資訊處
Office of Information Technology

# 各單位及所屬網站導入HTTPS說明

簡報單位：資訊處

簡報人員：蔡顯明

# 大綱

一、為什麼網站需要導入HTTPS

二、各單位及所屬網站導入HTTPS時程

三、網站安全連線狀況

四、網站環境及導入說明

A：資訊處標準環境vm主機

B：委外託管

C：單位自建

五、網站環境基本需求

六、其他資安相關事項

# 一、為什麼網站需要導入HTTPS

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 一、網站為什麼需要導入HTTPS

一、符合資通安全相關法令規範

二、提高網站資料傳輸的安全性

三、瀏覽器逐漸不支援非HTTPS網站


四、提升網站的可信任度

五、有助提升搜尋引擎排名


# 二、各單位及所屬網站導入HTTPS時程

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 二、各單位及所屬網站導入HTTPS時程

一、依行政院國家資通安全會報第31次委員會議決議、教育部107年3月21日臺教資(五)字第1070041450號函及108年10月24日臺教資(五)字第1080154973號函辦理。

發文日期：中華民國107年3月21日
發文字號：臺教資(五)字第1070041450號
速別：普通件
密等及解密條件或保密期限：
附件：國發會https簡報(1070041450_Attach1.pdf)

主旨：請依「政府機關導入網站安全傳輸通訊協定」推動目標及範圍(如附件)，依期程於107年6月底前完成所屬對外服務網站導入安全傳輸通訊協定(HTTPS)相關作業，請查照。

說明：依據國家發展委員會106年12月13日發資字第1061503130號函辦理。

正本：各國立大專校院、各國立大學附設醫院及農林場
副本：電子公文交換章 2018-03-21 15:49:57

# 二、各單位及所屬網站導入HTTPS時程

二、各單位所屬網站須於110.06.30前完成導入HTTPS。

三、未於期限內完成導入HTTPS之網站，自7月1日起將限制該網站之校外連線，未儘速完成改善者，除特殊原因外，考慮強制封鎖該網站。

四、請各單位收到「各單位及所屬網站HTTPS導入時程調查表」後，儘速填妥並核章後擲回資訊處。

如有未列出之網站，可自行至資訊處網站下載空白表單使用。

https://it.ccu.edu.tw/files/normal_form/HTTPS_20210125_v1.pdf

# 二、各單位及所屬網站導入HTTPS時程

五、填表問題舉例說明：

- 如何知道網站環境？
  - 自建主機可以洽詢網站主機管理人員
  - 委外託管者請洽委辦廠商。
- 網站已無再需要使用
  - 請關閉該網站，並於備註說明欄註明「已關閉此網站」
  - 使用資訊處vm主機者，請註明「請撤銷本vm主機」
- 網站已經(或將要)委由外包廠商處理中
  - 請註明「委外處理中」(網站完成後請歸還vm主機)
- 其他問題，請洽14105蔡先生

# 二、各單位及所屬網站導入HTTPS時程

國立中正大學各單位及所屬網站 HTTPS 導入時程調查表

編號：_____

| | | | |
|---|---|---|---|
| 單位名稱 | | | |
| 網站名稱 | | | |
| 網站ＩＰ | | | |
| 網站用途 | | | |
| 網站環境 | 作業系統：_____ （例:FreeBSD 9.2）<br>網站伺服器：_____ （例：Apache 2.4.38）<br>PHP 版本：_____ （例：7.1.26） | | |
| 導入時程 | 預計 110 年 ____ 月 ____ 日前完成（110.06.30 前） | | |
| 備註說明 | | | |
| 填表人 | | 主管簽章 | |

# 三、網站安全連線狀況

## (以Chrome為例)

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

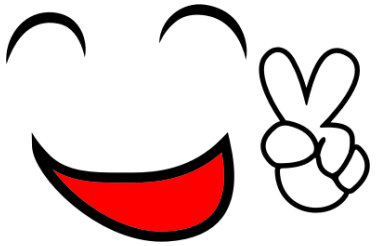
# 三、網站安全連線狀況

## 一、如何知道網站是否已經導入 HTTPS？

➢ **已導入**：

- 輸入https://網站名稱可正常顯示頁面，網址列出現安全瑣圖示。
- 輸入http://網站名稱被自動導向安全連線https://網站名稱。


➢ 點擊安全鎖圖示後，在彈出的訊息視窗上會出現「憑證(有效)」的資訊。



# 三、網站安全連線狀況

➢ **未導入**：

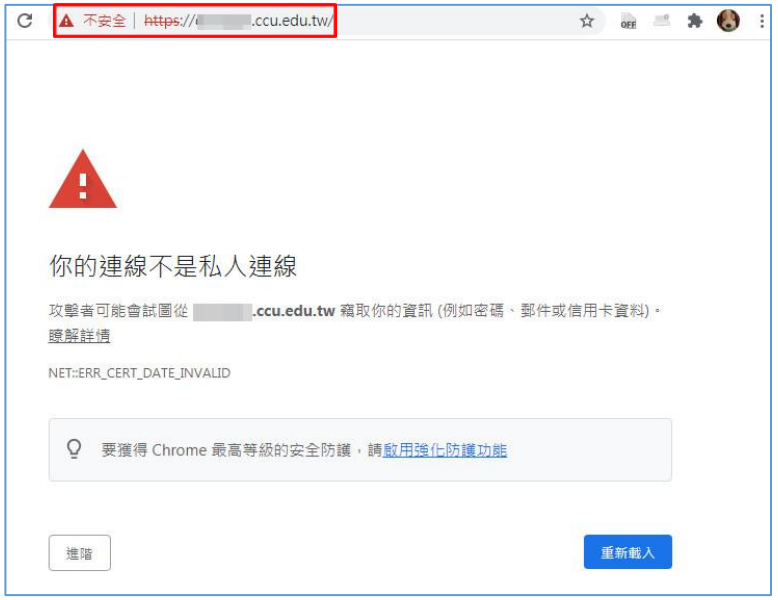
- 輸入http://網站名稱可正常顯示頁面，網址列出現不安全的三角形圖示，
- 將http://網站名稱改成https://網站名稱出現「無法連上這個網站」，網址列出現圓形驚嘆號符號。



※點擊不安全的三角形圖示或圓形i圖示，彈出的訊息視窗上沒有出現「憑證」的項目。

# 三、網站安全連線狀況

- **憑證過期**：已導入HTTPS的網站，連線時出現紅色三角形的不安全連線，點擊圖示彈出的訊息視窗上出現「憑證(無效)」。



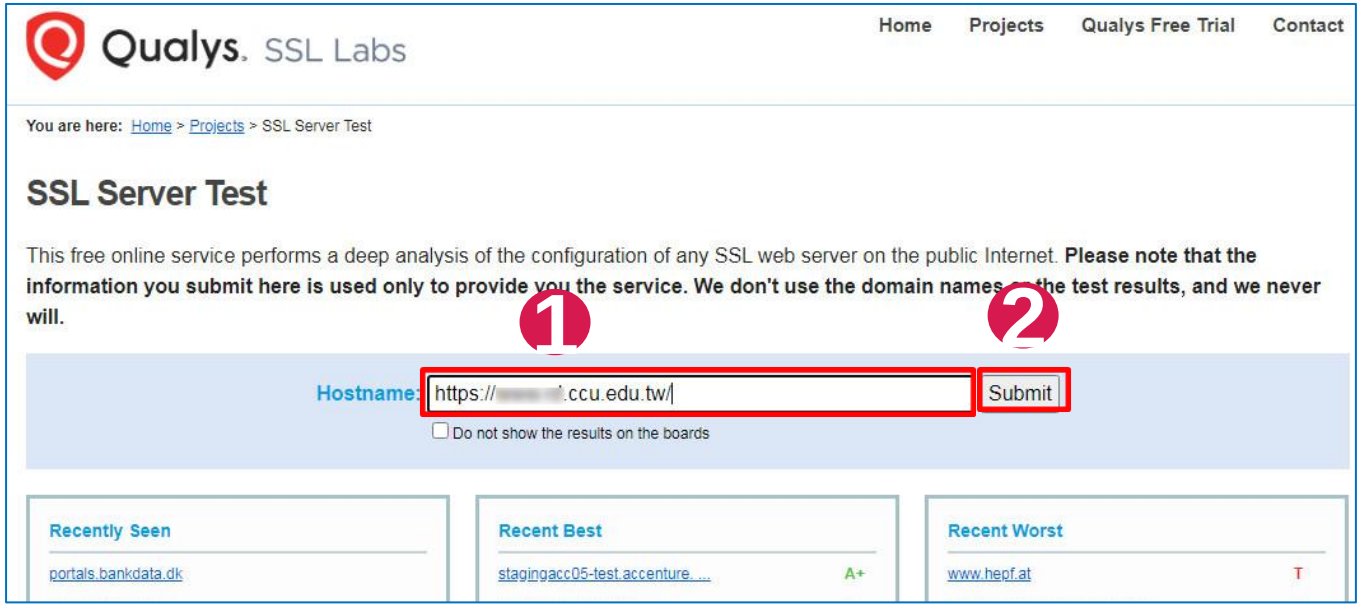


- **未強制導向**：已導入HTTPS之網站，以http://...方式連線沒有自動導到https://...，未強制導向仍具資安風險，須改為強制導向方式。

# 三、網站安全連線狀況

## 二、如何知道網站支援的TLS版本？

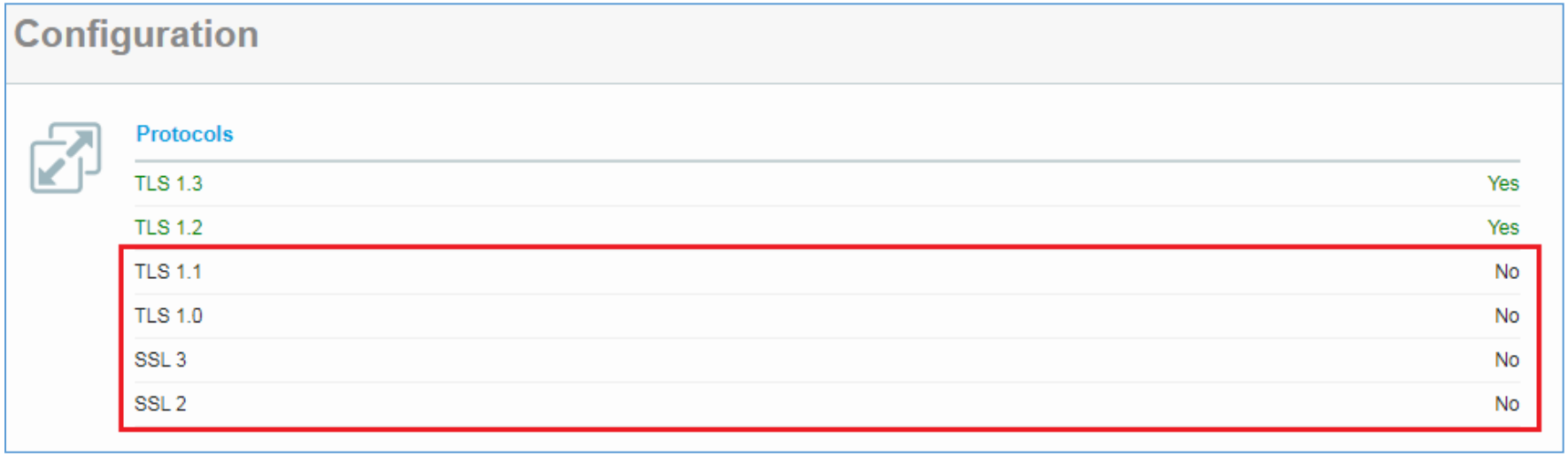
- 利用 Qualys SSL Labs 線上服務進行測試
- 未導入HTTPS之網站或使用IP型式之網址**無法測試!**




網址：https://www.ssllabs.com/ssltest/

# 三、網站安全連線狀況

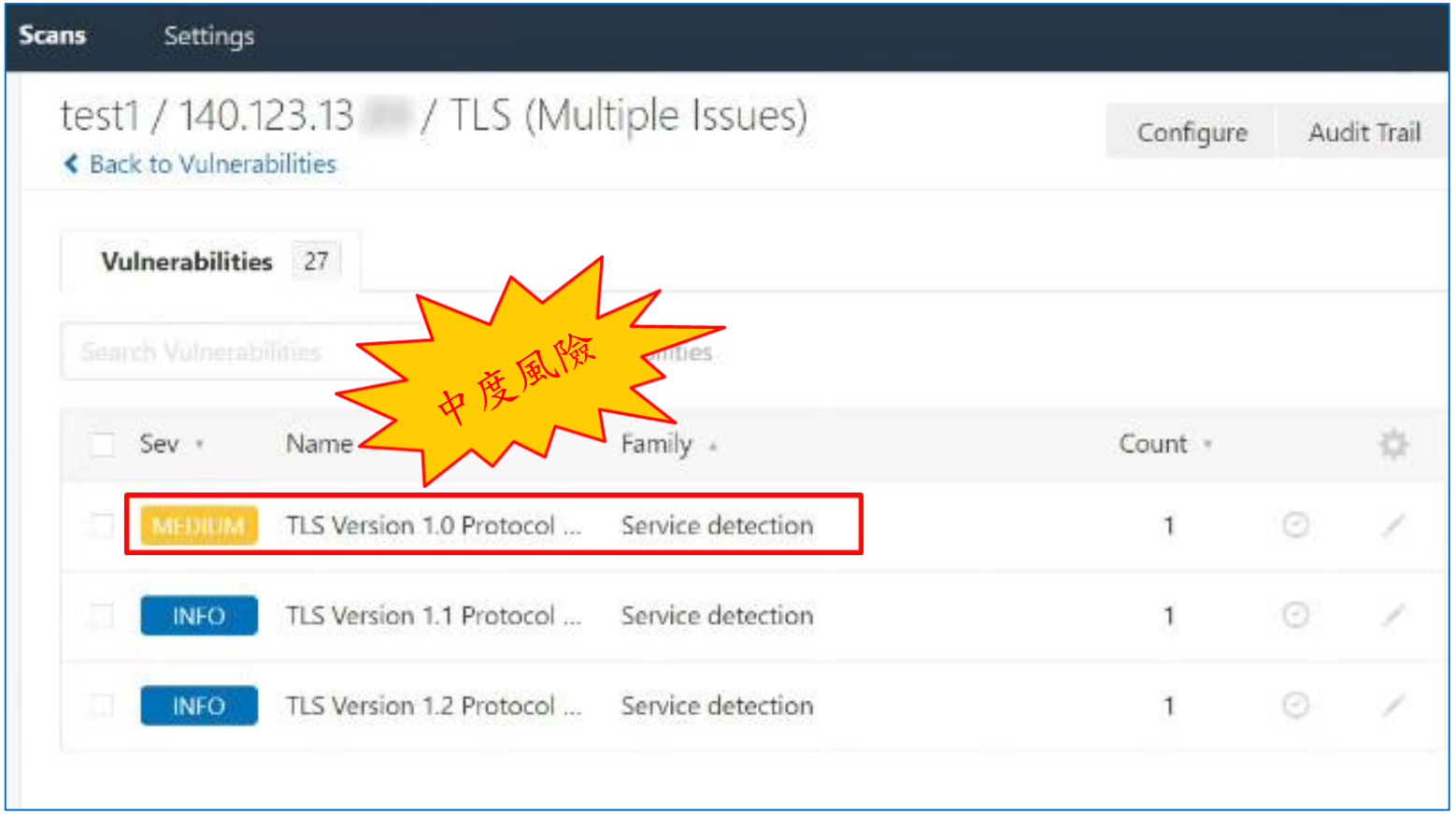
- 測試結果相當完整，請將畫面向下捲至Configuration處，即可看到傳輸層加密協定的狀態：




- 請確定 TLS1.1 / TLS1.0 / SSL3 / SSL2 均為 No。

# 三、網站安全連線狀況

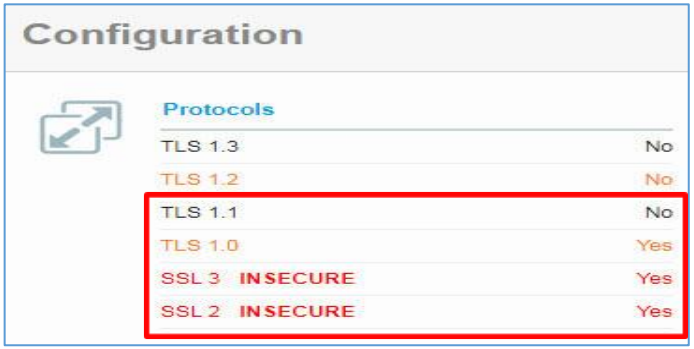
- 使用nessus資安弱掃軟體掃瞄，顯示網站有中度風險：



# 三、網站安全連線狀況

➢ 某單位網站實際案例：






- 已安裝憑證且在有效期限內，但開啟加密協定具高度資安風險。

# 四、網站環境及導入說明

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 四、網站環境及導入說明

## 環境一：資訊處提供之**標準環境vm主機**

- 網站環境(作業系統、Apache、PHP)需升級至最新版。原機升級可能導致網站無法正常運作，進行方式如下：
  - 申請借用新版環境之測試vm主機(本處不負責網站資料之搬移)
  - 完成網站測試，取代原vm主機(資料及資料庫請先完整備份)
  - 兩個步驟均需填寫單位網站VM主機服務異動申請表（參見下頁）
- 確定站內連結使用相對路徑寫法。
- 網站以IP形式連線者需先申請DNS。
  - 例如 http://140.123.13.141/
  - 校園網路領域名稱(DNS)及校外連線 申請/異動單（蕭先生 ext.14108）
- 完成網站環境升級後，由資訊處協助導入HTTPS。

# 四、網站環境及導入說明

## ➢ 單位網站VM主機服務異動申請表填寫說明

- 【系統升級**階段一**】借用新版vm測試主機：

| | |
|---|---|
| ■系統升級 | ■暫借vm測試主機，進行網站測試 □網站測試無誤，取代原vm主機(資料已備份完成)<br>1.本項服務僅限使用本處提供之標準環境，使用外包廠商環境者請自行洽廠商處理。<br>2.原機升級可能導致網站無法正常運作，本處將提供新版環境之暫時測試機供貴單位測試使用，待網站測試無誤後，再以測試機取代原主機。 |

- 【系統升級**階段二**】測試完成，取代原vm主機並導入HTTPS：

| | |
|---|---|
| ■系統升級 | □暫借vm測試主機，進行網站測試 ■網站測試無誤，取代原vm主機(資料已備份完成)<br>1.本項服務僅限使用本處提供之標準環境，使用外包廠商環境者請自行洽廠商處理。<br>2.原機升級可能導致網站無法正常運作，本處將提供新版環境之暫時測試機供貴單位測試使用，待網站測試無誤後，再以測試機取代原主機。 |
| ■導入HTTPS | 1.本項服務僅限使用本處提供之標準環境，使用外包廠商環境者請自行洽廠商處理。<br>2.網站環境(含作業系統、Apache、PHP)需升級至最新版本。<br>3.網站若為 IP 形式，需先申請DNS名稱。 |

# 四、網站環境及導入說明

## ➢ 單位網站VM主機服務異動申請表填寫說明

- 網站已委外託管，撤銷vm主機：

| | |
|---|---|
| ■撤銷vm主機 | 撤銷原因：網站已委外託管<br>(網站內容及資料庫請先自行備份，本處不負備份責任) |

- 已無需此網站，撤銷vm主機：

| | |
|---|---|
| ■撤銷vm主機 | 撤銷原因：已無須此網站<br>(網站內容及資料庫請先自行備份，本處不負備份責任) |

# 四、網站環境及導入說明

## 環境二：單位**自建主機**

- 單位自建主機，需由自己的網站主機人員自行處理。
- 網站以IP形式連線者需先申請DNS。
  - 校園網路領域名稱(DNS)及校外連線 申請/異動單（蕭先生 ext.14108）
- 網站環境(作業系統、Apache、PHP)請升級至最新版本。
- 安裝SSL憑證
  - 付費憑證：請洽 TWCA（台灣網路認證公司），效期可依需求購買。
  - 免費憑證：Let's Encrypt，效期僅3個月。
- 基於資安考量，請關閉TLS 1.1/TLS 1.0/SSL3/SS2協定。

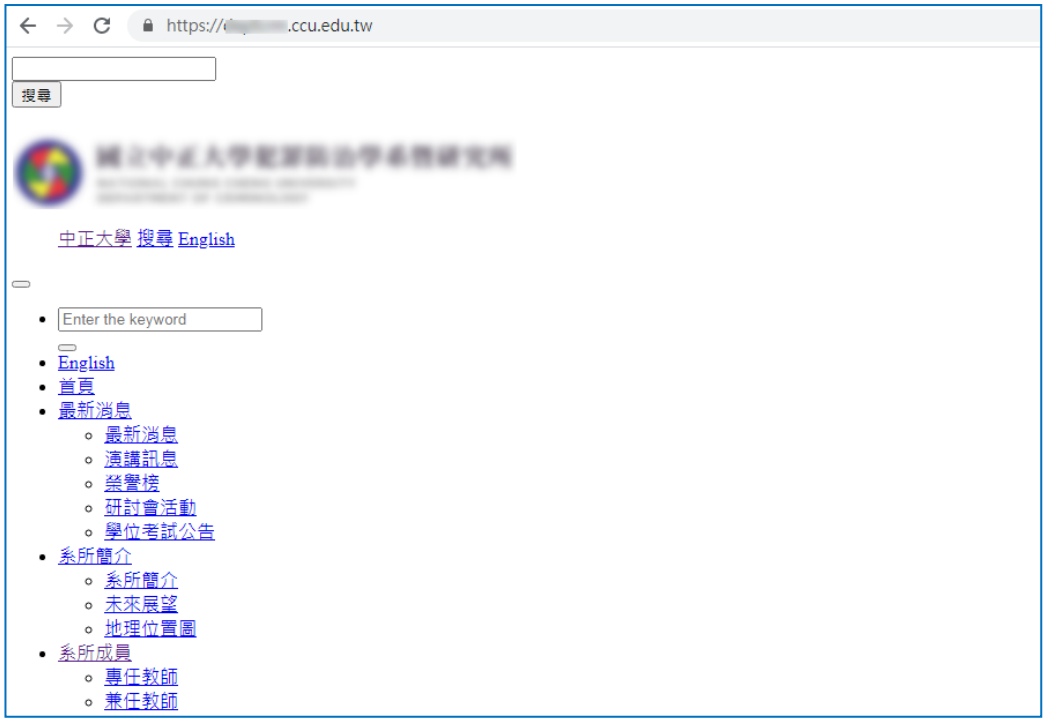
# 四、網站環境及導入說明

## 環境三、**委外託管**

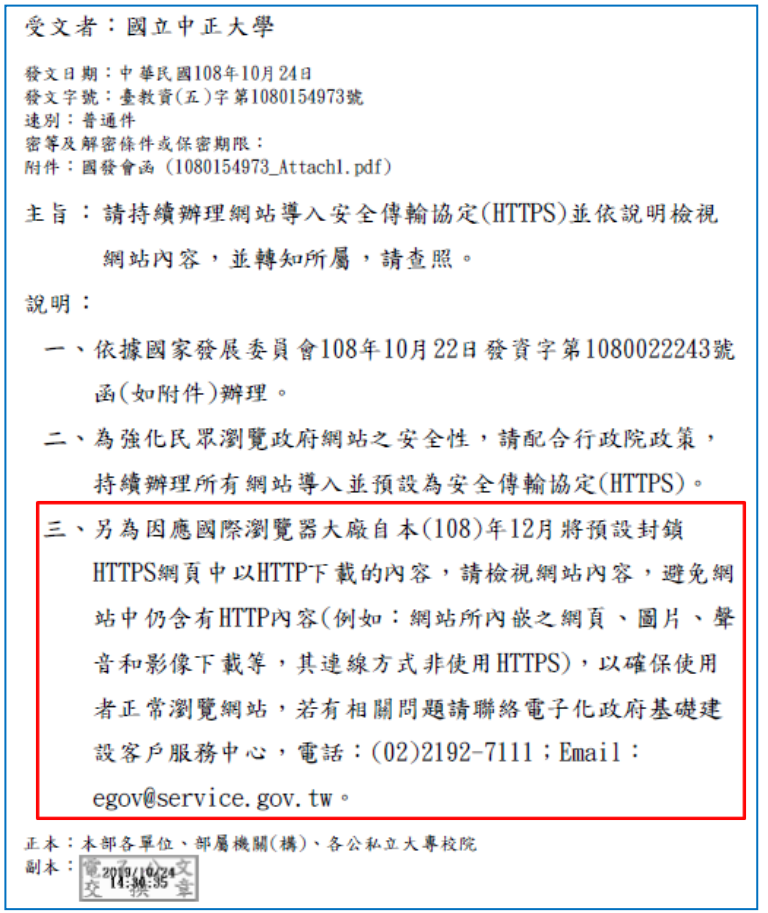
- 網站委外託管者，請洽委辦廠商協助處理。
- 請確認網站環境(作業系統、Apache、PHP)是否有經常修補安全漏洞，並適時升級至最新之安全版本。
- 請委辦廠商協助購買及安裝SSL憑證，並導入HTTPS。
- 基於資安考量，請關閉TLS 1.1/TLS 1.0/SSL3/SS2協定。

# 四、網站環境及導入說明

## 四、站內連結請使用相對路徑寫法




使用http://絕對路徑會導致某些檔案無法存取，使得畫面無法正常顯示。



受文者：國立中正大學

發文日期：中華民國108年10月24日
發文字號：臺教資(五)字第1080154973號
速別：普通件
密等及解密條件或保密期限：
附件：國發會函 (1080154973_Attach1.pdf)

主旨：請持續辦理網站導入安全傳輸協定(HTTPS)並依說明檢視網站內容，並轉知所屬，請查照。

說明：

一、依據國家發展委員會108年10月22日發資字第1080022243號函(如附件)辦理。

二、為強化民眾瀏覽政府網站之安全性，請配合行政院政策，持續辦理所有網站導入並預設為安全傳輸協定(HTTPS)。

三、另為因應國際瀏覽器大廠自本(108)年12月將預設封鎖HTTPS網頁中以HTTP下載的內容，請檢視網站內容，避免網站中仍含有HTTP內容(例如：網站所內嵌之網頁、圖片、聲音和影像下載等，其連線方式非使用HTTPS)，以確保使用者正常瀏覽網站，若有相關問題請聯絡電子化政府基礎建設客戶服務中心，電話：(02)2192-7111；Email：egov@service.gov.tw。

正本：本部各單位、部屬機關(構)、各公私立大專校院
副本：電子公文交換章 2019/10/24 14:39:35

# 四、網站環境及導入說明

## ※絕對路徑 vs. 相對路徑

- 絕對路徑(指明檔案所在的主機名稱或IP)
  - <a href="https://www.ccu.edu.tw/file.php">
  - <a href="http://140.123.13.100/folder/file.php">

- 相對路徑（不指定檔案所在的主機或IP)
  - <a href="file.php">
  - <a href="/folder/file.php">

# 五、網站環境基本需求

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 五、網站環境基本需求

一、作業系統

- FreeBSD 升級至 12.0 以上版本。
- Ubantu 升級至 19.0 以上版本。
- Windows Server 升級至 2019 以上版本。
  (Windows Server 2016或以前版本需導入GCB)

二、網站伺服器

- Apache 升級至 2.4 以上版本。
- nginx 升級至 1.18 以上版本。
- IIS 升級至 8.5 以上版本。

三、PHP 升級至 PHP 7.4 或以上版本。

四、關閉 TLS 1.0 / TLS 1.1 / SSL3 / SSL2。

# 六、其它網站資安問題

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 六、其它網站資安問題

一、Flash動畫存在資安風險，且Adobe官方已不再支援，因此各大瀏覽器廠商也不再支援，各單未網站如有使用Flash者，請儘早進行改版。


# 六、其它網站資安問題

二、應使用ssh及sftp等加密傳輸協定來維護網站，並停用telnet及ftp等未加密的傳輸協。

三、基於資安考量，網站主機應設定防火牆，僅開放特定IP來進行網站維護。

# 快速重點回顧

業務窗口：蔡先生 分機14105

技術窗口：陳先生 分機14104

# 快速重點回顧

一、各單位所屬網站應於6月30日前完成導入HTTPS。

二、各單位收到「各單位及所屬網站HTTPS導入時程調查表」後，請於一週內填妥經主管核章後擲回資訊處。

如有遺漏之網站，可自行至資訊處網站下載空白調查表填寫。

三、網站環境(包括作業系統、網站伺服器軟體、PHP等)更新至最新之穩定版本。

四、TLS1.0 / TLS 1.1 / SSL3 / SS2 具資安風險，應強制關閉。

五、業務窗口：蔡先生 ext.14105 tsices@ccu.edu.tw

技術窗口：陳先生 ext.14104 shchen@ccu.edu.tw

DNS 業務：蕭先生 ext.14108 vchsiao@ccu.edu.tw

THANK YOU

# 簡報完畢

國立中正大學 資訊處