Web HTTPS
服務規範

一、網站通過TWNIC的HTTPS檢測

至https://check.twnic.tw/檢測網站，並通過HTTP、TLS及Certificate等三項測試

1 HTTP

HTTPS 狀態

說明：
網站應提供HTTPS

Technical details:

Web server IP address	HTTPS existent
2001:288:6001:5:0:0:0:6	Yes
140.123.5.6	Yes

網站使用HTTPS

HTTPS 重導向

說明：
網站應設定會自動將HTTP網頁導向到HTTPS網頁

Technical details:

Web server IP address	HTTPS redirect
2001:288:6001:5:0:0:0:6	Yes
140.123.5.6	Yes

HTTP服務重導向HTTPS

HSTS

說明：
網站應提供HSTS政策

Technical details:

Web server IP address	HSTS policy
2001:288:6001:5:0:0:0:6	max-age=31536000
140.123.5.6	max-age=31536000

HSTS功能開啟並設定有效期

以IIS伺服器為例，在web.config檔案中新增下列指令進行配置，可達成重導向及啟用HSTS

重導向

啟用HSTS

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
    <rewrite>
        <rules>
            <rule name="HTTP to HTTPS redirect" stopProcessing="true">
                <match url="(.*)" />
                <conditions>
                    <add input="{HTTPS}" pattern="off" ignoreCase="true" />
                </conditions>
                <action type="Redirect" url="https://{HTTP_HOST}/{R:1}"
                    redirectType="Permanent" />
            </rule>
        </rules>
        <outboundRules>
            <rule name="Add Strict-Transport-Security when HTTPS" enabled="true">
                <match serverVariable="RESPONSE_Strict_Transport_Security"
                    pattern=".*" />
                <conditions>
                    <add input="{HTTPS}" pattern="on" ignoreCase="true" />
                </conditions>
                <action type="Rewrite" value="max-age=31536000" />
            </rule>
        </outboundRules>
    </rewrite>
</system.webServer>
</configuration>
```

註：HSTS的作用是強制客戶端（如：瀏覽器）使用HTTPS與伺服器建立連線，使用者無需手動在URL位址列中輸入HTTPS，

2 **Certificate**

trust chain of certificate

說明：
網站之憑證應由可信之CA單位簽署並且chain應完整

Technical details:

Web server IP address	Untrusted certificate chain
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

網站使用可信CA

public key of certificete

說明：
網站之憑證應包含足夠安全長度的public key

Technical details:

Web server IP address	Public key with insufficient length
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

金鑰長度2048 位元

註：可使用免費SSL憑證，如非營利組織網路安全研究小組（ISRG) 營運的Let’s Encrypt 憑證。
網址：https://letsencrypt.org/zh-tw/

signature of certificate

說明：
網站之憑證是使用足夠安全之演算法進行簽署

Technical details:

Web server IP address	Insecure hash algorithm
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

使用SHA256以上雜湊演算法

domain name on certificate

說明：
網站目前使用之domain name符合憑證內容的domain name

Technical details:

Web server IP address	Unmatched domains on certificate
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

使用的憑證網址與網站網址一致

憑證網址與網站網址相同

3 TLS

TLS版本

說明：

網站應提供安全的TLS版本支援

Technical details:

Web server IP address	Insecure TLS versions
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

使用TLS1.2以上

加密演算法(Cipher suite)

說明：

網站應提供安全的Cipher suite支援

Technical details:

Web server IP address	Insecure cipher suites
2001:288:6001:5:0:0:0:6	NONE
140.123.5.6	NONE

加密AES256以上
雜湊SHA256以上

SECURE RENEGOTIATION

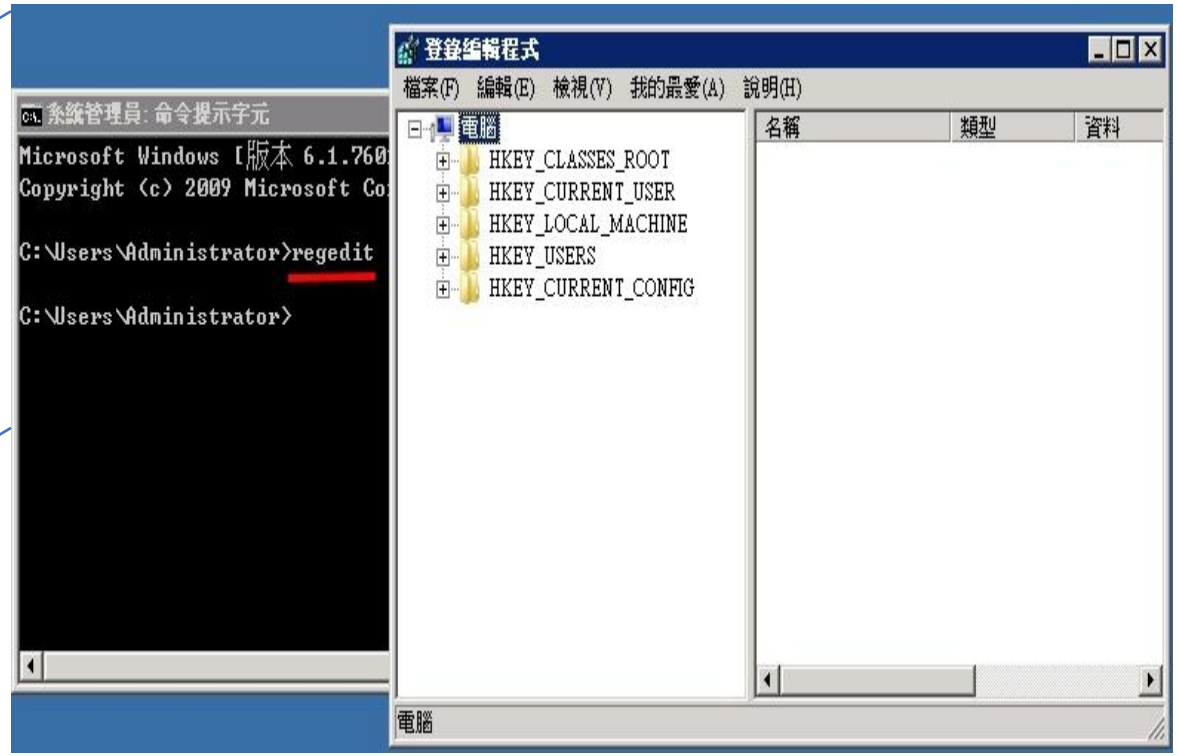
說明：

網站應支援TLS之 secure renegotiaton

Technical details:

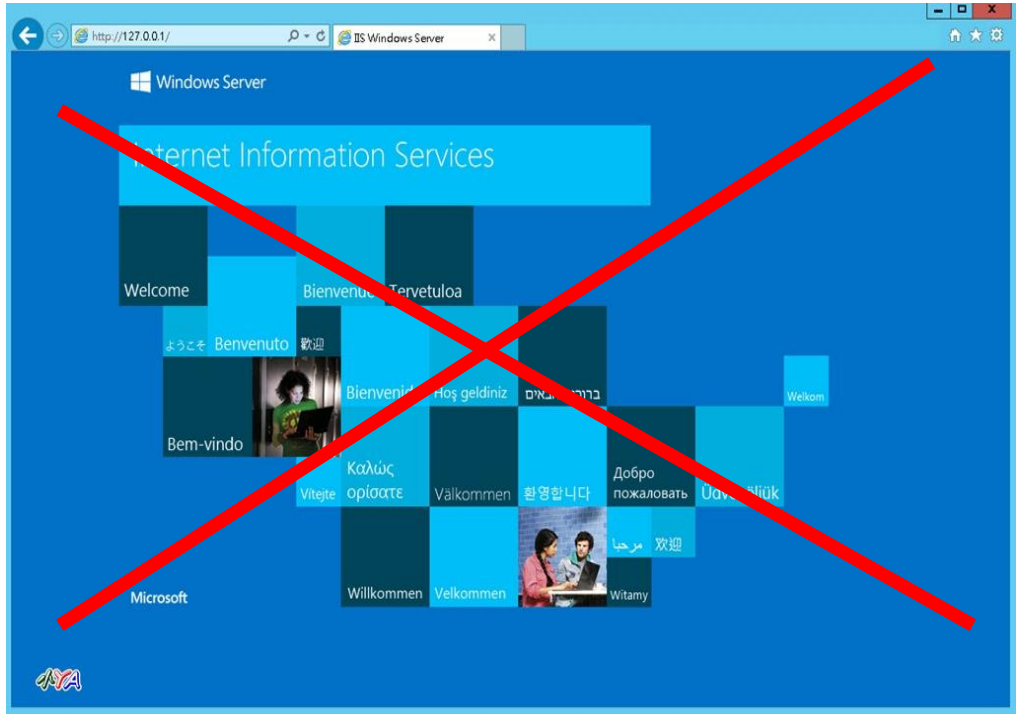
Web server IP address	Secure renegotiation
2001:288:6001:5:0:0:0:6	Yes
140.123.5.6	Yes

以windows 伺服器為例，在登錄檔可停用TLS1.0以下加密演算法



二、關閉非必要服務或資訊

- 無用網站請關閉並刪除DNS紀錄



- 內部系統網址勿暴露IP

三、【選項】

1. HTTP 和 HTTPS 的重導向行為應一致
   - 反例 www.5pc.gov.tw
     - http://www.[redacted].gov.tw 導向至[redacted].gov.tw
     - https://www.[redacted].gov.tw 導向至[redacted]rpb.gov.tw

同一網址的HTTP與HTTPS需導向同一網站

2. 部分網站僅有 www.XXXX.gov.tw
   - XXXX.gov.tw 不存在
   - XXXX.gov.tw 未正確導向 www.XXXX.gov.tw

*.edu.tw網址需與www. *.edu.tw同一網站

建議使用前述 HTTP 導向 HTTPS 所提之方法