大學聯招網路選填志願之設計與實作

郭建邦
國立成功大學電機系
isaackuo@crypto.ee.ncku.edu.tw

陳日昇
國立成功大學計網中心
zschen@mail.ncku.edu.tw

賴溪松
國立成功大學電機系
laihcs@eembox.ncku.edu.tw

摘要

本論文在於介紹我國首次舉辦的網路選填志願作業之安全性考量暨相關作業，由於國內甚至全世界尚未有將此類重要服務網路化的經驗，故希望藉由此篇論文將此一寶貴經驗分享出來。文中將簡介網路選填志願過程中相關的角色定位，同時說明如何達到網路選填志願的四個重要目標：1)可用性、2)完整性、3)安全性、4)公平性。其中將著重說明安全性的部分，在此部分我們共作了三項測試以及提出一項建議，藉以確保網路選填志願服務能夠順利運作。

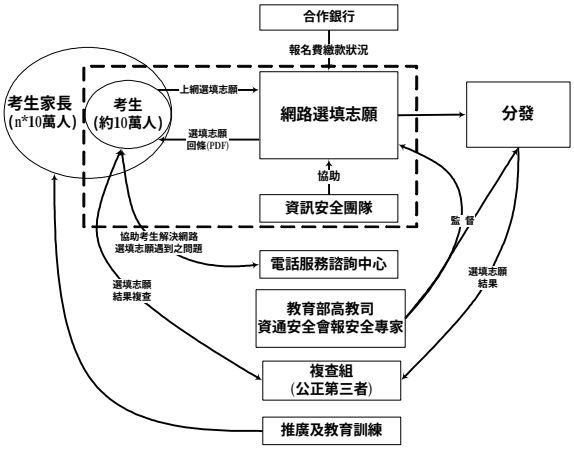
關鍵詞：網路選填志願、安全性測試

一、前言

隨著網際網路時代的來臨，舉凡食、衣、住、行、育、樂都可以透過網路取得，許多原本必須本人親自辦理的事項也都漸漸網路化，甚至也有所謂『多用網路，少用馬路』等口號喊出，凸顯利用網路辦事可以更加省時有效率。我國的莘莘學子在經歷高中三年苦讀的求學生涯後，隨即面對個人未來生涯發展至關重要的選填志願；以往的選填志願是利用劃卡繳交的方式進行，但是此一方式有著下列幾項缺點：1)限定劃填 90 個志願、2)無法顯示校系名稱，易畫錯志願代碼、3)志願卡污損導致讀卡機無法正確判讀。在這個網路化的時代，若能將選填志願一事改以網路進行，相信能夠提供考生最大的便利性並且避免上述的缺點，同時利用網路的特性，可以減少考生及家長們舟車勞頓的辛勞，也不用受限需於特定時間才能夠到各服務學校進行繳卡作業，只要輕鬆的在家中利用自己的電腦及網路即可進行選填志願。另外，由於是利用網路進行選填志願，因此在未完成送出前的階段，考生可以反覆地思考所選填的志願是否適合，待最後確認後才將志願送出，而志願送出後即如同傳統的繳卡作業完成，將無法再進行更改。利用網路選填志願主要是提供考生一較傳統方式更加便利的管道進行，所有的作業程序仍舊依照聯合分發委員會既有的流程進行。

二、網路選填志願關係圖及目標說明

94 年聯合分發委員會在經過討論，根據中央大學於 91 年所做的調查以及成功大學 93 年試辦網路選填志願的結果，決定將 94 學年度的選填志願由傳統的劃卡方式改為利用網路選填志願，此一作法可謂我國網路服務上的一大創舉，因為選填志願一事對於甫畢業的高中生而言影響深遠，乃關乎其一生的生涯規劃發展。因為明瞭網路選填志願的重要性，故聯分會針對網路選填志願亦不斷進行沙盤推演、排練，並費盡心思期望能夠提供考生一安全無虞的環境進行選填志願，同時亦能夠確保選填志願過程一切順暢以及維持分發作業的正確性。下圖為依據此次網路選填志願作業所描繪出的關係圖，本論文主要著重於探討下圖中的虛線框，即資訊安全的部分。



1. **考生及家長：**

考生為網路選填志願系統之直接使用者，94 年度報名參與網路選填志願之考生共有 100,265 人，最後完成選填志願者共有 99,900 人；而每位考生的父母或親友對選填志願作業亦會參與或關心，此部分的人數則至少為參與選填志願之考生人數的兩倍。

2. **網路選填志願：**

此部分為選填志願之核心，所有的網路選填志願作業皆在此部分進行；選填志願所牽涉到的資料非常多，每位考生可選填至 100 個志願，同時國內各大學院校加總起來的校系數共有 1469 個，而

全部又有 497 種加權以及其它的限制條件，為確保網路選填志願作業過程中所呈現的資料正確無誤，光在此一部分即花費許多的時間進行人工查核、檢驗，以確保考生在選填志願過程中不致接收到錯誤的訊息而導致錯填志願。

3. 資訊安全團隊：

為確保國內首次舉辦的網路選填志願作業能夠讓考生安心使用，故規劃一外部資安團隊協助進行網路選填志願作業的安全查核。資安團隊主要的目標在於協助找出網路選填志願所使用的應用程式、軟硬體及網路架構是否足夠安全，讓考生能夠在網路選填志願時，不會發生選填志願資料外洩或是選填志願主機甚至分發主機遭受入侵及攻擊，導致選填志願作業中斷。故資安團隊在此次的網路選填志願中扮演極重要的角色，可謂是系統上線前最重要的把關者。

4. 教育部高教司、資通安全會報安全專家：

教育部高教司為我國高等教育之負責單位，網路選填志願亦獲得高教司之支持與協助，同時為確保網路選填志願的安全性，高教司亦請國家資通安全會報之安全專家協助檢視架構設計是否足以抵禦可能之攻擊。

5. 分發：

網路選填志願除了要讓考生能夠順暢地利用網路完成選填志願，亦必須在選填志願結束後，儘速且正確地完成分發結果；此部分亦需耗費大量人力進行抽查檢驗。

6. 複查組：

複查組此次由淡江大學擔任，於網路選填志願中扮演的角色為一公正第三者，加密志願檔所使用的金鑰由此一公正第三者產製給電算組使用；同時複查主機之管理全由複查組掌控，電算組僅能將完成之選填志願資料存入複查主機並無其它權限。

7. 推廣及教育訓練：

由於網路選填志願為第一次舉辦，為讓考生、家長及各高中教師能夠及早對網路選填志願作業有所瞭解，自 94 年 2 月份開始即陸續舉辦高中種子教師說明會、家長說明會、製作選填志願教學版…等推廣及教育訓練措施。

8. 電話服務諮詢中心：

因首次舉辦網路選填志願，故聯分會規劃設置一 24 人編制之電話服務諮詢中心，協助考生解決進行網路選填志願時所遇到的問題。

9. 合作銀行：

與銀行相關的作業主要是考生需繳交登記分發報名費方能進行網路選填志願作業，考生於繳款完畢後可先行查詢繳款狀態，若已完成則可立即登入網路選填志願網站進行志願選填。

為確保網路選填志願的作業一切正常無誤，我們為此次作業訂下下列四個目標：

1. 可用性：

為使第一次舉辦的網路選填志願作業能夠讓使用者(考生)在使用上減輕負擔，不需額外花費太多時間學習，故在系統設計上我們以網頁的形式呈現，使用者只需要利用瀏覽器(Internet Explorer 5.5 以上)即可使用，使用方式與平常瀏覽網站相仿，可讓使用者減少額外的學習時間。

同時為確保網路選填志願的可用性，亦請中華電信協助進行壓力測試以及舉辦模擬選填志願測試，確保網路選填志願的可用性。

2. 完整性：

網路選填志願最重要的就是考生所選填的志願與最後用以進行分發作業的志願資料必須一致，同時也是整個網路選填志願的重心所在；而此一份志願檔資料也是將來考生若要進行複查作業時會用到的，故維持考生志願檔的完整性為網路選填志願作業中重要的一環。

3. 安全性：

由於此次選填志願全部都是在網路上進行，故網路安全的防護必須特別注意，主要須避免任何的系統、網路漏洞存在，給予有心人士或駭客可趁之機。另外，我們除了考量網路安全的問題外，亦一併考量整體網路流量的分流情形。在規劃中，整個網路選填志願系統全部都納在防火牆後方，同時並針對防火牆的策略設定進行多次的討論，藉以尋求出最適合的方案，期能兼顧網路選填志願的便利性以及安全性。同時也針對此一架構反覆進行相關測試，以確保安全無虞。

4. 公平性：

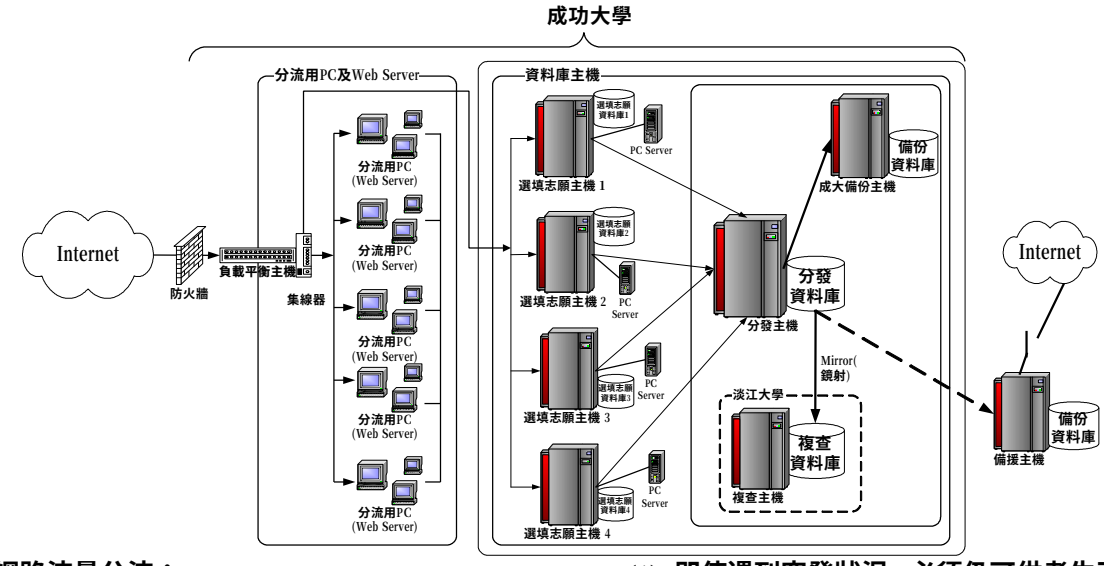
此點的目標主要是希望使用者能夠放心、安心的使用網路選填志願系統，藉由複查組產製加密的金鑰供電算組使用，由複查組扮演公正第三者的角色，讓考生以及社會大眾對於網路選填志願系統能有正面的看法，不致於認為是黑箱作業；並藉此昭告網路選填志願系統的透明以及公開化。

三、網路選填志願之實作與數據說明

為達到上節中所述的四個主要目標，我們設計出的網路選填志願架構圖如下頁圖中所示，簡略說明如下：

1. 防火牆：

我們將整個網路選填志願系統納入防火牆的保護，而防火牆的策略設定亦經不過斷反覆討論及驗證後才定案。



2. **網路流量分流：**

為因應約 10 **萬考生可能同時上線的可能性，我們規劃一台高階的硬體分流器，同時亦依照考生的準考證號碼進行分流，將約** 10 **萬考生分流到四台選填志願主機中，藉以減少單一主機可能承載過量導致無法服務的情況發生。**

3. **選填志願主機：**

選填志願主機主要用於讓考生暫存志願檔資料，在此主機上的資料考生可任意修改、儲存，待最後確認志願檔內容後，由考生按下確定送出的按鈕才會將志願檔資料寫入到分發主機中。

4. **分發主機：**

分發主機僅接受四台選填志願主機的寫入，同時當志願檔寫入後即無法再行更改，如同傳統作法繳卡後即無法再修改志願資料。

5. **備援主機：**

在架構圖中，選填志願主機、分發主機皆有備援機器可供隨時替換，藉以將硬體故障因素導致無法提供服務的機率及時間減到最低。同時除在成功大學內部準備之外，亦於台南科學園區中設置一備援主機以因應不時之需。

6. **複查主機：**

為維護此次網路選填志願的公正性以及後續分發複查的作業，設置一複查主機，其內的資料皆與分發主機上的完全相同，而此一主機的管理權則由複查組全權負責。

接著則針對前一節中所欲達成的四個目標，詳述我們所做的規劃及相關測試說明。

1. **可用性：**

在網路選填志願的可用性方面除了前述所講減少考生的使用學習時間外，其細項也包括了底下：

(1) **即使遇到突發狀況，必須仍可供考生正常使用；**
(2) **必須有防火牆針對網路選填志願的架構進行防護；**
(3) **網站所能容納的人數必須達到最大，故必須要有足夠的硬體資源可供使用；**
(4) **需有詳盡的權限存取管制措施，藉以確保不致被內部人員隨意存取、洩漏相關志願檔資料。**

為達到上述的第一點，我們除了在成功大學內部異地設置備援主機外，亦在台南科學園區架設一備援主機，當有突發狀況時，確保能夠在四小時以內恢復正常服務運作。第二、四點的部分則於安全性的部分再行說明；第三點的部分，我們所使用的硬體為大型主機系統，每台主機皆有 4 **顆** CPU **及** 4-8G **的記憶體可供使用，另外亦安排了兩種不同的模擬測試，分別是委由中華電信以及高中生進行模擬測試，下表為兩種測試之說明。**

方式	**軟體模擬測試暨** Web AP **測試**	**人員模擬測試**
時間	05/19, 06/10, 07/16	05/25
主機架構	1/4(**註**)	1/4
執行人員	**中華電信協助**	**各高中職生**
實際參與	250 **人版**	9,958 **人**
目標	**測試應用系統是否正常**	**確認系統可靠性**
成果	1. **系統穩定度可再加強並已於測試後調整。** 2. **發現數項缺點需進行改進，且已於測試後完成。**	1. **系統穩定足以負荷** 2. **取得的測試用志願檔案與以往讀卡方式取得的志願檔格式相符。** 3. **聯分會電算組與大考中心就測試取得的志願資料執行分**

		發程式，其模擬分發結果一致，證明目前的分發程式正確無誤。

註：1/4，即只用一台分發主機的資源進行

除了系統的部分之外，我們亦以下列方式進行推廣，以期使考生在使用網路選提志願系統的學習曲線能夠縮到最短，盡快上手使用。

(1) 舉辦推廣教育訓練會；

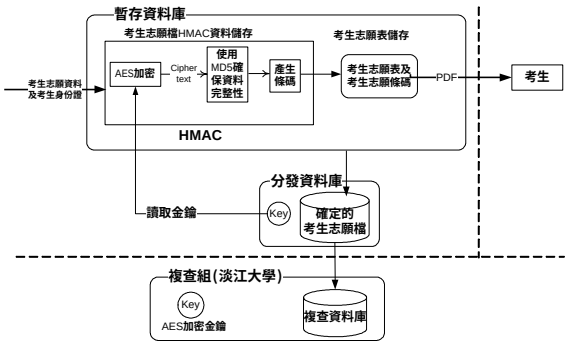
(2) 設計 Q&A 手冊以及設立電話服務諮詢中心；

(3) 製作教學版光碟及及單機版程式，供考生可先行觀看和練習使用。

提供網路選填志願單機版程式目的在於讓考生可在自己的電腦上先行模擬網路選填志願作業及熟悉其流程，單機版程式所產生的志願碼可讓考生在實際進行網路選填志願作業時，於進入系統後直接貼上志願碼，藉以節省考生在網路選填志願系統上操作的時間；但即使考生在網路選填志願系統中直接貼上志願碼後，仍可對志願內容進行檢視、修改，待一切確認無誤後才送出。

另外此次為國內第一次進行網路選填志願故在設計硬體資源、頻寬上均以投入最大資源為原則；以實際監測數據顯示，所規劃之網路架構及設備均足以應付正常使用狀況。以事前擔心的網路塞車問題而言，此次頻寬最大流量僅達 12.4mb，以規劃之頻寬是綽綽有餘。同時此次的過程中亦發現一些有趣的數字，例如有考生反覆登入選填志願網站進行志願檔暫存，直到最後送出志願檔時，共花了 25.6 小時；也有考生進行志願檔暫存的次數達到 366 次。另因是利用網路進行的關係，也發現有部分考生是在國外完成選填志願，可見網路選填志願提供相當大的便利性。

2. 完整性：



為了維持考生志願檔的完整性，我們做了如上圖的規劃；上圖中最主要的一點在於金鑰的產製，加密金鑰的演算法我們是採用 AES-128，同時加密金鑰是由複查組 (淡江大學)產生後，再交由電算組使用。進行網路選填志願時，分發資料庫僅接受選填志願主機的寫入動作，不開放其它使用權限，並僅在選填志願期間上線，其餘時間皆是離線作業。

在完整性規劃中，當考生完成選填志願後，會產生一張 PDF 檔案供考生另行存檔或列印使用，此張 PDF 檔案中的條碼記載了考生的身份資料以及志願檔內容，若考生對於分發結果有所疑問的話，則需以此份文件申請複查。

3. 安全性：

安全性的部分主要區分為實體安全及軟體安全。實體安全的部分網路選填志願使用之主機及相關備援主機皆放置於成功大學機房之內，故已經有一定程度之安全防護，只需確實做好門禁管制禁止閒雜人等進出即可；而在電力設施的部分，亦進行例行檢查，確保用電無虞。

軟體安全的部分我們則做了下列數項的測試及要求：

(1) 防火牆

防火牆的測試過程中我們共使用 150 台個人電腦進行測試，其中 120 台進行攻擊測試並以 40 台為單位，分三次加入攻擊測試過程；其餘 30 台則進行正常連線測試，測試過程中亦僅使用 1/4 的主機資源進行。測試項目著重在下列兩項：

a. 當防火牆遭受 DDoS 攻擊時，防火牆是否能夠快速的過慮掉 Fake IP 連線，允許選填志願主機服務正常連線要求

b. 當防火牆無法提供防護阻擋的功能時，選填志願主機是否能夠承受 DDoS 攻擊

測試結果：

- 在模擬之攻擊規模情況下，防火牆能夠迅速的過濾掉 DDoS 攻擊所產生的 Fake IP 連線，使聯分會系統能夠正常的提供服務。
- 以此次模擬的攻擊來說，DDoS 攻擊期間最多產生一萬多個 Fake IP Sessions 同時建立，在防火牆不提供任何防禦的情況下，選填志願主機仍可正常提供服務。

(2) 選填志願網站與應用程式測試

針對選填志願網站與應用程式的測試部分我們著重在網頁應用程式的前端及使用者介面，規劃出一些項目進行攻擊，以便找出可能的漏洞加以防範。同時也請聯分會電算組提供主機上的檔案清單，協助判斷是否有不必要之檔案存在。進行的測試項目有如下幾項：

a. 應用程式採用的技術或程式語言、套件分析

b. 各類 Buffer Overflow 的可能攻擊與測試

c. HTTP/SSL 的可能攻擊

d. 其它輸入資料驗證的攻擊

e. SQL Injection 和 PHP Injection 測試

f. File Injection

g. 知名 Web 滲透測試工具的使用

測試結果：

經由測試過程發現選填志願主機上具有少數幾個未使用之通訊埠開啟，同時網站上存有部分不需要但具敏感性的資料存在，於發現後立即通知相關人員進行關閉及移除；而在 SQL Injection, PHP Injection, File Injection, HTTP/SSL 以及 Buffer Overflow 等攻擊測試的結果則未發現漏洞。

(3) 選填志願主機資訊收集與分析

針對選填志願主機上的應用程式進行版本弱點和蠕蟲收集，之後由外部網路穿透防火牆嘗試植入蠕蟲於主機上，也針對應用程式弱點進行測試。

測試結果：

在取得選填志願主機相關應用程式、伺服器等資訊後，比對 CERT (Computer Emergency Response Team)所發布的弱點，建議將所使用的應用程式及伺服器版本更新或是安裝所有已發佈的修補程式，以確保應用程式及系統的安全性。

(4) 以網站生命週期觀點提出建議

針對選填志願主機以及分發主機的運作，我們從網站生命週期的角度提出相關建議如下：

a. 主機服務時間

選填志願主機服務時間嚴格限制在 07/21 09:00 至 07/29 24:00 提供服務，其餘時間僅開放首頁內容提供選填志願相關訊息以及重要時間提醒。

b. 防火牆政策制訂

並非安裝防火牆就可保證主機安全性，必須針對提供的服務、服務主機及應用程式特性進行防火牆設定政策的制訂；同時需經反覆驗證才能訂出最佳化之防火牆政策。

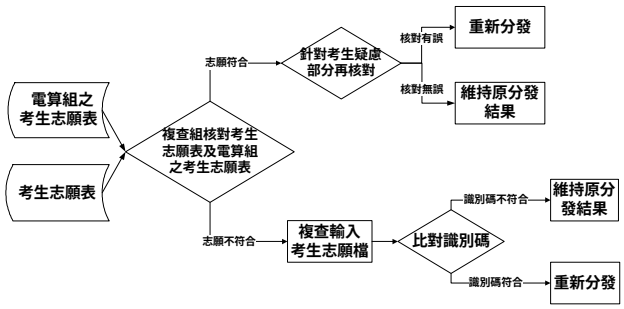
c. 移除不必要之網頁資料或檔案

並非將測試期間所使用的連結移除不顯示在正常使用的頁面即可，而是需將所有測試階段所使用的網頁、檔案等資料全部移至其它離線主機上備份，以避免相關之系統參數、設定外洩。

在網路選填志願的九天當中，根據監測資料顯示雖有遭受零星之網路攻擊行為，但因防火牆策略設定得宜皆已將攻擊阻擋下來，並未影響到正常的服務。而網站應用程式的部分也皆正常運作無誤，使考生能夠順利完成選填志願。

4. 公平性：

為維護網路選填志願的公平性，除了由複查組擔任公正第三者產生加密用金鑰供電算組使用之外，亦設計一詳盡之複查流程遵守，讓考生對分發結果有所疑慮時，能夠依照設計的複查流程進行，藉以維護考生的權益，複查流程如下圖所示。



當考生提出複查時，複查組必須取得考生以及電算組留存之志願表以進行作業，若比對結果相符時，則針對考生有所疑慮的部分進行核對，若核對有誤時則進行重新分發；無誤則維持原分發結果。但若考生的志願表與電算組之志願表內容不符時，則由複查組另行輸入考生送交申請複查的志願表內容，然後再比對識別碼，若結果出來的識別碼不符合，則維持原分發結果；若是符合則進行重新分發。

此次網路選填志願過後，申請複查人數方面較去年(93 年)減少將近一半，僅有 333 人進行複查，而複查結果中並未有因為網路選填志願系統的關係而影響分發結果。

四、結論

經過一整年的籌備規劃，94 學年度的網路選填志願作業已圓滿結束，同時 94 學年度的網路選選填志願作業有下列的優點：

1. 最多可填 100 個有效志願；
2. 考生不用舟車勞頓到服務學校繳卡；
3. 避免劃卡產生錯誤，導致機器判讀有誤；
4. 節省劃卡、繳卡等相關成本。

藉由網路進行選填志願，考生不需要親自到服務學校繳交卡片，只需要在有電腦及網路可使用

的地方即可上網進行選填志願，提供給考生相當大的便利性以及時間效益，這點相信對居住偏遠地區的考生極為便利，而對於解決城鄉數位落差也將有一定之助益，這點可從此次的網路選填作業期間雖有 29 所服務學校提供服務，但使用的人數不多，甚至部分地區九天當中僅有個位數的人數尋求協助，與以往繳卡時各服務學校大排長龍的景象相差甚多。

希望能夠藉由這樣良好的模式，增加我國網路使用者的信心，讓政府或企業單位能將更多的服務夠過網路進行，早日使我國不僅只在資訊硬體產業執全球牛耳，在網路服務應用方面亦能成為領先者。

最後，此次網路選填志願能夠圓滿結束，主要必須感謝教育部高教司、電算中心的全力支持，聯分會分發組在行政方面的大力配合，協助教育訓練以及電話諮詢中心的設置，而整個工作團隊的互相配合更是此次網路選填志願作業能夠圓滿達成的核心。另外，密碼與網路安全實驗室的資安團隊(林敬皇、鄭毓芹、陳威宇)在資訊安全防護上所投入的心力亦為此次的網路選填志願作業提供最佳的安全保證，不致使此次作業成為一資安事件範例。”

五、參考文獻

[1] 鄭毓芹、陳威宇、林敬皇，“聯分會系統測試報告”, 2005 年 7 月

[2] 林敬皇、賴溪松，“透過網站生命週期促進網站的安全”, pp.134-138, RUN! PC 2004 年 7 月號

[3] 賴溪松主編，“資通安全專輯之十四-網路攻防實驗教材”，財團法人國家實驗研究院科技政策研究與資訊中心，2005 年 6 月

[4] 郭建邦 賴溪松，“網站壓力測試計畫書”, 2005 年 4 月

[5] 郭建邦 賴溪松，“網站壓力測試報告書”, 2005 年 7 月

[6] 聯合分發委員會，“九十四學年度大學考試分發入學登記分發相關資訊”, 2005 年 5 月

[7] 聯合分發委員會電算組，“聯合分發委員會標準作業程序-電算組”, 2005 年 8 月

[8] Computer Emergency Response Team, http://www.cert.org

[9] SecuriTeam , http://www.securiteam.com/

[10] SecurityFocus, http://www.securityfocus.com/