

# Web HTTPS 服務規範

# 一、網站通過TWNIC的HTTPS檢測

✘ HTTPS

HTTPS(HyperText Transfer Protocol Secure),被說明為HTTP over TLS、HTTP over SSL或HTTP Secure,是透過網路進行安全通訊的傳輸協定,HTTPS經由HTTP進行通訊,進一步利用SSL/TLS來加密傳輸封包

1 HTTP

- ✔ HTTPS 狀態
- ✔ HTTPS 重導向
- ✔ HSTS

2 TLS

- ✔ TLS版本
- ✔ 加密演算法(Cipher suite)
- ✔ SECURE RENEGOTIATION

3 Certificate

- ✔ trust chain of certificate
- ✔ public key of certificate
- ✔ signature of certificate
- ✔ domain name on certificate

DANE

- ✘ DANE existence
- ✘ DANE validaty



## 現代化網路協定檢測

測試你的網站 Test your website

測試說明  
先進IP協定位址?網域名稱DNSSEC認證?安全連線?網路安全選項?  
[▶ about the test](#)

你的網址

開始測試

測試你的郵件主機 Test your email

測試說明  
先進IP協定位址?網域名稱DNSSEC認證?防止網路釣魚?網路安全選項?  
[▶ about the test](#)

你的 email 地址

開始測試

address

[▶ about the test](#)

開始測試

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

2001:288:6001:5:0:0:0:6

140.123.5.6

HTTPS existent
Yes
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

2001:288:6001:5:0:0:0:6

140.123.5.6

HTTPS redirect
Yes
Yes

HTTP服務重導  
向HTTPS

重導向

## HSTS

### 說明：

網站應提供HSTS政策

### Technical details:

#### Web server IP address

2001:288:6001:5:0:0:0:6

140.123.5.6

HSTS policy
max-age=31536000
max-age=31536000

HSTS功能開啟  
並設定有效期

啟用HSTS

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

```
<?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。

### 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	2001:288:6001:5:0:0:0:6
	140.123.5.6

Untrusted certificate chain	NONE
	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	2001:288:6001:5:0:0:0:6
	140.123.5.6

Public key with insufficient length	NONE
	NONE

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/>

金鑰長度2048 位元

✔ 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	2001:288:6001:5:0:0:0:6
	140.123.5.6

Insecure hash algorithm	NONE
	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	2001:288:6001:5:0:0:0:6
	140.123.5.6

Unmatched domains on certificate	NONE
	NONE

使用的憑證網址與網站網址一致

www005006.ccu.edu.tw

憑證

憑證資訊

這個憑證的使用目的如下：

- 向遠端電腦證明您的身分
- 確保遠端電腦的識別
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

\*請參照憑證授權單位敘述中的詳細資訊。\*

發給: www005006.ccu.edu.tw

簽署者: R3

有效期自 2021/3/11 到 2021/6/9

簽發者聲明(S)

確定

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

2001:288:6001:5:0:0:6  
140.123.5.6

Insecure TLS versions
NONE
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

2001:288:6001:5:0:0:6  
140.123.5.6

Insecure cipher suites
NONE
NONE

加密AES256以上  
雜湊SHA256以上

#### ✓ SECURE RENEGOTIATION

##### 說明：

網站應支援TLS之 secure renegotiaton

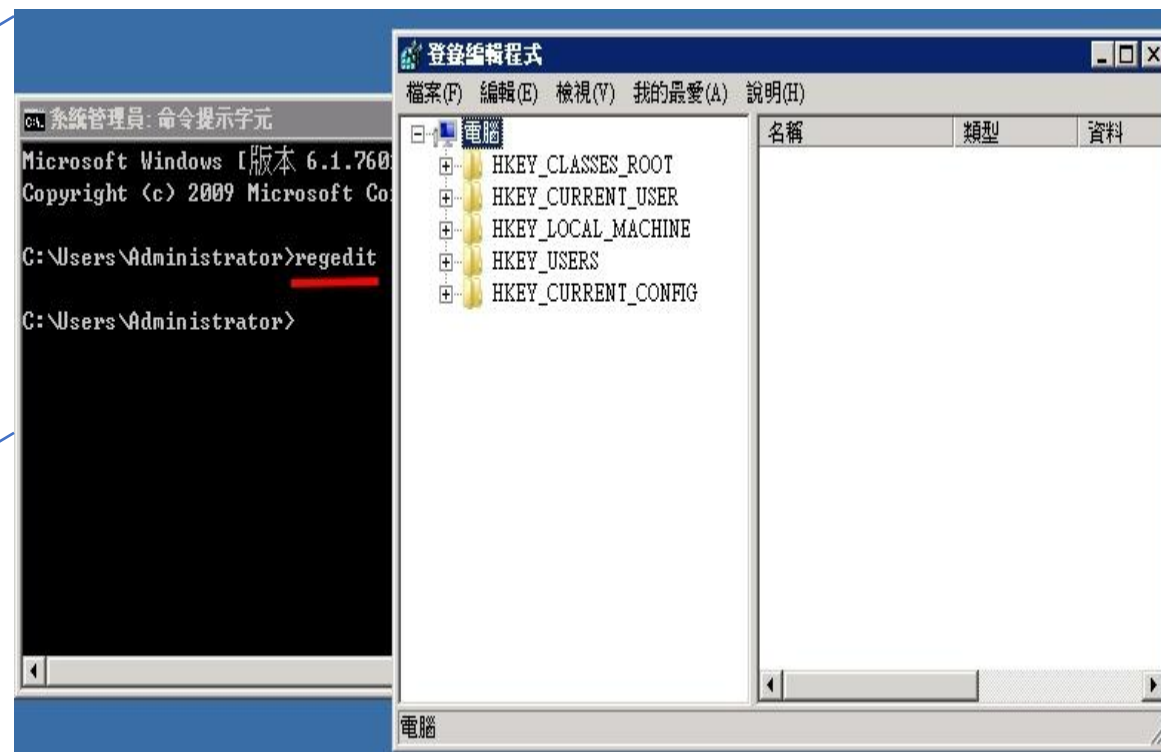
##### Technical details:

###### Web server IP address

2001:288:6001:5:0:0:6  
140.123.5.6

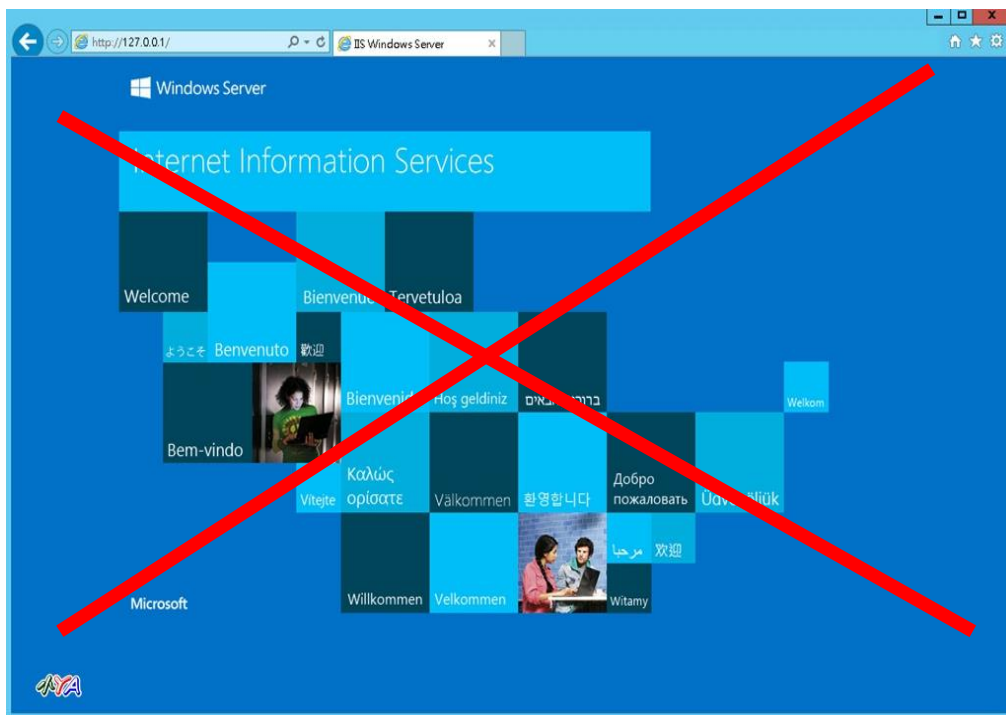
Secure renegotiation
Yes
Yes

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

- NAS(大宗)
  - [http://tn107-116. \[ \] edu.tw](http://tn107-116. [ ] edu.tw)
  - [http://tn107-116. \[ \] edu.tw](http://tn107-116. [ ] edu.tw)
- 網路印表機(大宗)
  - [http://tn106-37. \[ \] edu.tw](http://tn106-37. [ ] edu.tw)
  - [http://ip-120-125-14-252. \[ \] tw](http://ip-120-125-14-252. [ ] tw)
  - [http://ip-216-121. \[ \] edu.tw](http://ip-216-121. [ ] edu.tw)
- 網路攝影機
  - [http://tn106-187. \[ \] edu.tw](http://tn106-187. [ ] edu.tw)
- 非公開資料
  - TFS 資料庫 [http://203-71- \[ \] edu.tw](http://203-71- [ ] edu.tw)
- Infrastructure
  - ESXi 節點 [http://ip-120-125- \[ \] edu.tw](http://ip-120-125- [ ] edu.tw)

# 三、【選項】

## 1 HTTP 和 HTTPS 的重導向行為應一致

同一網址的HTTP與  
HTTPS需導向同一網站

○ 反例 www.5pc.gov.tw

- [http://www.\[\] .gov.tw](http://www.[] .gov.tw) 導向至 [\[\] .gov.tw]([] .gov.tw)
- [https://www.\[\] .gov.tw](https://www.[] .gov.tw) 導向至 [\[\] rpb.gov.tw]([] rpb.gov.tw)

## 2 部分網站僅有 www.XXXX.gov.tw

\*.edu.tw網址需與  
www.\*.edu.tw同一網站

- XXXX.gov.tw 不存在
- XXXX.gov.tw 未正確導向 www.XXXX.gov.tw

建議使用前述 HTTP 導向 HTTPS 所提之方法