HTTPS Security

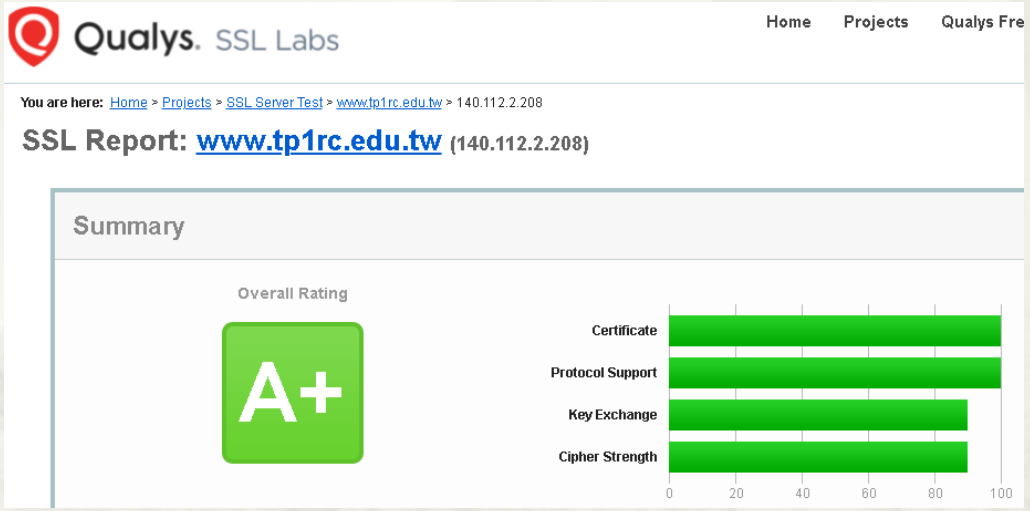
臺灣大學計資中心
網路組
游子興

大綱

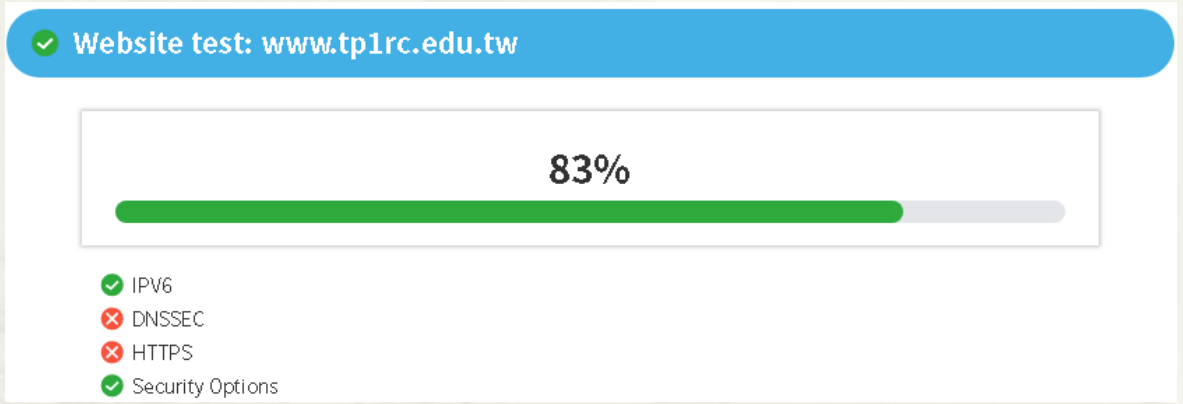
* Apache
* IIS

SSL Server Test

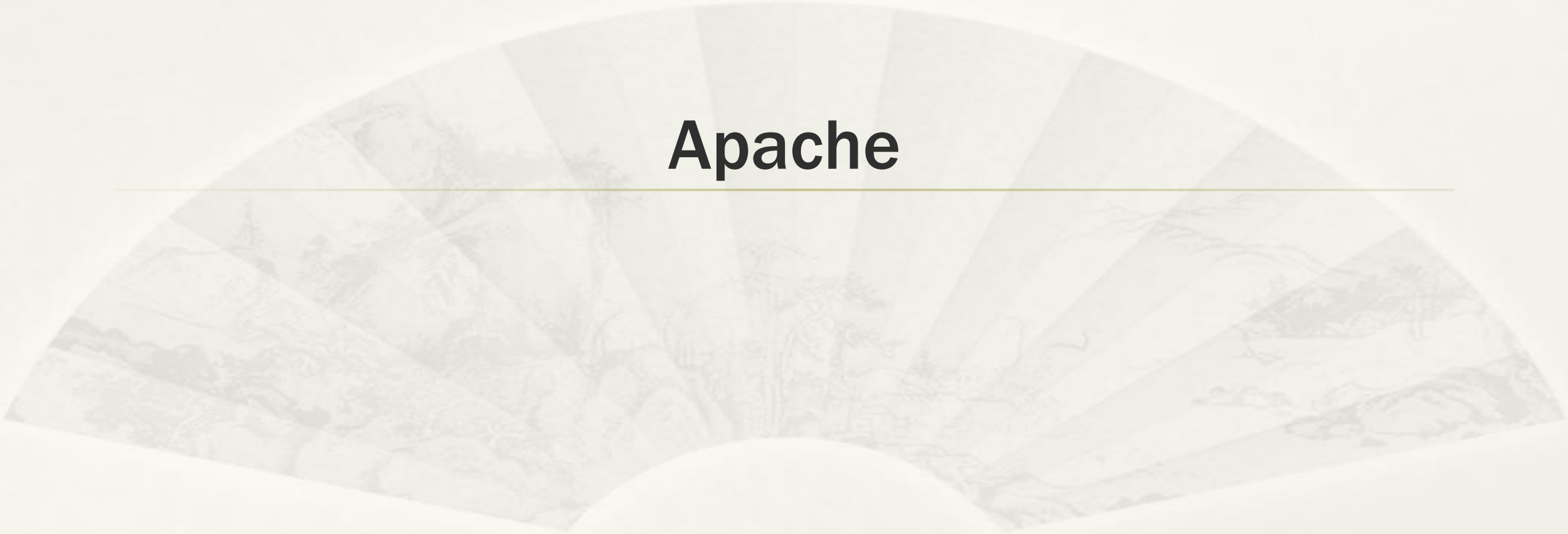
* https://www.ssllabs.com/



* https://check.twnic.tw/



Apache



SSL Server Test
disable SSLv3

- SSLProtocol all -SSLv2 -SSLv3 -TLSv1.0 -TLSv1.1
- SSLCipherSuite ALL:+HIGH:!ADH:!EXP:!SSLv2:!SSLv3:!MEDIUM:!LOW:!NULL:!aNULL
- SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH:+HIGH:!ADH:!EXP:!SSLv2:!SSLv3:!MEDIUM:!LOW:!NULL:!aNULL

```
#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by default:
SSLProtocol all -SSLv2 -SSLv3

#   SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
```

CIPHER LIST FORMAT

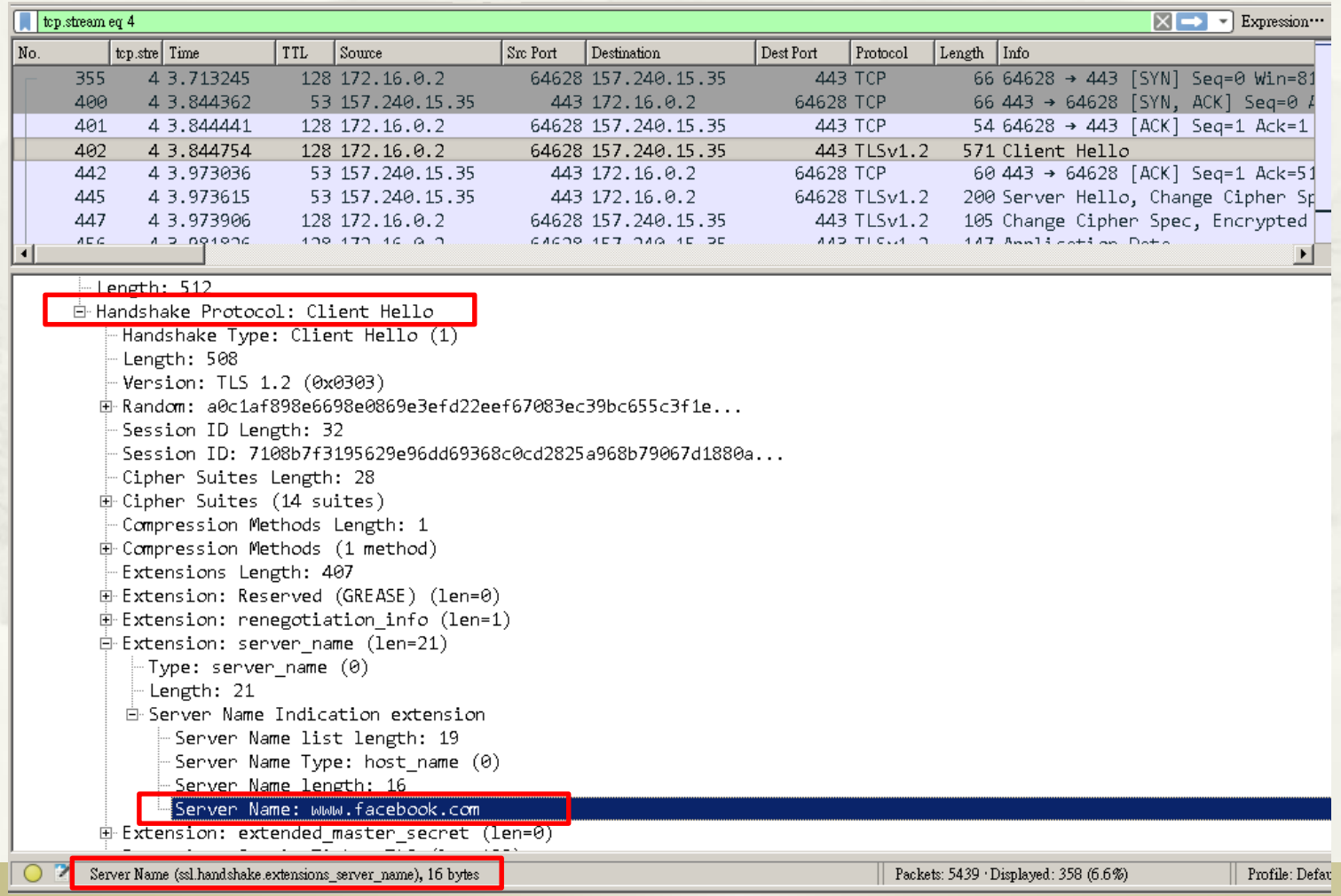
- + Add
  - Adds the following option to the existing protocol list.
- - Delete
  - Delete the following option. This option can be added again if it is found at a subsequent point.
- ! Exclude
  - Permanently excludes the following option and ignores any subsequent attempt to add an option.

CIPHER STRINGS

- ALL
  - All cipher suites except the eNULL ciphers.
- HIGH
  - with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.
- MEDIUM
  - some of those using 128 bit encryption.
- LOW
  - those using 64 or 56 bit encryption algorithms but excluding export cipher suites. All these cipher suites have been removed as of OpenSSL 1.1.0.
- eNULL NULL
  - Offering no encryption.
- aNULL
  - Offering no authentication

https in Wireshark

* ssl.handshake.extensions_server_name



Header 相關設定

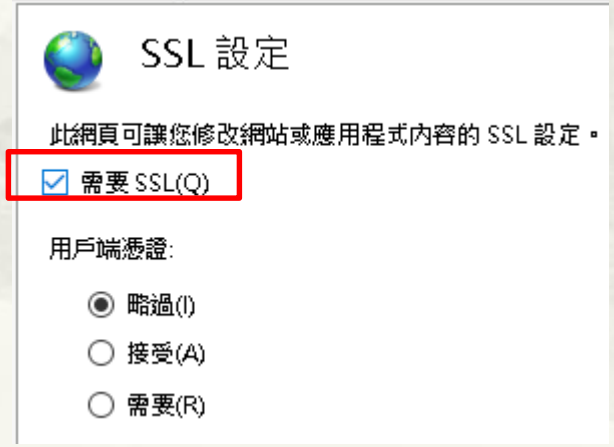
- Ubuntu
  - Install apache headers module
    - sudo a2enmod headers
  - header 設定檔案
    - /etc/apache2/conf-available/security.conf
- CentOS
  - 不需要

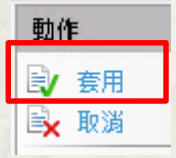
* Header always set Strict-Transport-Security "max-age=31536000; includeSubdomains; preload“

* Header always append X-Frame-Options SAMEORIGIN
* Header always append X-Content-Type-Options nosniff
* Header always append X-XSS-Protection 1
* Header always append Content-Security-Policy default-src=self
* Header always append Referrer-Policy strict-origin

IIS

HTTPS Redirect



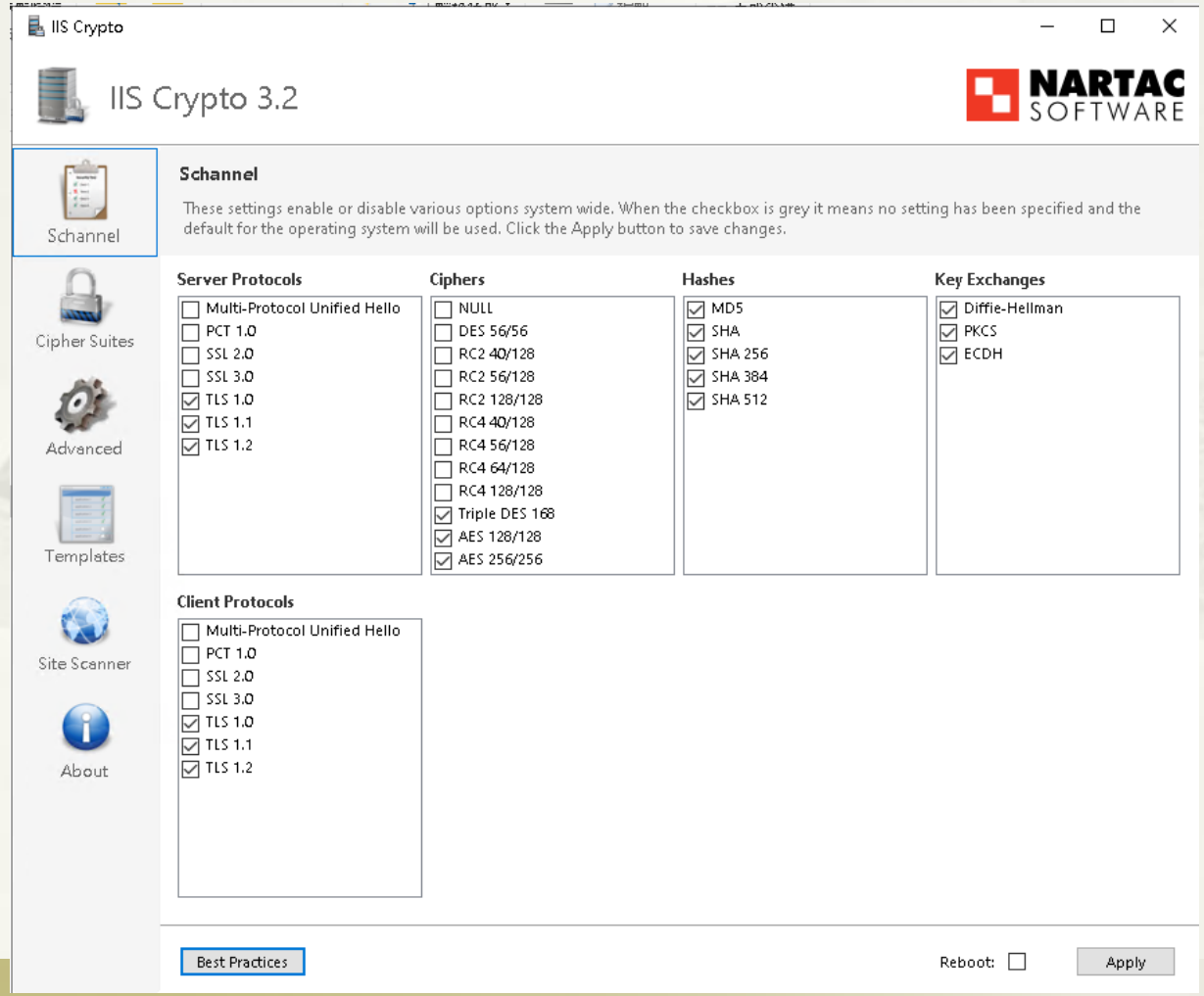


Weak SSL Cipher

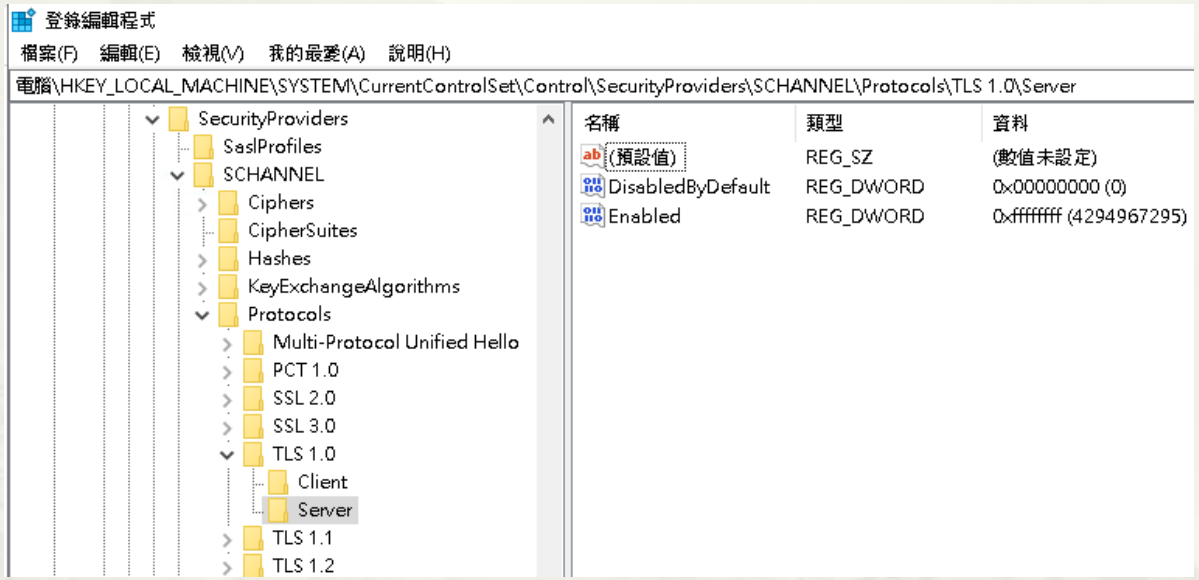
- 手動
  - Reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" /v "Enabled" /t REG_DWORD /d "0" /f
  - Reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v "Enabled" /t REG_DWORD /d "0" /f
  - Reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" /v "Enabled" /t REG_DWORD /d "0" /f
  - Reg.exe add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" /v "Enabled" /t REG_DWORD /d "0" /f

Weak SSL Cipher
IIS Crypto

* https://www.nartac.com/Products/IISCrypto/Download

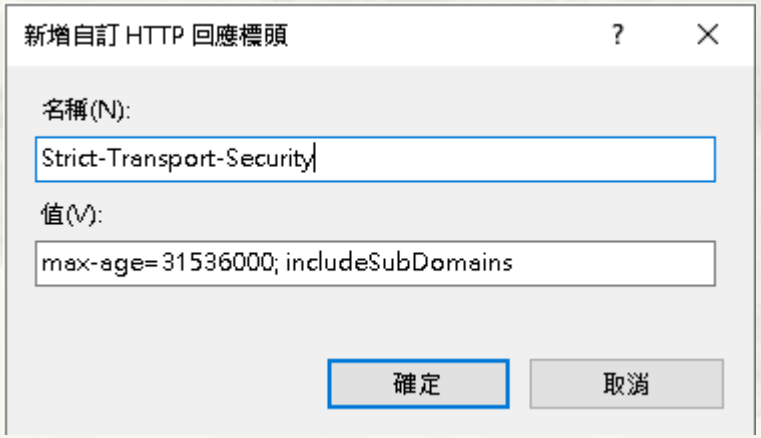


* regedit



Header 相關設定

HSTS

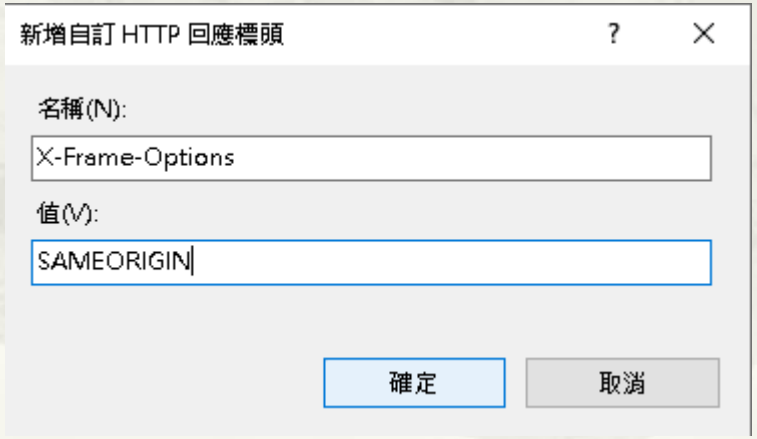


* 名稱: Strict-Transport-Security
* 值: max-age=31536000; includeSubDomains

HSTS
Windows Server 2019

* Click on HSTS. Check Enable and set the Max-Age to 31536000 (1 year). Check IncludeSubDomains and Redirect Http to Https

Other Setting



簡報完畢
謝謝