HTTPS服務導入

國立中山大學圖書與資訊處

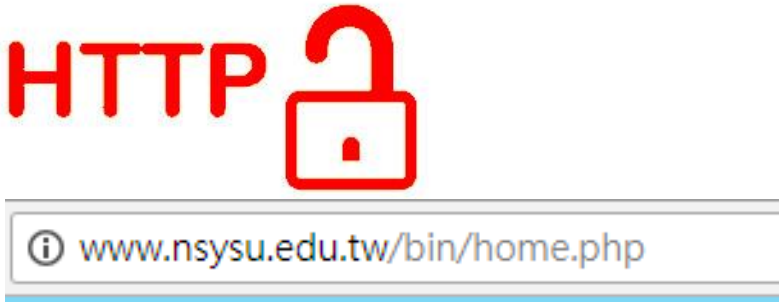
資安組王聖全

教育部公文來函導入範圍說明

- 行政院所屬二、三級機關於106年12月底前完成官網使用HTTPS傳輸協定
- 行政院各級機關對外服務網站於107年6月底前完成導入HTTPS傳輸協定
- 網站強制導入(輸入http://...自動轉址至https://...)

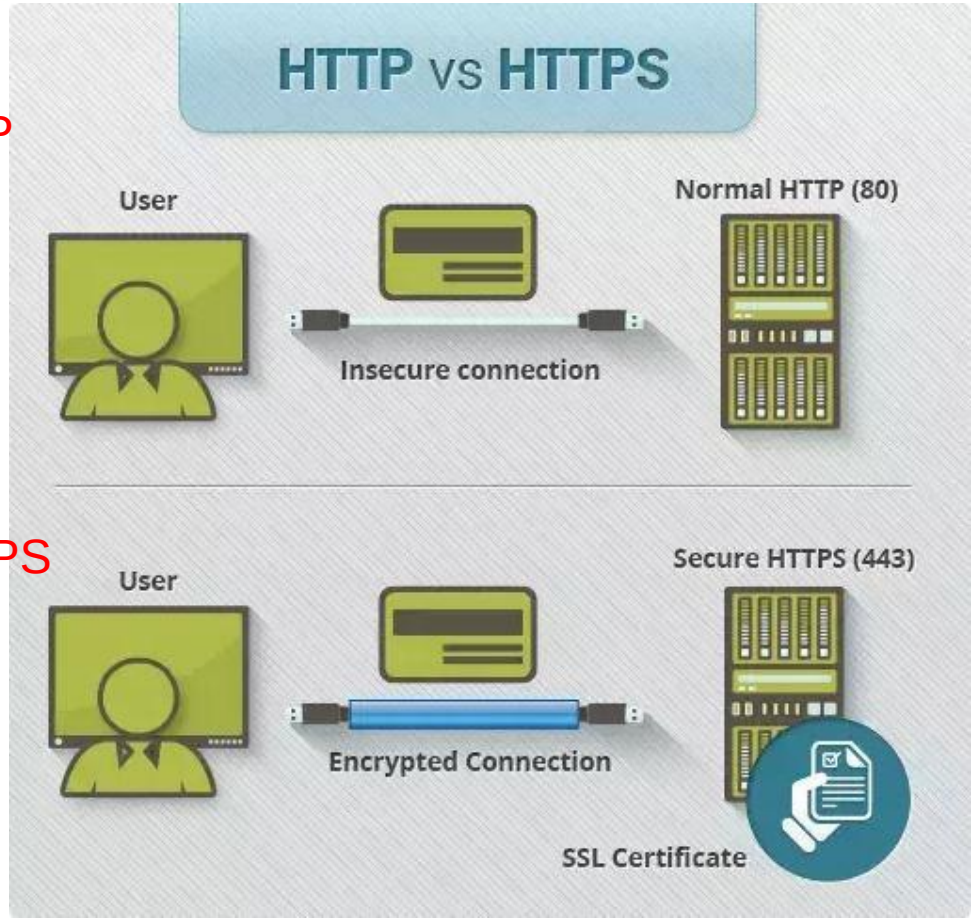
HTTPS

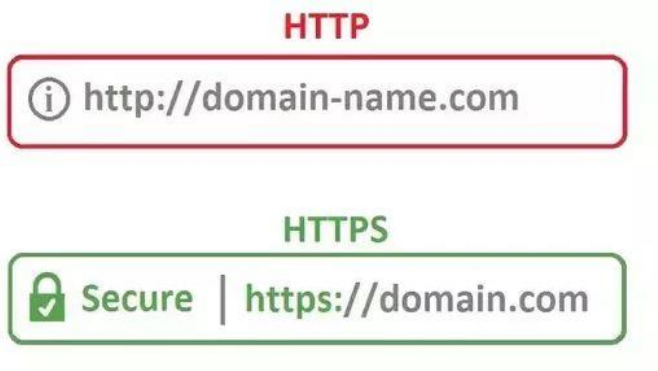
- HTTP:一個用戶端終端(用戶)和伺服器端(網站)請求和應答的標準
  - http://www.nsysu.edu.tw
- HTTPS
  - 加過密的 HTTP，用SSL/TLS來加密封包
  - 在不安全的網路上建立一安全信道，並可在使用適當的加密套件和伺服器憑證可被驗證且可被信任時，對竊聽和中間人攻擊提供合理的防護。



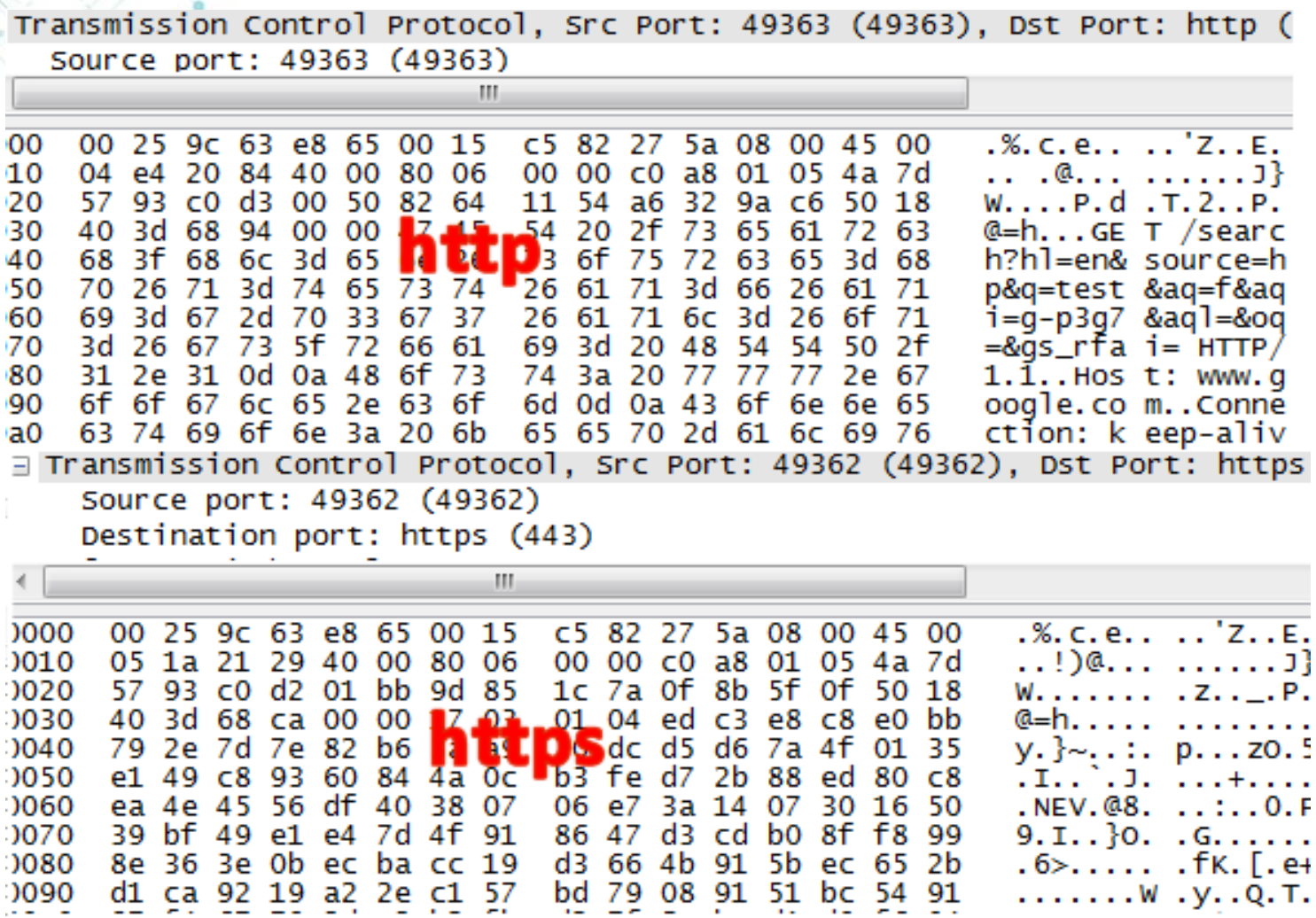
HTTP v.s. HTTPS

HTTP

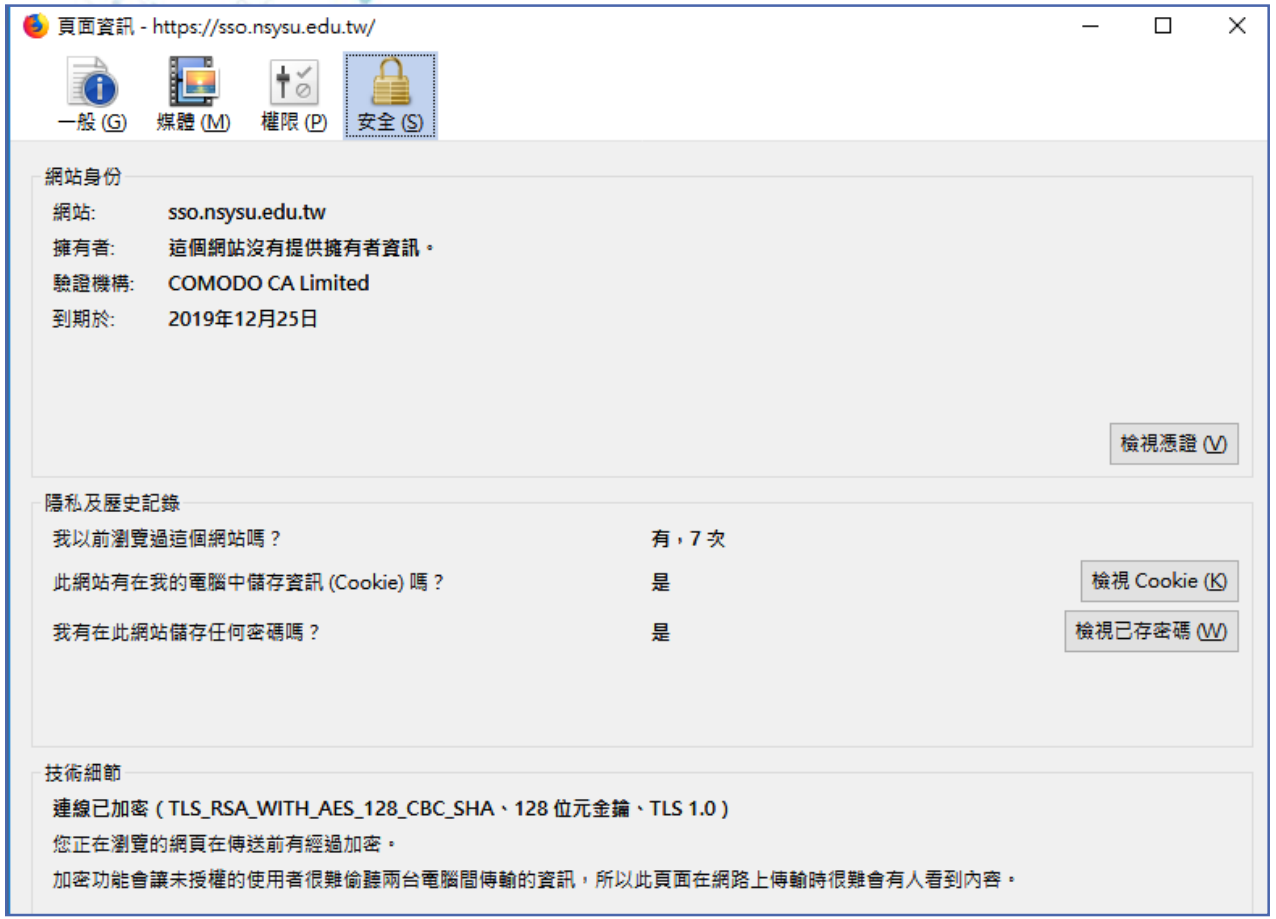


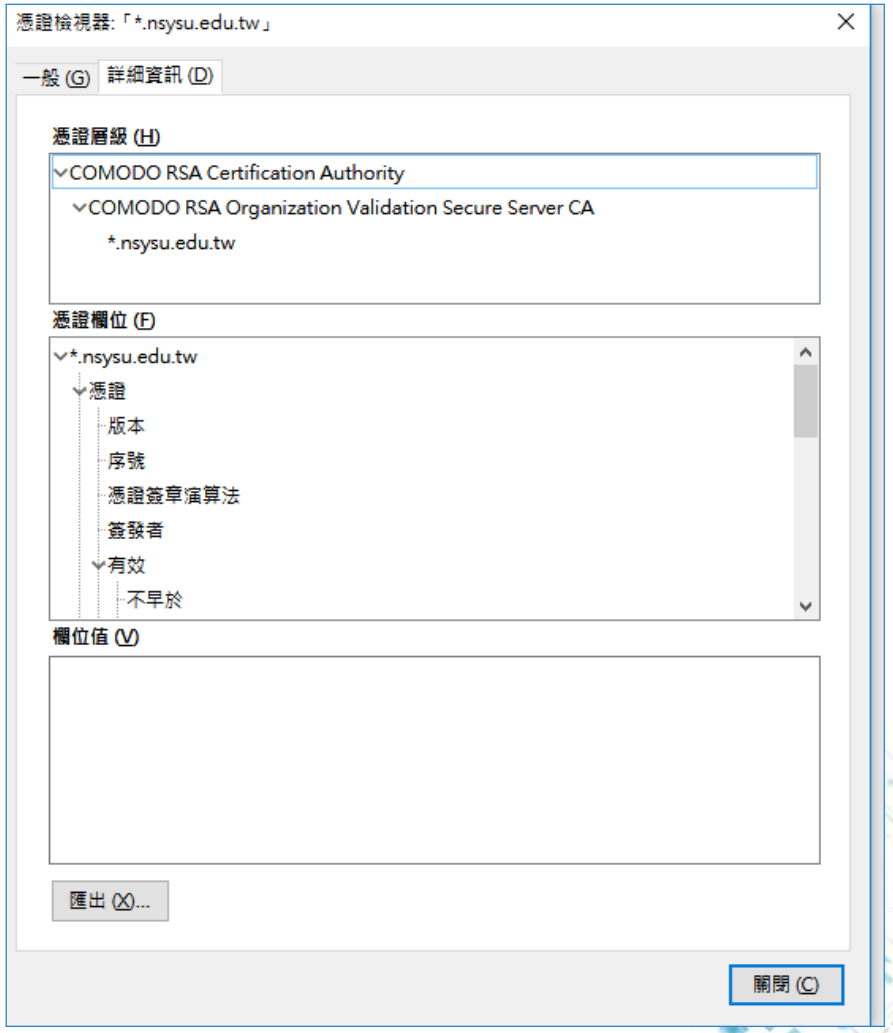


HTTP v.s. HTTPS (cont.)



SSL憑證


頁面資訊 - https://sso.nsysu.edu.tw/
一般 (G)
媒體 (M)
權限 (P)
安全 (S)
網站身份
網站: sso.nsysu.edu.tw
擁有者: 這個網站沒有提供擁有者資訊。
驗證機構: COMODO CA Limited
到期於: 2019年12月25日
檢視憑證 (V)
隱私及歷史記錄
我以前瀏覽過這個網站嗎？ 有，7 次
此網站有在我的電腦中儲存資訊 (Cookie) 嗎？ 是
檢視 Cookie (K)
我有在此網站儲存任何密碼嗎？ 是
檢視已存密碼 (W)
技術細節
連線已加密 (TLS_RSA_WITH_AES_128_CBC_SHA、128 位元金鑰、TLS 1.0)
您正在瀏覽的網頁在傳送前有經過加密。
加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊，所以此頁面在網路上傳輸時很難會有人看到內容。


憑證檢視器:「*.nsysu.edu.tw」
一般 (G)
詳細資訊 (D)
憑證層級 (H)
COMODO RSA Certification Authority
COMODO RSA Organization Validation Secure Server CA
*.nsysu.edu.tw
憑證欄位 (F)
*.nsysu.edu.tw
憑證
版本
序號
憑證簽章演算法
簽發者
有效
不早於
欄位值 (V)
匯出 (X)...
關閉 (C)

免費 V.S. 付費

	免費憑證	付費憑證
優點	• 快速、免費 • 自動驗證(Domain Validation Only)	• 使用期限長(1~2年) • 安全性較高 • CA會support
缺點	• 使用期限短(30~90天) • 安全性相對較低 • No Support	• 申請時間較長 • 付費(子網域憑證需分開購置)

目前本處已購置之憑證

- 一層
  - *.nsysu.edu.tw
- 二層
  - *.lib.nsysu.edu.tw
  - *.lis.nsysu.edu.tw
  - *.cloud.nsysu.edu.tw
  - *.ezproxy.lis.nsysu.edu.tw

Linux 平台憑證導入

- 啟動Apache SSL module
  - a2enmod ssl
- 複製Apache設定檔
  - cp /etc/apache2/site-available/default-ssl.conf /etc/apache2/site-enable/ ssl.conf
- 修改ssl.conf設定檔，更改憑證路徑
  - SSLCertificateFile /存放路徑/nsysu2014.cer
  - SSLCertificateKeyFile /存放路徑/nsysu2014.key
  - SSLCertificateChainFile /存放路徑/bundle-sha2.cer

Linux 平台憑證導入 (cont.)

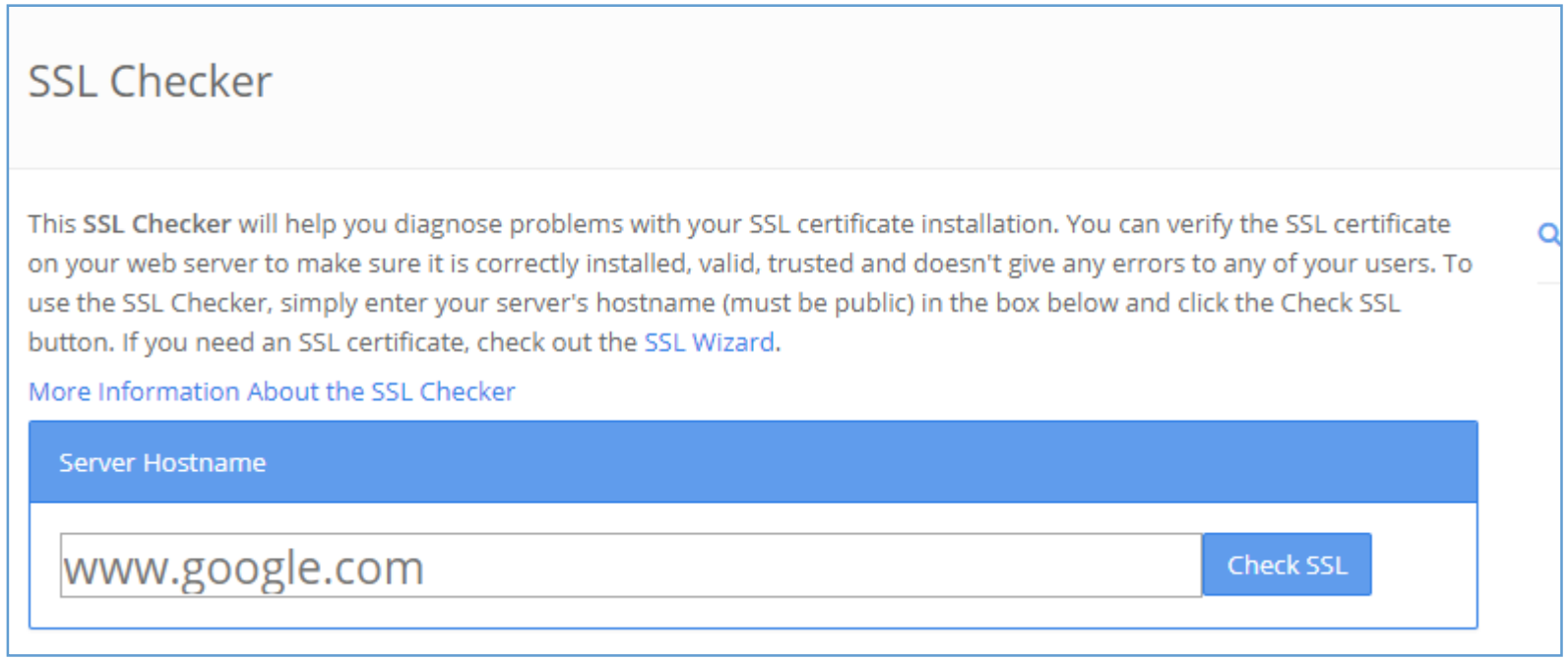
```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin [redacted]
                ServerName [redacted]
                DocumentRoot /var/www/html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
        #       SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
        #       SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
                SSLCertificateFile /etc/apache2/ssl/nsysu2014.cer
                SSLCertificateKeyFile /etc/apache2/ssl/nsysu2014.key
                SSLCertificateChainFile /etc/apache2/ssl/bundle-sha2.cer
                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
                <Directory /var/www/>
                Options FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
                SSLOptions +StdEnvVars
                </Directory>
        </VirtualHost>
</IfModule>
```

Linux 平台憑證導入 (cont.)

- 設定檔修改完成後，重新啟動Apache Server
  - sudo systemctl restart apache2.service

憑證檢查

- SSL Checker
  - https://www.sslshopper.com/ssl-checker.html
  - 確認安裝過程有無問題



憑證檢查(cont.)

- SSL lab
  - https://www.ssllabs.com/ssltest/
  - 確認憑證安全性等級