

HTTPS Security

臺灣大學計資中心
網路組
游子興

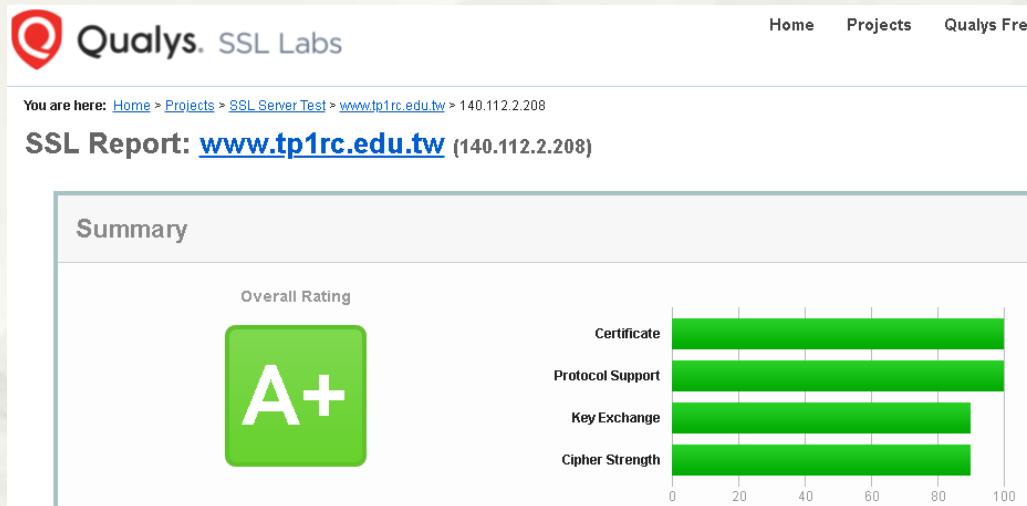
大綱

- * Apache
- * IIS

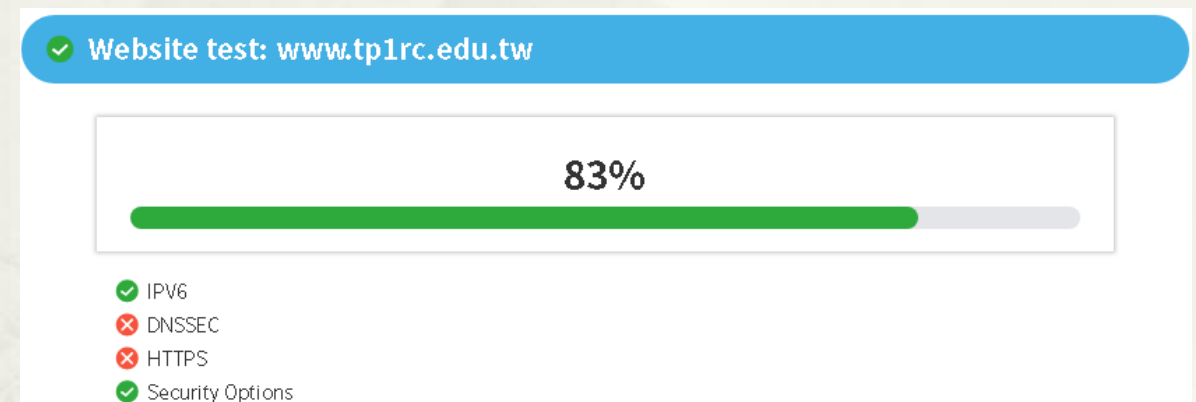


SSL Server Test

* <https://www.ssllabs.com/>



* <https://check.twnic.tw/>



The background of the slide features a large, faint, fan-shaped graphic. Inside this fan shape is a detailed, monochromatic illustration of a landscape, possibly a mountain range or a forest scene, rendered in a style reminiscent of traditional East Asian ink wash painting. The fan shape is centered on the slide and has a curved top and bottom edge.

Apache

SSL Server Test

disable SSLv3

Configuration



Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

- * 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

tcp.stream eq 4

No.	tcp.stre	Time	TTL	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
355	4	3.713245	128	172.16.0.2	64628	157.240.15.35	443	TCP	66	64628 → 443 [SYN] Seq=0 Win=81
400	4	3.844362	53	157.240.15.35	443	172.16.0.2	64628	TCP	66	443 → 64628 [SYN, ACK] Seq=0 A
401	4	3.844441	128	172.16.0.2	64628	157.240.15.35	443	TCP	54	64628 → 443 [ACK] Seq=1 Ack=1
402	4	3.844754	128	172.16.0.2	64628	157.240.15.35	443	TLSv1.2	571	Client Hello
442	4	3.973036	53	157.240.15.35	443	172.16.0.2	64628	TCP	60	443 → 64628 [ACK] Seq=1 Ack=51
445	4	3.973615	53	157.240.15.35	443	172.16.0.2	64628	TLSv1.2	200	Server Hello, Change Cipher Sp
447	4	3.973906	128	172.16.0.2	64628	157.240.15.35	443	TLSv1.2	105	Change Cipher Spec, Encrypted
456	4	3.981876	128	172.16.0.2	64628	157.240.15.35	443	TLSv1.2	147	Application Data

Length: 512

- Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: a0c1af898e6698e0869e3efd22eef67083ec39bc655c3f1e...
 - Session ID Length: 32
 - Session ID: 7108b7f3195629e96dd69368c0cd2825a968b79067d1880a...
 - Cipher Suites Length: 28
 - Cipher Suites (14 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 407
 - Extension: Reserved (GREASE) (len=0)
 - Extension: renegotiation_info (len=1)
 - Extension: server_name (len=21)
 - Type: server_name (0)
 - Length: 21
 - Server Name Indication extension
 - Server Name list length: 19
 - Server Name Type: host_name (0)
 - Server Name length: 16
 - Server Name: www.facebook.com
 - Extension: extended_master_secret (len=0)

Server Name (ssl.handshake.extensions_server_name), 16 bytes

Packets: 5439 · Displayed: 358 (6.6%) Profile: Defa

The background of the slide features a large, semi-circular graphic that resembles an open folding fan. Inside the fan's segments is a traditional Chinese landscape painting, likely a woodblock print, depicting mountains, trees, and a winding path. The entire graphic is rendered in a light, monochromatic style. Overlaid on this is the title text.

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

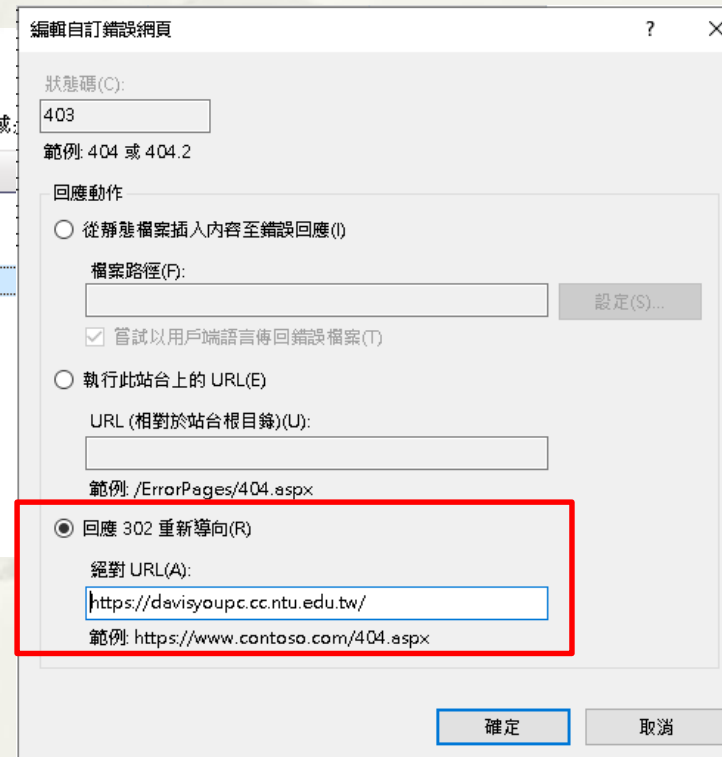
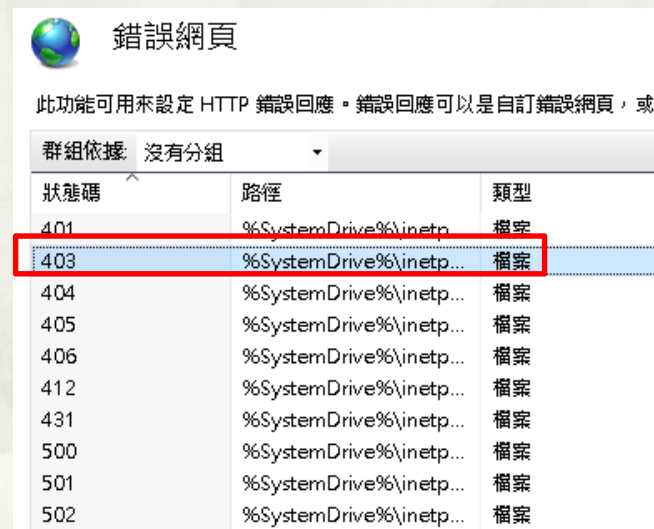
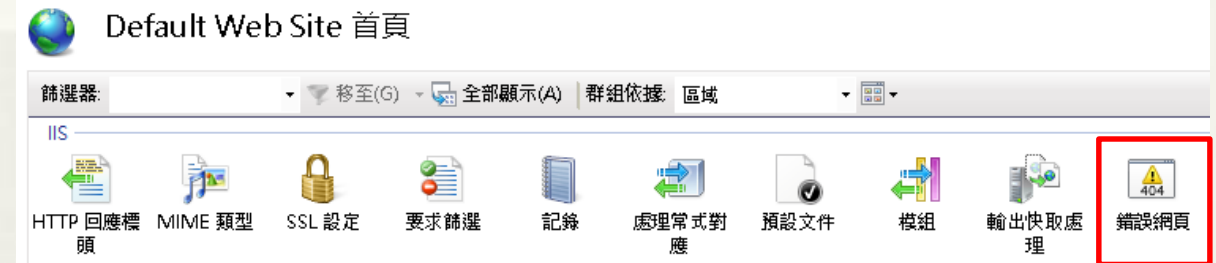
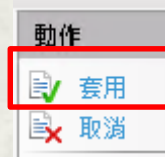
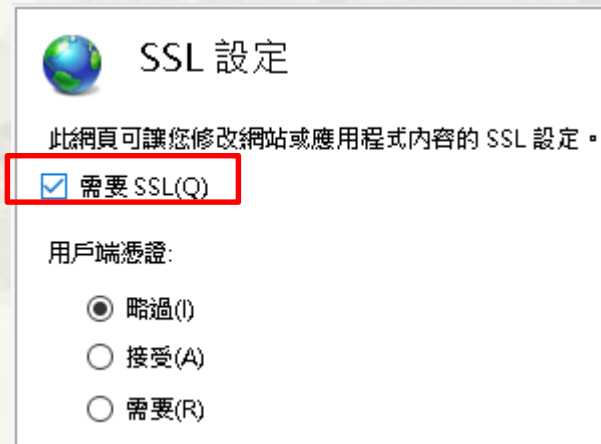
- * 不需要

- * 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

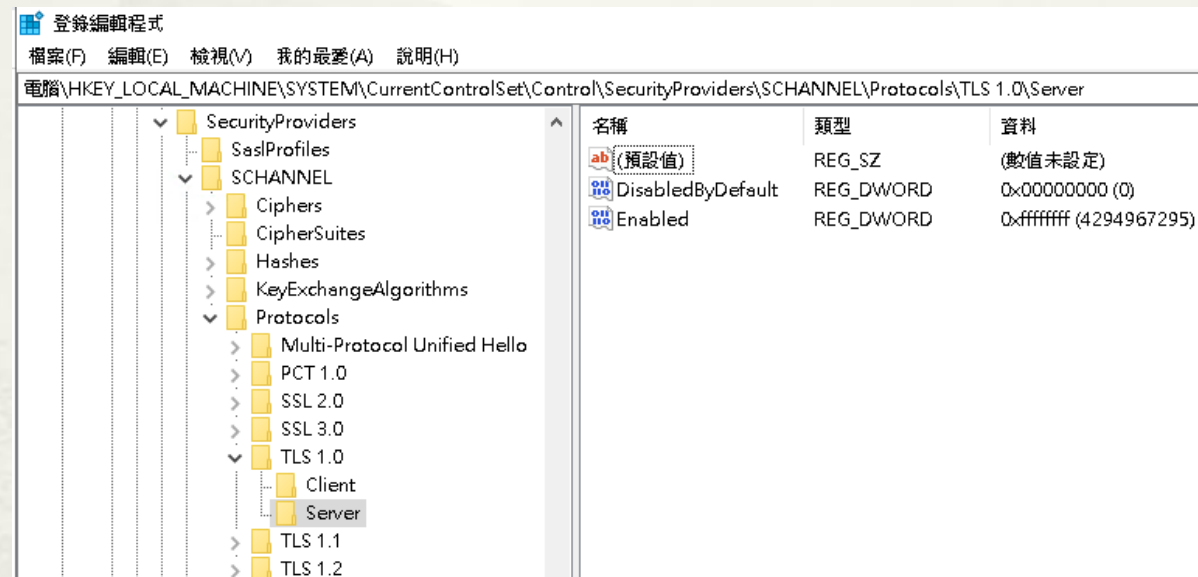
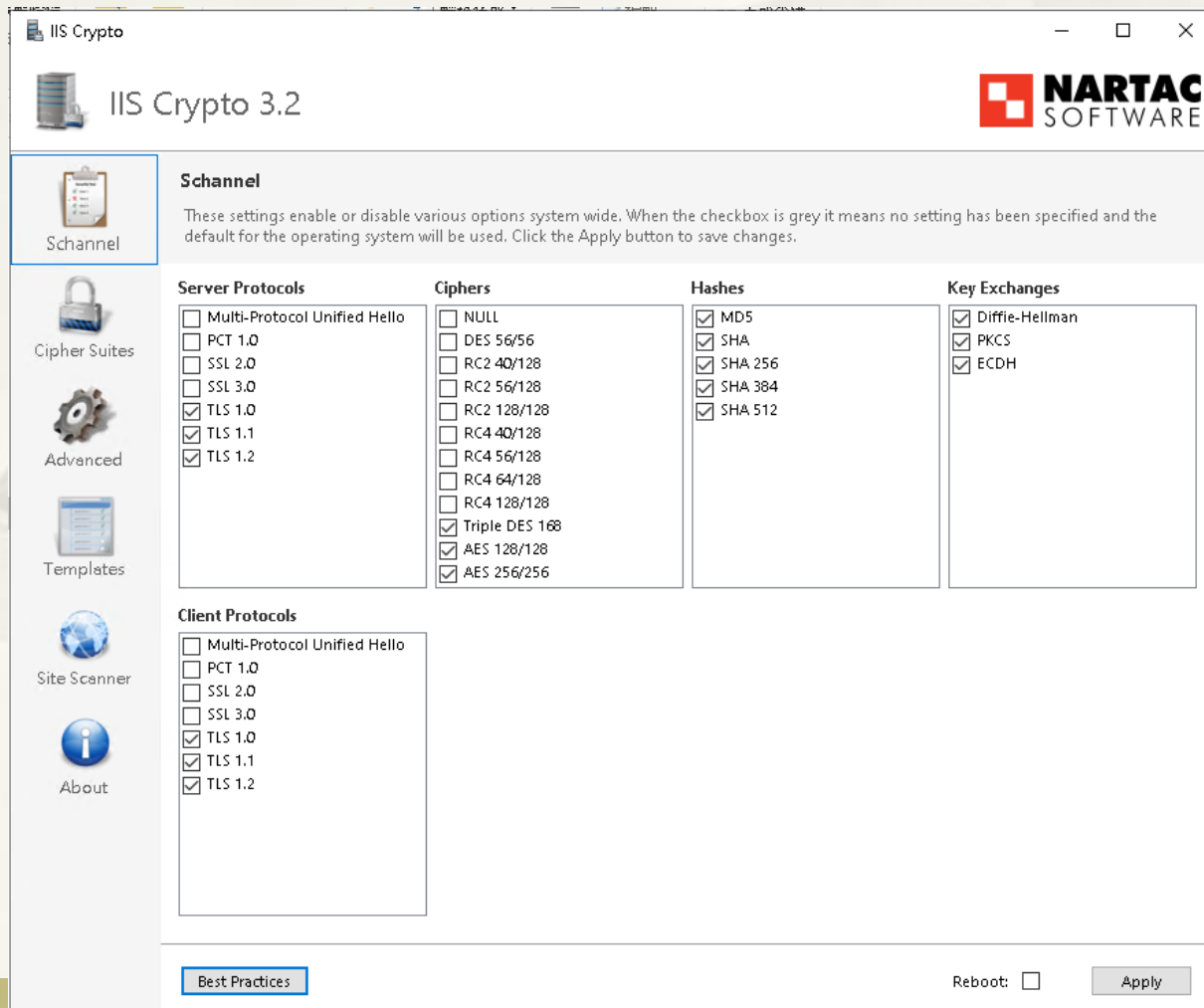
- * 手動

- * 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>

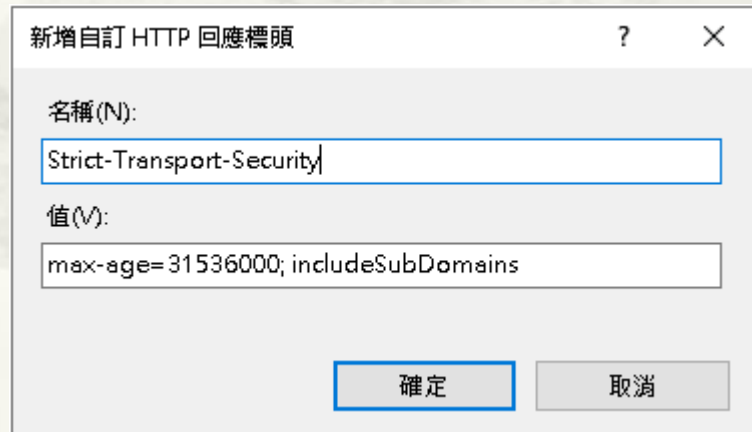
* regedit





Header 相關設定

HSTS



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

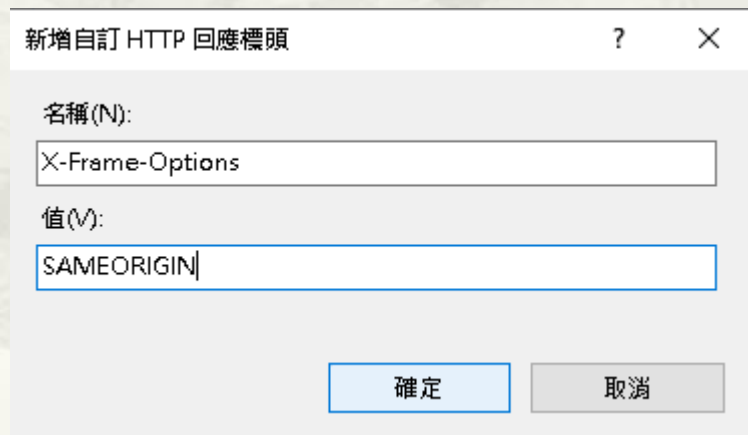



HSTS

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