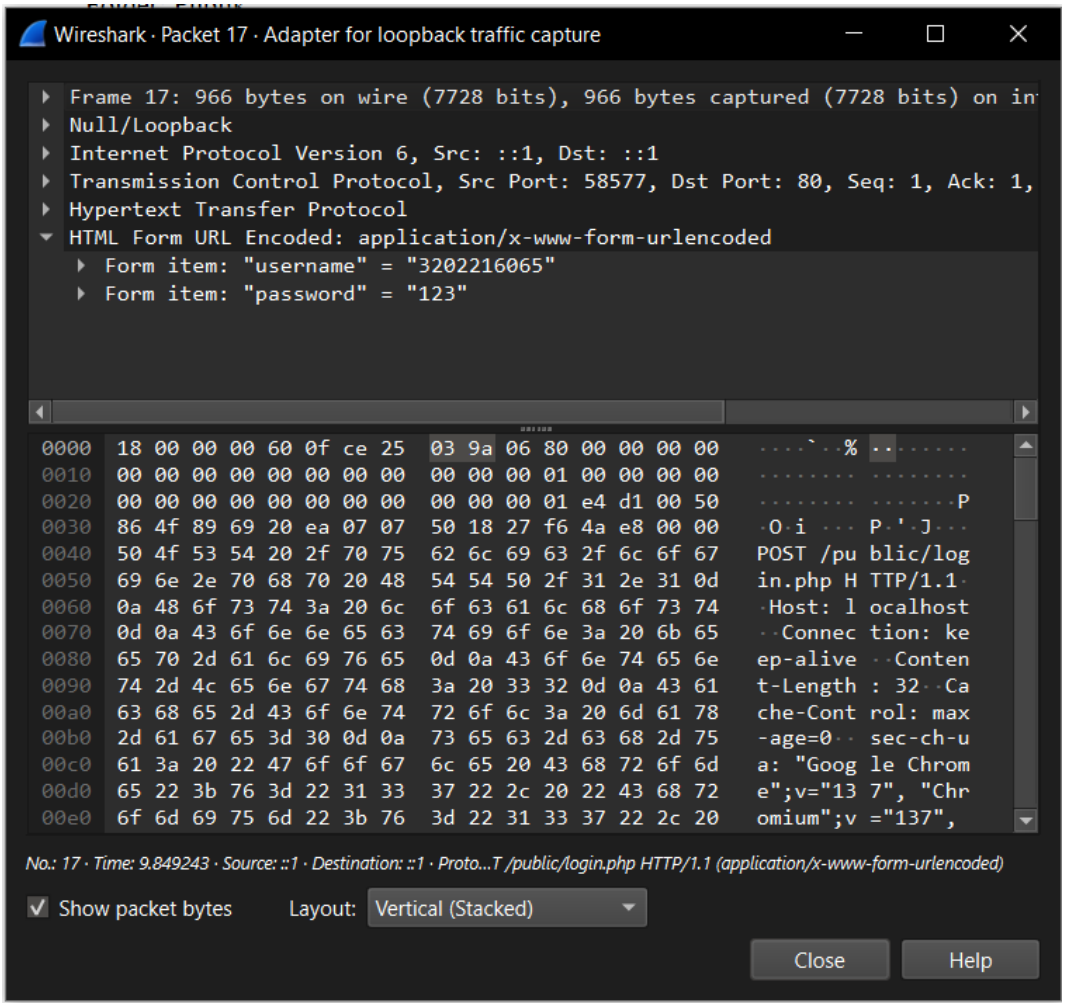
Password:
•••

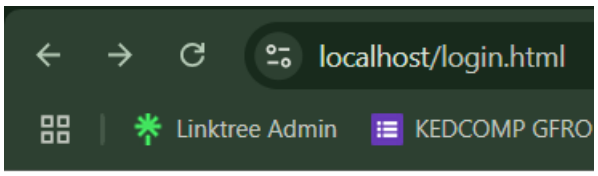
Login



Login successful!
Username: 3202216065
Password: 123





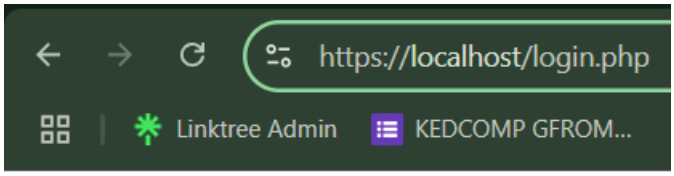


Login Page Private

Username:
pcnqwyt

Password:
•••••••••

Login



Login successful!
Username: pcnqwyt
Password: 123456789