



架設https伺服器之 申請免費SSL憑證

國立臺中教育大學 數位內容科技學系

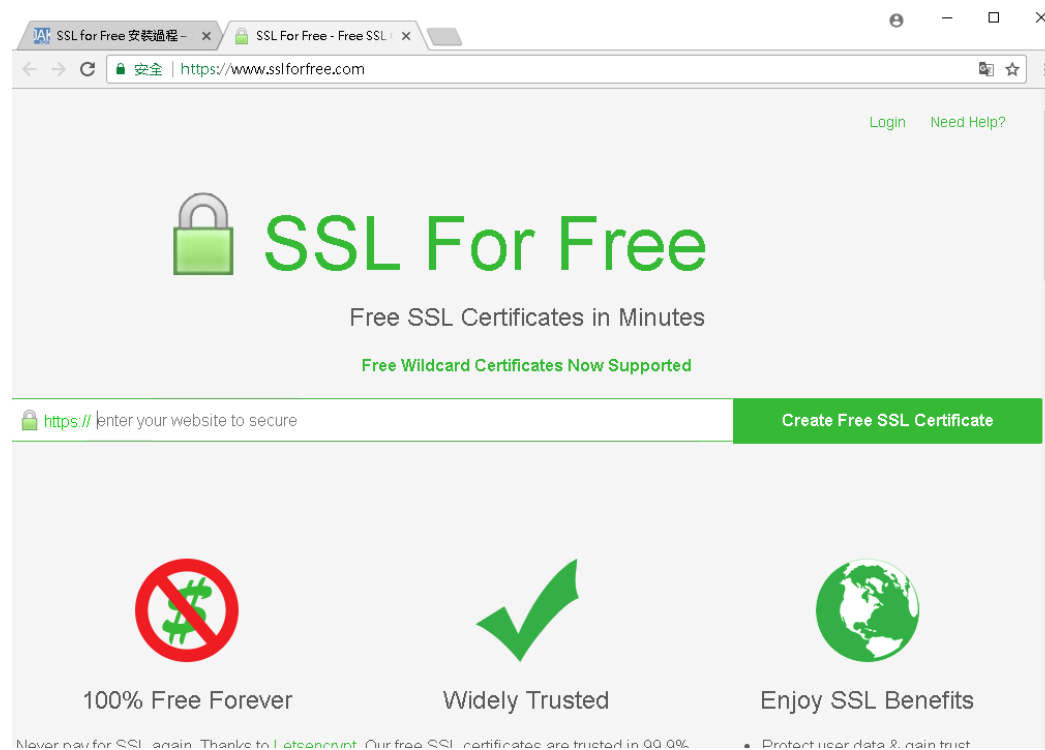
吳智鴻 教授

EMAIL:CHWU@MAIL.NTCU.EDU.TW

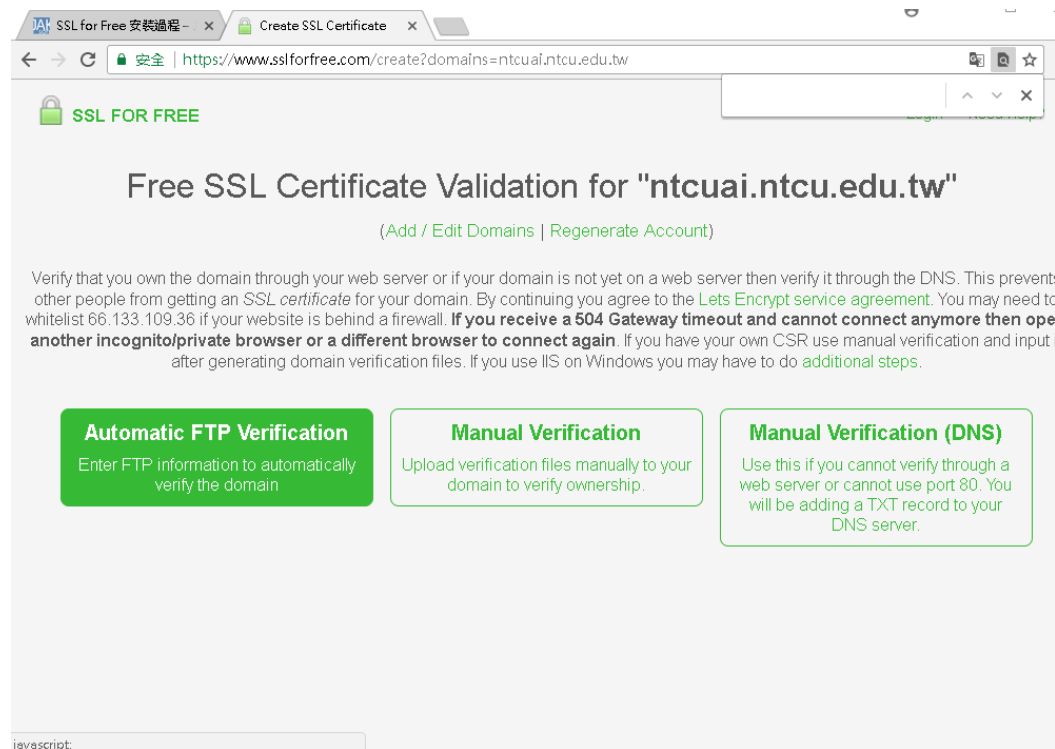
步驟

1. 連到 [SSL For Free](#) 官方網站
2. 輸入網域名稱後，按 Create Free SSL Certificate
3. 選中間的 Manual Verification，下方會出現 Manually Verify Domain 點一下
4. 出現 Download File 檔案 (Windows IIS Server 出現一個，Linux Apache Server 會出現兩個)，全部下載
5. 在網頁目錄建立資料夾 .well-known/acme-challenge，把剛剛抓到的檔案放進去
 - windows 建立 .well-known 要用 DOS 指令 `mkdir .well-known` 建立
 - 於IIS的要建立的網站設定內，點選 MIME 類型，右上角新增，副檔名填入.，MIME類型填入text/plain
6. 回到網頁剛才第五點 Verify successful upload by visiting the following links in your browser 下方會有個連結網址，這是讓我們確認剛才放的檔案是否可以正常讀取，點一下測試，若出現文字就代表正常
7. 正常以後點下方 Download SSL Certificate
8. 可以看到有提示寫到免費憑證為 90 天，下方有 E-mail 提醒機制，填好資料按 Create Account 以後就會自動提醒
9. 往下拉看到 Download All Certificate File 來下載全部的憑證檔案
10. 解開可看到三個檔案 ca_bundle.crt, certificate.crt, private.key
11. 再來需要把 private.key 轉成 pfx 格式，我們的 IIS Server 才能接受，下載 [64bit OpenSSL 轉檔工具](#)，[32bit OpenSSL 轉檔工具](#)
 - 依照作業系統下載轉檔工具 ([轉檔工具官方網站](#))
12. 再來把剛才解壓縮的 sslforfree 資料夾放到 d:\Downloads，於 cmd 模式切換到剛才安裝 OpenSSL 工具的目錄
 1. cd C:\OpenSSL-Win64\bin (我安裝 64bit，所以這邊是 Win64)
 2. openssl pkcs12 -export -out D:\Downloads\sslforfree\certificate.pfx -inkey D:\Downloads\sslforfree\private.key -in D:\Downloads\sslforfree\certificate.crt -certfile D:\Downloads\sslforfree\ca_bundle.crt
 3. 打完上述指令，接著會要輸入此金鑰的開啟密碼，待會會用到，要記好!
13. 完成後會產生新的檔案 certificate.pfx，把這檔案 copy 到 IIS server
14. 於IIS全域的設定區域點選 伺服器憑證
15. 點右上的 匯入，上面選擇剛才 .pfx 的檔案，下面則輸入剛才的密碼
16. 點選區域網站的設定區塊，右上的聯繫
17. 點新增，左上類型選擇 https，下方 SSL 憑證選擇剛才匯入的憑證

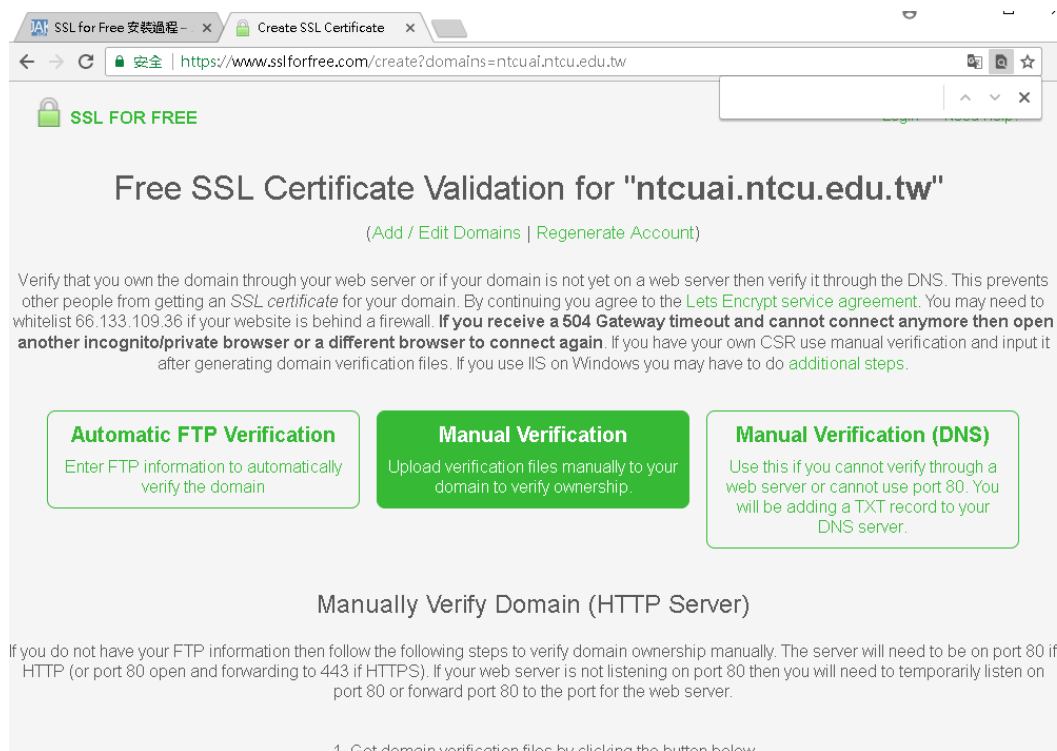
www.sslforfree.com 申請免費網域



選擇Manual Verification手動認證



選中間的手動認證



The screenshot shows a web browser window with the URL <https://www.sslforfree.com/create?domains=ntcuai.ntcu.edu.tw>. The page title is "Free SSL Certificate Validation for 'ntcuai.ntcu.edu.tw'". Below the title, there are three main verification options presented in green-bordered boxes:

- Automatic FTP Verification**: Enter FTP information to automatically verify the domain.
- Manual Verification**: Upload verification files manually to your domain to verify ownership.
- Manual Verification (DNS)**: Use this if you cannot verify through a web server or cannot use port 80. You will be adding a TXT record to your DNS server.

Below these options, the page is titled "Manually Verify Domain (HTTP Server)". The text explains that if the user does not have FTP information, they should follow the following steps to verify domain ownership manually. The server will need to be on port 80 if HTTP (or port 80 open and forwarding to 443 if HTTPS). If the web server is not listening on port 80, the user will need to temporarily listen on port 80 or forward port 80 to the port for the web server.

1. Get domain verification files by clicking the button below.

下載所需要的txt檔

SSL for Free 安裝過程 - x Create SSL Certificate x

安全 | <https://www.sslforfree.com/create?domains=ntcuai.ntcu.edu.tw>

3. Download your **free ssl certificate**

[Retry Manual Verification](#)

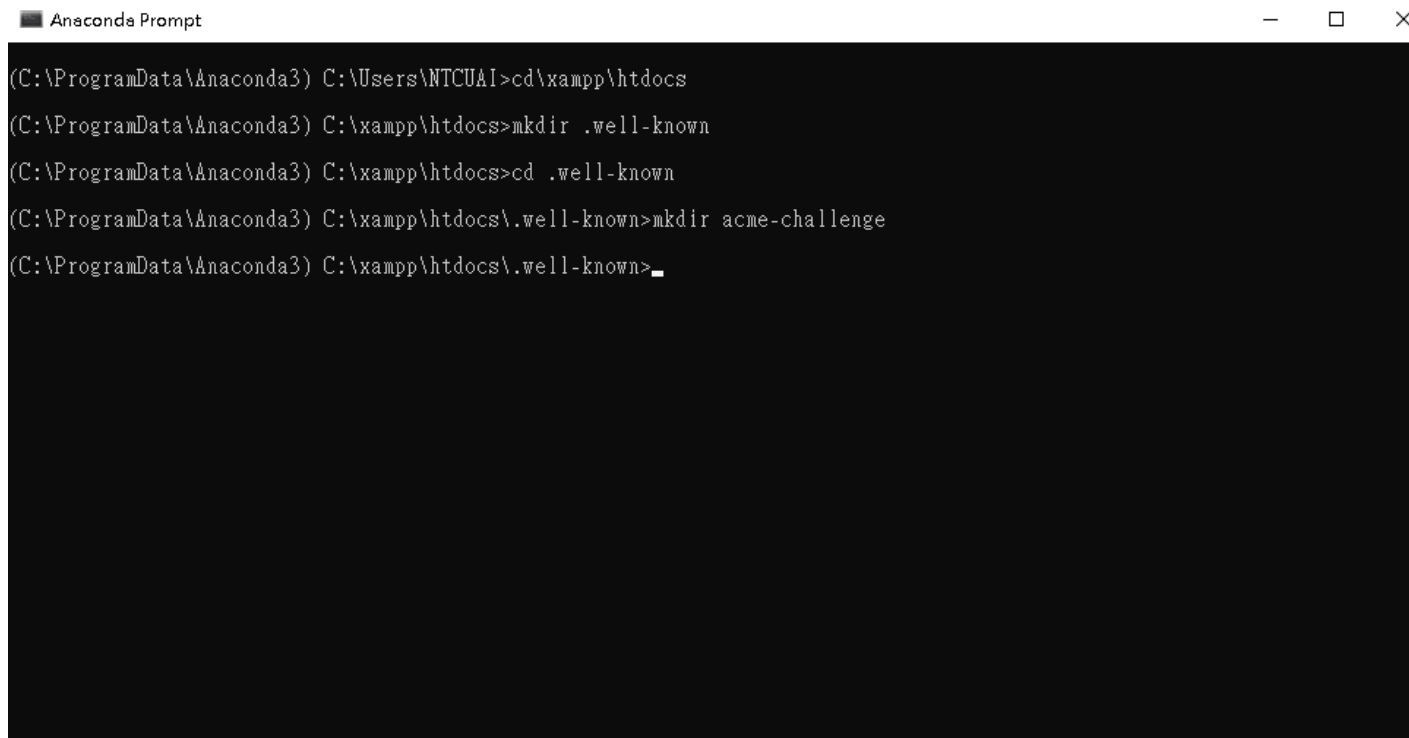
Upload Verification Files

- Download the following verification files by clicking on each link below
 - [Download File #1](#)
- Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
- Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
- Upload the downloaded files to the "acme-challenge" folder
- Verify successful upload by visiting the following links in your browser
 - <http://ntcuai.ntcu.edu.tw/.well-known/acme-challenge/VoMIKlgtUuRoieG2toY1taSylNoQdfsTuSF7a9O5uw>
- If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up but the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or the wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
- Click Download SSL Certificate below.

[Download SSL Certificate](#)

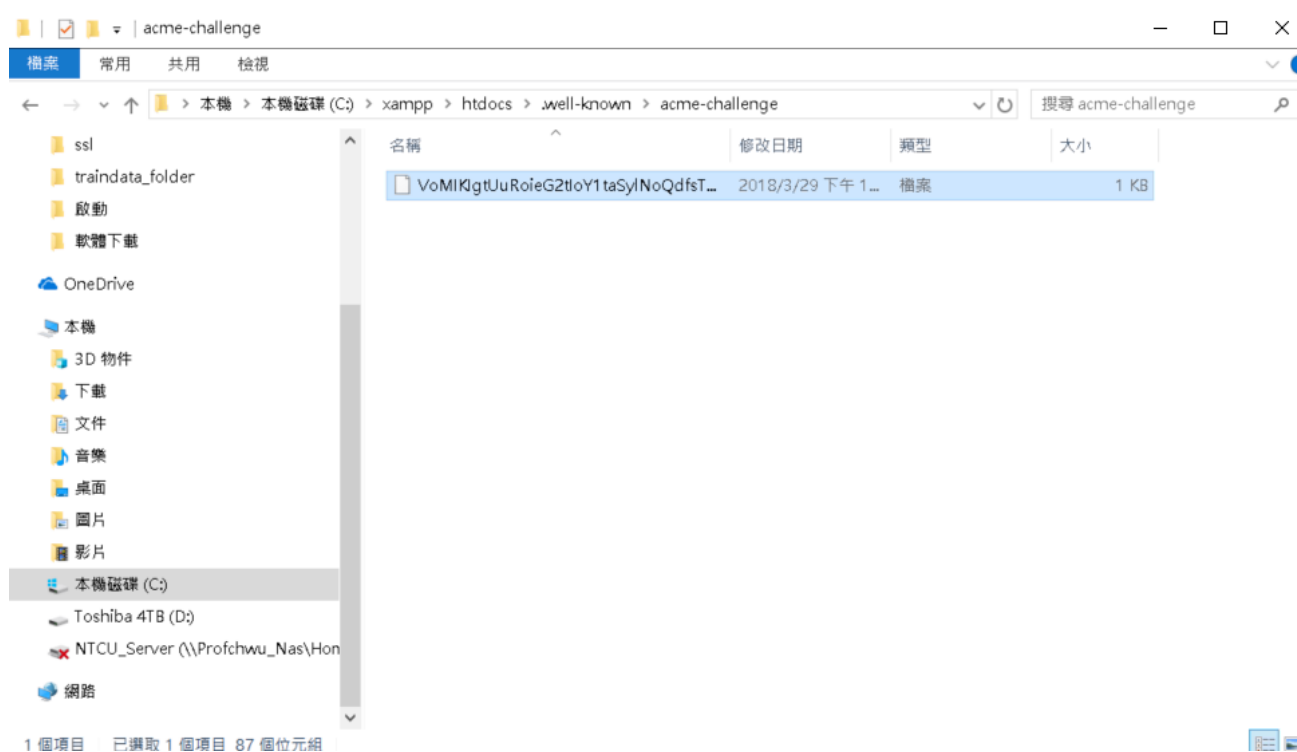
I Have My Own CSR

在WINDOS下 用CMD建立目錄 .well-known/acme-challenge

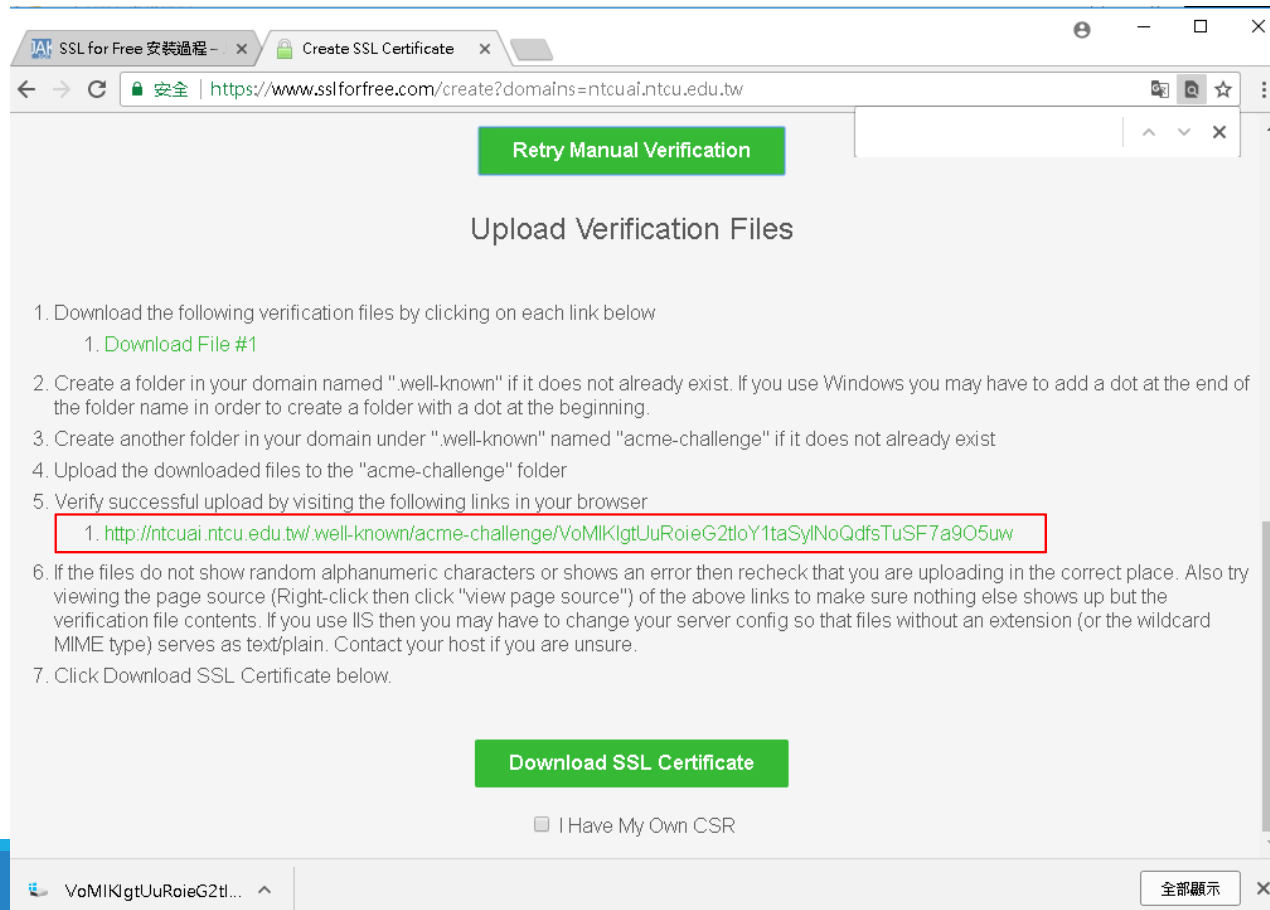


```
Anaconda Prompt
(C:\ProgramData\Anaconda3) C:\Users\WTCUAI>cd \xampp\htdocs
(C:\ProgramData\Anaconda3) C:\xampp\htdocs>mkdir .well-known
(C:\ProgramData\Anaconda3) C:\xampp\htdocs>cd .well-known
(C:\ProgramData\Anaconda3) C:\xampp\htdocs\.well-known>mkdir acme-challenge
(C:\ProgramData\Anaconda3) C:\xampp\htdocs\.well-known>.
```

把之前步驟下載的檔案搬移到 那個目錄中



啟動xampp 然後點選下方的認證



SSL for Free 安裝過程 - x Create SSL Certificate x

安全 | <https://www.sslforfree.com/create?domains=ntcuai.ntcu.edu.tw>

[Retry Manual Verification](#)

Upload Verification Files

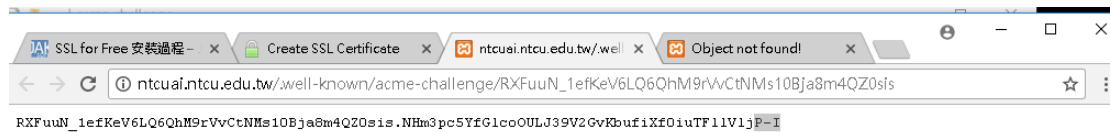
1. Download the following verification files by clicking on each link below
 1. [Download File #1](#)
2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder
5. Verify successful upload by visiting the following links in your browser
 1. <http://ntcuai.ntcu.edu.tw/.well-known/acme-challenge/VoMIKlgtUuRoieG2tloY1taSyINoQdfsTuSF7a9O5uw>
6. If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up but the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or the wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
7. Click Download SSL Certificate below.

[Download SSL Certificate](#)

I Have My Own CSR

VoMIKlgtUuRoieG2tl... ^ [全部顯示](#) x

成功的話會出現文字



認證成功後就可以下載憑證了

SSL for Free 安裝過程 - x Create SSL Certificate x ntcuai.ntcu.edu.tw/well x Object not found!

安全 | <https://www.sslforfree.com/create?domains=ntcuai.ntcu.edu.tw>

Retry Manual Verification

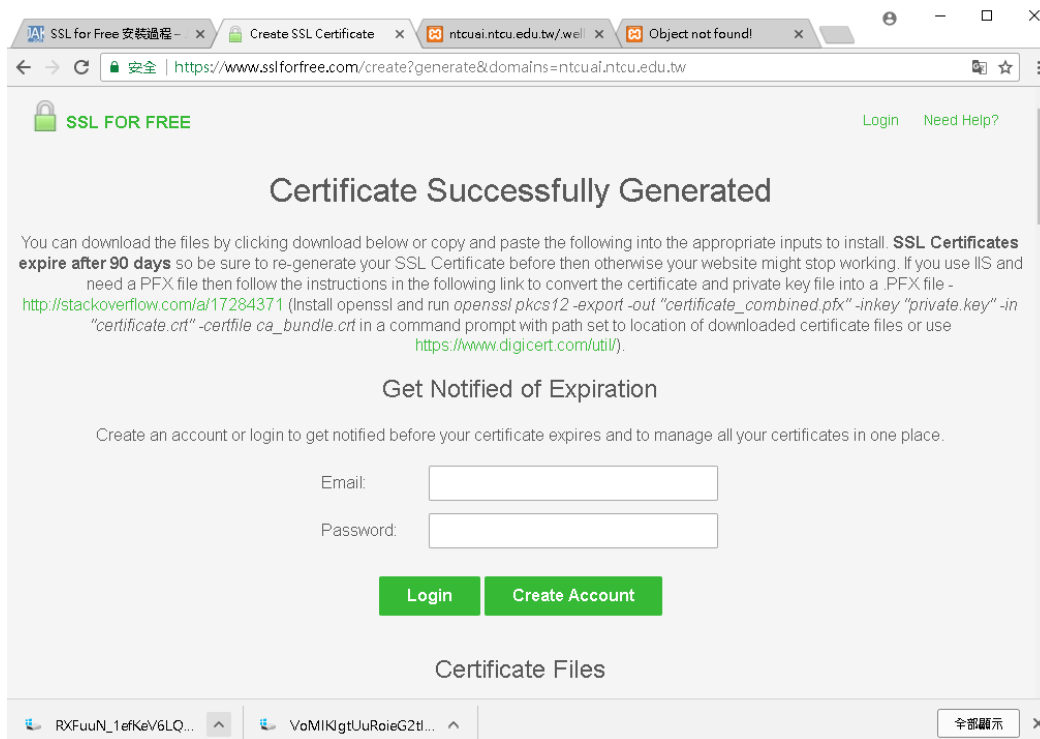
Upload Verification Files

1. Download the following verification files by clicking on each link below
 1. [Download File #1](#)
2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder
5. Verify successful upload by visiting the following links in your browser
 1. http://ntcuai.ntcu.edu.tw/.well-known/acme-challenge/RXFuuN_1efKeV6LQ6QhM9rVvCtNMs10Bja8m4QZ0sis
6. If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up but the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or the wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
7. Click Download SSL Certificate below.

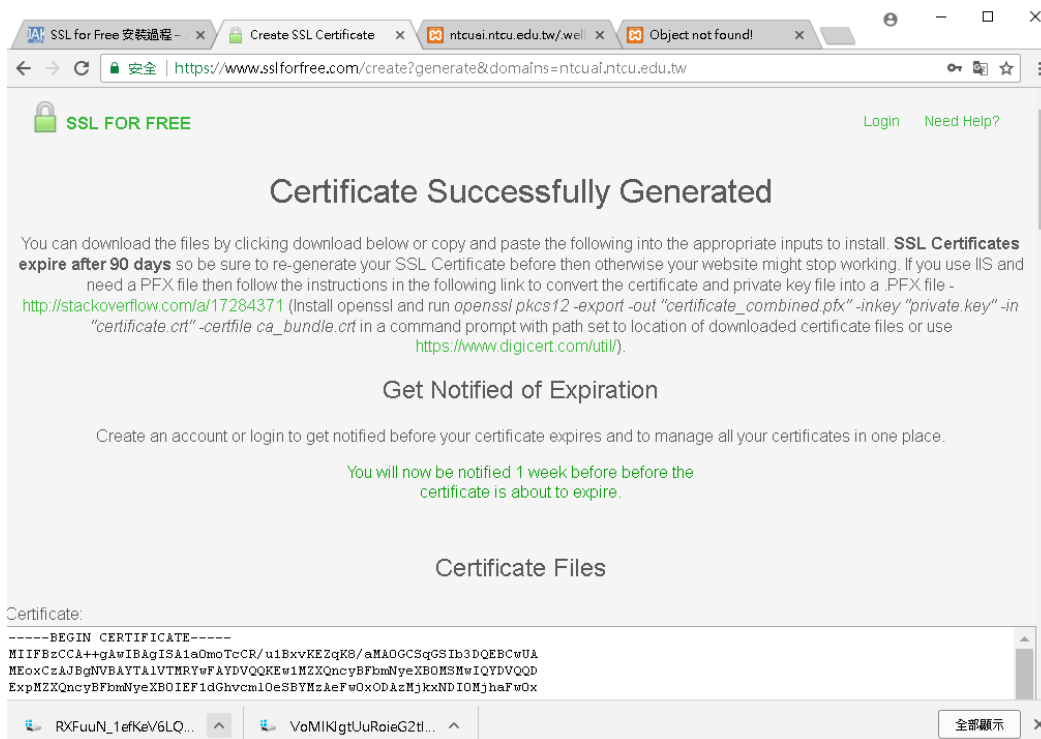
Download SSL Certificate

I Have My Own CSR

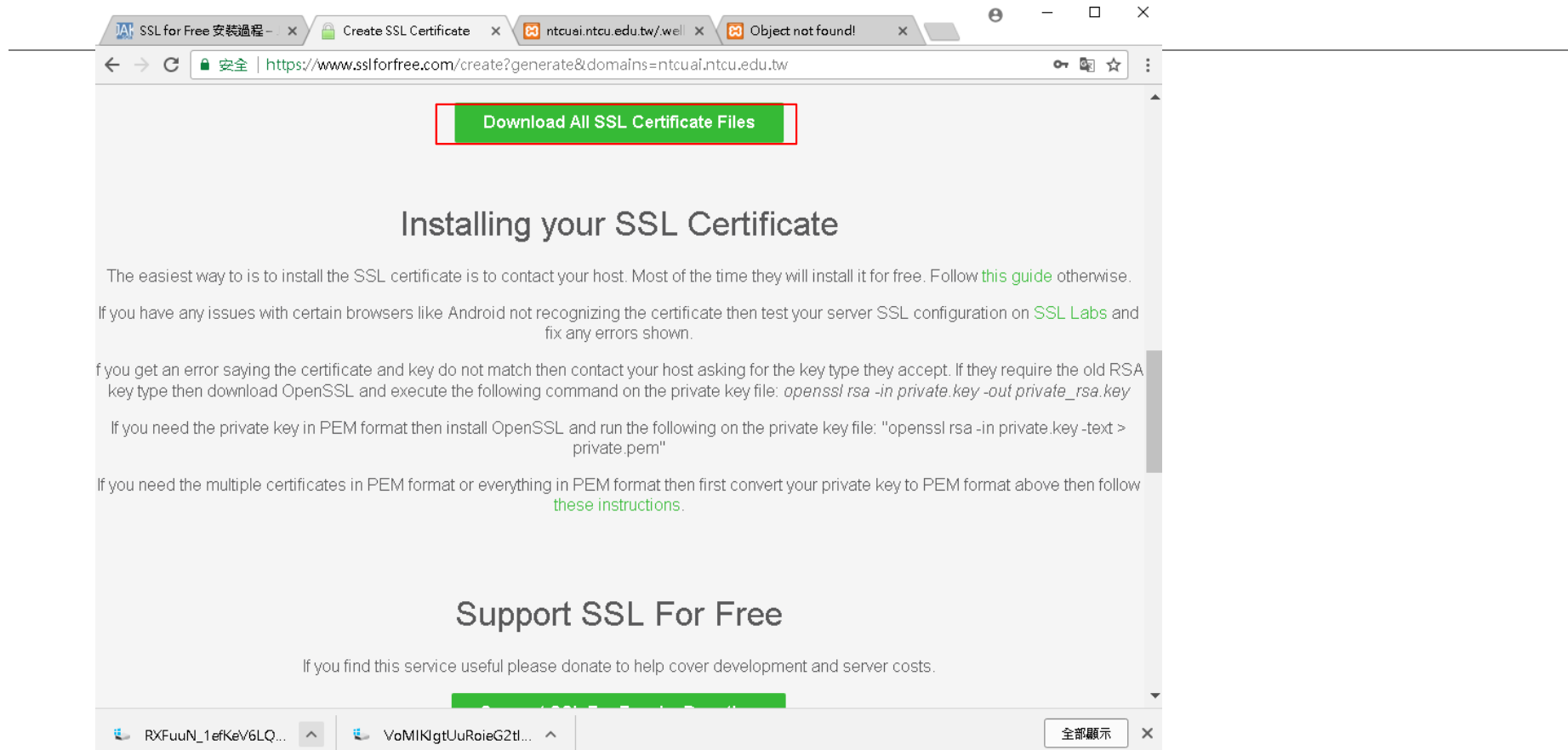
憑證成功建立了，建立一個通知帳號 (90天需要更新)



帳後建立後如下圖



點選 Download All SSL Certificate Files



下載成功後，解壓縮會有這三個檔案

名稱	類型	壓縮大小	受密碼保護	大小
 ca_bundle.crt	安全性憑證	2 KB	否	
 certificate.crt	安全性憑證	2 KB	否	
 private.key	KEY 檔案	2 KB	否	

需要修的地方

開啟 http-ssl.conf

```
# Listen 443 改為 Listen 443
```

```
# SSL Engine Switch:  
# Enable/Disable SSL for this virtual host.  
SSLEngine on
```

```
# Server Certificate:  
# Point SSLCertificateFile "conf/ssl.crt/server.crt"  
# the certificate is encrypted, then you will be prompted for a  
# pass phrase. Note that a kill -HUP will prompt again. Keep  
# in mind that if you have both an RSA and a DSA certificate you  
# can configure both in parallel (to also allow the use of DSA  
# ciphers, etc.)  
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)  
# require an ECC certificate which can also be configured in  
# parallel.
```

```
SSLCertificateFile "conf/ssl.crt/server.crt"  
#SSLCertificateFile "conf/ssl.crt/server.crt"  
#SSLCertificateFile "conf/ssl.crt/server.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 "conf/ssl.key/server.key"  
#SSLCertificateKeyFile "conf/ssl.key/server.key"  
#SSLCertificateKeyFile "conf/ssl.key/server.key"
```

```
.....
```

certificate.crt 更名為 server.crt 後存放到如上圖的server.crt位置

private.key 更名為 server.key 後存放到如上圖的server.key位置

ca_bundle.crt 不管它

開啟 httpd.conf

加入網站

```
1 | ServerName yourname.com
2 | DocumentRoot "E:/xampp/htdocs/web/yourname.com"
3 | SSLEngine on
4 | SSLCertificateFile "E:/xampp/apache/conf/ssl.crt/server.crt"
5 | SSLCertificateKeyFile "E:/xampp/apache/conf/ssl.key/server.key"
```

重啟Apache，完成^^

查看你目前申請了那些SSI及到期日期：<https://www.sslforfree.com/certificates>

查看你目前申請了那些SSL及到期日期 <https://www.sslforfree.com/certificates>



如果是IIS，還需要下載OPENSSL程式 或者需要certificate.pfx檔案時

<http://slproweb.com/products/Win32OpenSSL.html>

Download Win32 OpenSSL

Download Win32 OpenSSL today using the links below!

File	Type	Description
Win32 OpenSSL v1.1.0h Light	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.0h (Recommended for users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.0h	30MB Installer	Installs Win32 OpenSSL v1.1.0h (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0h Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0h (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0h	33MB Installer	Installs Win64 OpenSSL v1.1.0h (Only install this if you are a software developer needing 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.0.2o Light	2MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.0.2o (Recommended for users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.0.2o	20MB Installer	Installs Win32 OpenSSL v1.0.2o (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.0.2o Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.0.2o (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.0.2o	23MB Installer	Installs Win64 OpenSSL v1.0.2o (Only install this if you are a software developer needing 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

產生certificate.pfx

再來把剛才解壓縮的 sslforfree 資料夾放到 d:\Download , 於 cmd 模式切換到剛才安裝 OpenSSL 工具的目錄

下以下指令

- `cd C:\OpenSSL-Win64\bin` (安裝 64bit , 所以是 Win64 或者你是32bit , 要換成Win32)
- `openssl pkcs12 -export -out D:\Downloads\sslforfree\certificate.pfx -inkey D:\Downloads\sslforfree\private.key -in D:\Downloads\sslforfree\certificate.crt -certfile D:\Downloads\sslforfree\ca_bundle.crt`

打完上述指令 , 接著會要輸入此金鑰的開啟密碼 , 待會會用到 , 要記好!

完成後會產生新的檔案 certificate.pfx

```
(C:\ProgramData\Anaconda3) c:\OpenSSL-Win64\bin>openssl pkcs12 -export -out d:\download\certificate.pfx -inkey d:\download\private.key -in d:\download\certificate.crt -certfile d:\download\ca_bundle.crt
Enter Export Password:
Verifying - Enter Export Password:
(C:\ProgramData\Anaconda3) c:\OpenSSL-Win64\bin>
```

最後完成的檔案

指令

```
(C:\ProgramData\Anaconda3) c:\OpenSSL-Win64\bin>openssl pkcs12 -export -out d:\download\certificate.pfx -inkey d:\download\private.key -in d:\download\certificate.crt -certfile d:\download\ca_bundle.crt
Enter Export Password:
Verifying - Enter Export Password:
(C:\ProgramData\Anaconda3) c:\OpenSSL-Win64\bin>
```

產生的檔案

名稱	修改日期	類型	大小
ca_bundle.crt	2018/3/29 下午 1...	安全性憑證	2 KB
certificate.crt	2018/3/29 下午 1...	安全性憑證	2 KB
certificate.pfx	2018/3/31 下午 0...	個人資訊交換	5 KB
private.key	2018/3/29 下午 1...	KEY 檔案	2 KB

如果需要PEM檔案

```
openssl rsa -in private.key -text > private.pem
```

即可以產生PEM檔案

參考來源

1. <https://jakson.online/2017/08/03/ssl-for-free-%E5%AE%89%E8%A3%9D%E9%81%8E%E7%A8%8B/>
2. <https://blog.hahasmile.com/xampp-free-lets-encrypt-ssl/>
3. <https://blog.hahasmile.com/%E5%9C%A8apache%E4%B8%8A%E8%A8%AD%E5%AE%9A%E5%AE%89%E8%A3%9Dssl%E6%86%91%E8%AD%89/>