教育部國民及學前教育署
114 年度滲透測試服務案
滲透測試服務報告-第二階段
技術型高中產學鏈結平台_114

文件編號：H07S11403112_1_114

V1.0 版

114 年 7 月 23 日

安碁資訊股份有限公司

文件制／修訂記錄

版次	日期	說明	作者	修訂中	定稿
1.0	114.7.23	定稿	游府鑫		V

【目　　錄】

【圖 目 錄】

【表 目 錄】

壹、 關於本報告

一、 報告說明

滲透測試（Penetration Test）是以駭客思維與手法進行的入侵演練測試。本報告為安碁資訊股份有限公司承接教育部國民及學前教育署（下稱貴公司）「114 年度滲透測試服務案」（以下稱本案），依貴我雙方約定之作業範圍，在取得最少資訊的情況下，嘗試突破網路或系統的防禦、尋找應用軟體及網路服務等系統設備之安全弱點與漏洞，並設法取得控制權限或未授權之機敏資訊，以評估企業之整體安全性後，就本次作業所見之項目進行說明陳述，提供相關優化、精進之資安防護機制之建議，供貴公司做為後續防護規劃之依循參考。

二、 盡責聲明

滲透測試為在一定的時間內，使用不同手法盡可能確認測試標的的安全性，並非以找出全部的系統漏洞為目標。當攻擊者的攻擊時程較長、或是測試標的更新、或是有了全新的攻擊手法出現，都會使得系統或網站的安全性降低。唯有透過定期進行滲透測試，才能確保系統與網站的安全性足夠抵禦外來的惡意攻擊。

本報告所使用之分析與檢測手法，為當前資訊安全產業所通用之技術與工具，本公司謹盡合理可能之最大努力，就所見所聞如實提出本報告，容或有不足之處，仍請考量當前科技所能達成之極限，予以諒解。

貳、 執行計畫摘要

一、 執行期間

滲透測試時間自民國 114 年 05 月 01 日至民國 114 年 07 月 21 日止。在執行階段，除了貴單位提出特別排除的測試時間限制之外，原則上一天 24 小時任何時段均可進行，每天 2 人進行 8 小時為原則。

二、 執行項目

參考 OSSTMM（Open-Source Security Testing Methodology Manual）建立執行架構，共分為三個步驟：資料蒐集、資訊分析及標的滲透，並以 OWASP（Open Web Application Security Project）之弱點分類做為主要測試標準，但仍會依情況所需，適當地採用不同的弱點滲透。同時因為「應用程式滲透測試」與「系統、網路滲透測試」兩者在執行時性質不同，故在執行階段即將「應用程式」及「系統、網路」分開考慮，分別以不同方式進行。

滲透測試的進行是個迭代的過程，在蒐集資料後，滲透測試團隊依其經驗分析資訊，推演可能之結果，再針對問題進行滲透，並逐步深入網路或系統。

（一） 資料蒐集

透過工具或以人工手動的方式蒐集有關滲透範圍的資訊。

- 網路資訊：滲透測試範圍內與網路相關的資訊，如網路名稱（Domain Name）、路由（Routing）等資訊。
- 系統資訊：滲透測試範圍內與主機、系統相關的資訊，如作業系統（OS）、版本、使用者、通訊埠（Ports）。
- 服務資訊：滲透測試範圍內屬於應用程式相關的資訊，如通訊埠對應的執行程式、版本。

- 安全資訊：滲透測試範圍內可能的安全漏洞。由於目前許多單位主要的對外服務皆是以網頁應用程式為主，因此將著重於應用程式的安全漏洞測試。
- 其他資訊：其他與測試範圍相關的資訊，如 Google 上所取得與滲透測試範圍相關的資訊。

（二） 資訊分析

分析蒐集的資料，藉以研判可能問題、規劃滲透路徑，並據以建立滲透情境。

- 資料整理：判斷已蒐集之資料的重要性，將具有價值的資料整理出來，並確認弱點是否可以利用。
- 弱點分析：依據可利用之弱點推演滲透過程可能的情況，了解可使用之手法及相關之滲透工具。
- 情境規劃：依團隊人員專長之不同，排定負責的滲透路徑及擬定滲透計劃，建立滲透測試模擬情境。

（三） 標的滲透

依據滲透情境，決定使用特定之攻擊程式（Exploits）或手工執行之攻擊手法來進行模擬攻擊，並視情況修改網頁系統進行驗證、或植入無害之後門程式，並於證據收集完畢之後刪除程式或告知路徑。若成功取得權限或弱點利用方式，則會進一步深入或擴大攻擊，並依獲得的新資訊更新滲透手法。

（四） 系統滲透測試內容

表1　系統滲透測試內容

測試類型	測試類別	測試項目
作業系統	遠端服務	至少包含遠端服務套件弱點測試等項目
	本機服務	在已取得系統控制權限的條件下，可執行至少包含本機服務套件弱點測試等項目
網站服務應用程式	設定管理	至少包含應用程式設定測試、檔案類型處理測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項目
	使用者認證	至少包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目
	連線管理	至少包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試、Session 變數傳遞測試及 CSRF 測試等項目
	使用者授權	至少包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目
	邏輯漏洞	至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	輸入驗證	至少包含 XSS 漏洞測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSI Injection 測試、XPath Injection 測試、Code Injection、OS Commanding 測試及偽造 HTTP 協定測試等項目
	Web Service	至少包含 WSDL 測試、XML 架構測試、XML 內容測試及 XML 參數傳遞測試等項目
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目
應用程式密碼破解	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	電子郵件服務套件	至少包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	檔案傳檔服務套件	至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試

測試類型	測試類別	測試項目
		項目
	遠端連線服務套件	至少包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	網路服務套件	至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	其他	包含 Firewall、IDS/IPS、Database、LDAP、SMB、LPD、IPP、Jetdirect 及 RTSP 等常見應用程式或網路套件之弱點掃描項目
密碼破解	密碼強度測試	至少包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試

三、 執行範圍

滲透測試標的為貴單位所提供如下之標的詳細列表，測試範圍包含其標的下同網域之相關鏈結。

表2　滲透測試標的列表

編號	標的	名稱
1	https://database.k12ea.gov.tw/	技術型高中產學鏈結平台

四、 專案人員

由安碁資訊資安滲透服務部門及資安檢測服務部之同仁為主要執行人員，執行滲透測試或是出席報告會議。

參、 執行結果摘要說明

本次滲透測試結果摘要如下圖。基本上風險現象的嚴重等級分為嚴重、高、中、低等四級。其定義如下（此乃業界一般共通之定義準則）：

- 嚴重：具有可被立即入侵、服務中斷或機密資料洩漏的風險
- 高　：可能具有被入侵、服務中斷或機密資料洩漏的風險
- 中　：具有可輔佐或間接用於入侵之風險，或洩漏資料之等級不高
- 低　：潛在威脅，未來可能提升為中高風險

測試過程中，若有發現威脅性極低、或是不具有威脅性（例如：程式設計建議等）的項目，會以「一般資訊」的形式列出，作為參考資訊。

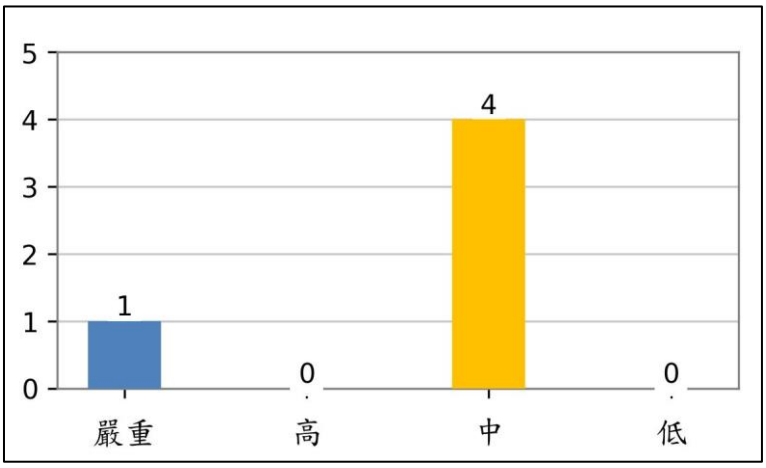

圖1　各種風險等級數量統計

一、 受測標的風險等級與數量列表

依受測標的為序，表列包含所有風險等級及其漏洞數量。如表 3 所示。

表3　受測標的風險等級與數量列表

編號	標的	風險等級	漏洞數量
1	https://database.k12ea.gov.tw/	嚴重	1
		高度	0
		中度	4
		低度	0

二、 受測標的風險漏洞名稱列表

依受測標的為序，表列包含所有漏洞名稱、漏洞數量及風險等級。如表 4 所示。

表4　受測標的風險漏洞名稱列表

編號	標的	漏洞名稱	漏洞數量	風險等級	風險現象
1	https://database.k12ea.gov.tw/	不完整的存取控管	1	嚴重	攻擊者可以提權操作網站功能
		網頁回傳過多訊息	1	中	攻擊者有可能取得系統的重要資訊
		上傳檔案格式未妥善驗證	1	中	攻擊者可上傳 Webshell，嘗試取得權限
		錯誤訊息非客製化結果而夾帶太多技術訊息	1	中	網頁回傳過多後端錯誤技術資訊
		Robots.txt 網站結構曝光	1	中	可透過 Robots.txt 得知網站架構資訊

三、 風險漏洞分布列表

依漏洞名稱為序，表列包含所有漏洞數量、安全等級及受影響系統。如表 5 所示。

表5　受測標的風險漏洞分布列表

編號	漏洞名稱	漏洞數量	安全等級	受影響系統
1	不完整的存取控管	1	嚴重	https://database.k12ea.gov.tw/
2	網頁回傳過多訊息	1	中	https://database.k12ea.gov.tw/
3	上傳檔案格式未妥善驗證	1	中	https://database.k12ea.gov.tw/
4	錯誤訊息非客製化結果而夾帶太多技術訊息	1	中	https://database.k12ea.gov.tw/
5	Robots.txt 網站結構曝光	1	中	https://database.k12ea.gov.tw/

肆、 滲透測試弱點發現與改善建議

一、 檢測目標：https://database.k12ea.gov.tw/

（一） 弱點名稱：不完整的存取控管

- 問題 URL 或 IP：
  - https://database.k12ea.gov.tw/nss/site/main/saveemail
- 問題參數：
  - _id
  - email
- 測試語法：無
- IP 或網域名稱：database.k12ea.gov.tw
- 風險等級：嚴重
- CVE 編號：無
- 弱點分類：使用者授權
- 弱點說明：網站開發者於處理程式功能時，應更加嚴格的驗證身分權限，避免攻擊者利用漏洞存取未經授權的功能，或更改使用者權限。
- 修補建議：建議徹查網站，將頁面設定妥善權限。詳細修補建議請參考附件。
- 檢測說明：檢測發現，於「權限」功能頁面中的個人資料管理進行修改通訊信箱，使用代理伺服器攔截後即可將 id 及信箱修改成其他使用者的信箱資訊，這些資訊可從進階管理頁面中的權限設定查看到其他使用者的 id 及 mail 等詳細資訊，最後再於忘記密碼功能將其他使用者的帳號寄出至修改後的信箱，進一步修改其他使用者的密碼。
- 檢測畫面與測試截圖：（續下頁）

圖2　權限功能頁面-1

圖3　修改功能發現包含使用者參數-2

圖4　進階管理頁面查詢功能-3

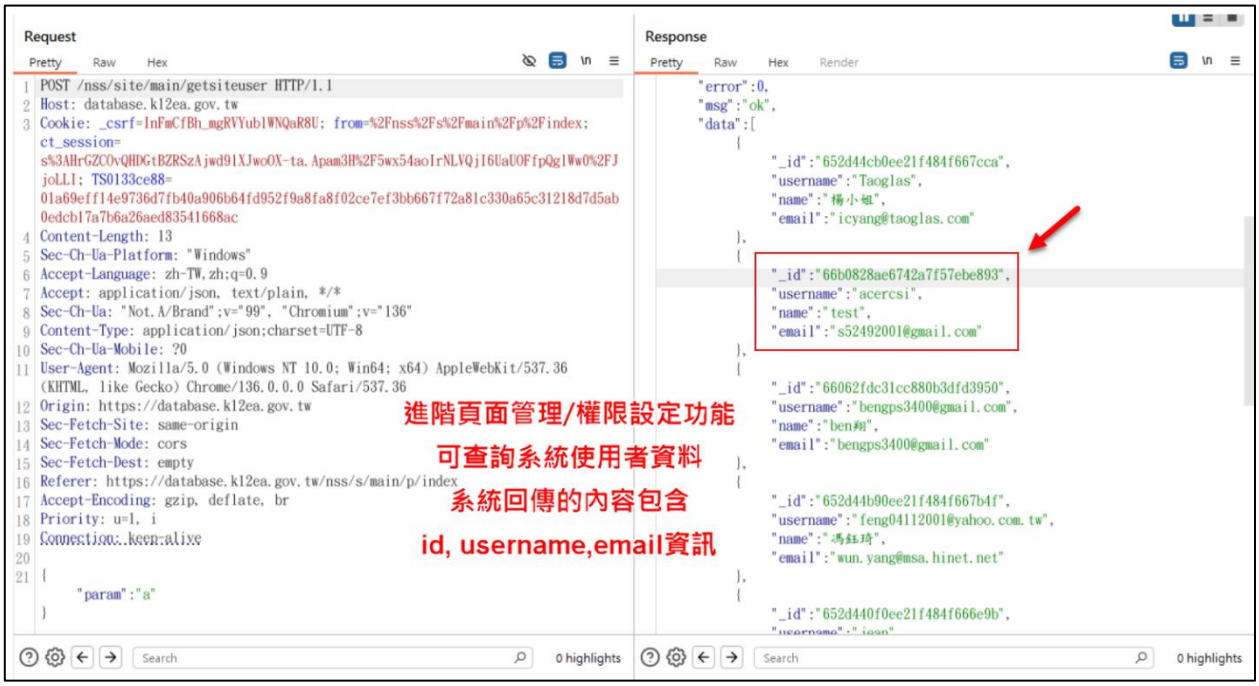

圖5　可查詢其他使用者詳細資料-4

圖6　回到權限功能頁面-5

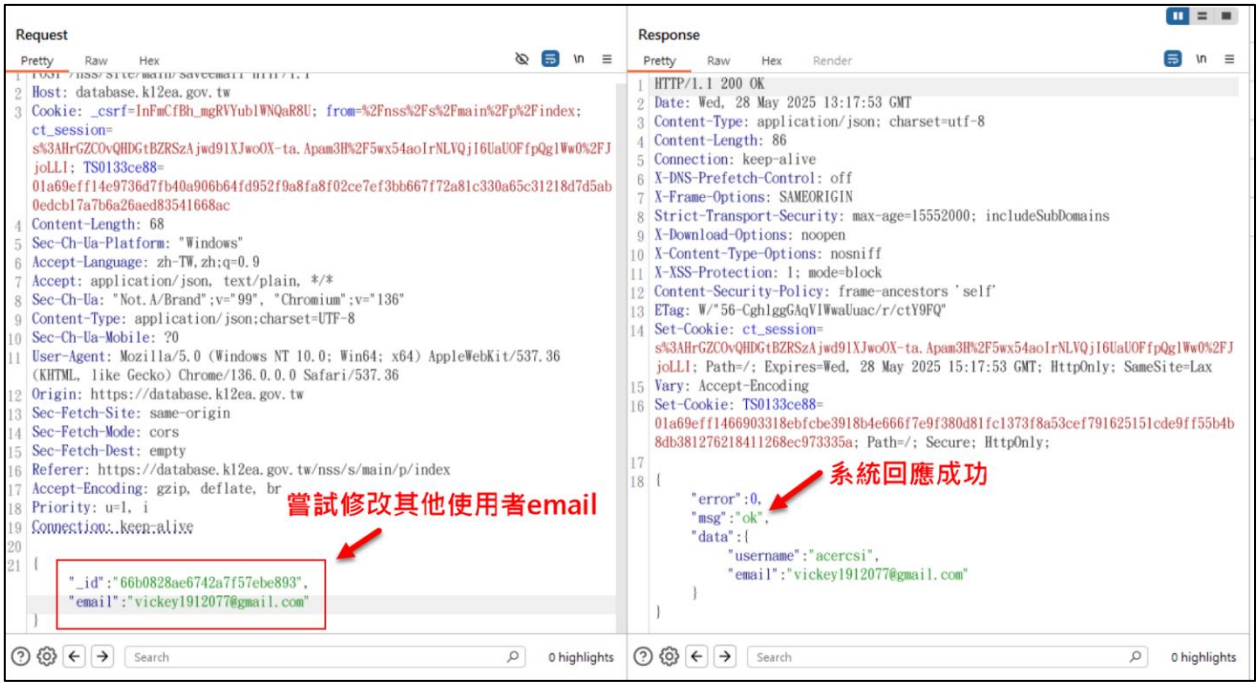

圖7　成功修改其他使用者參數-6

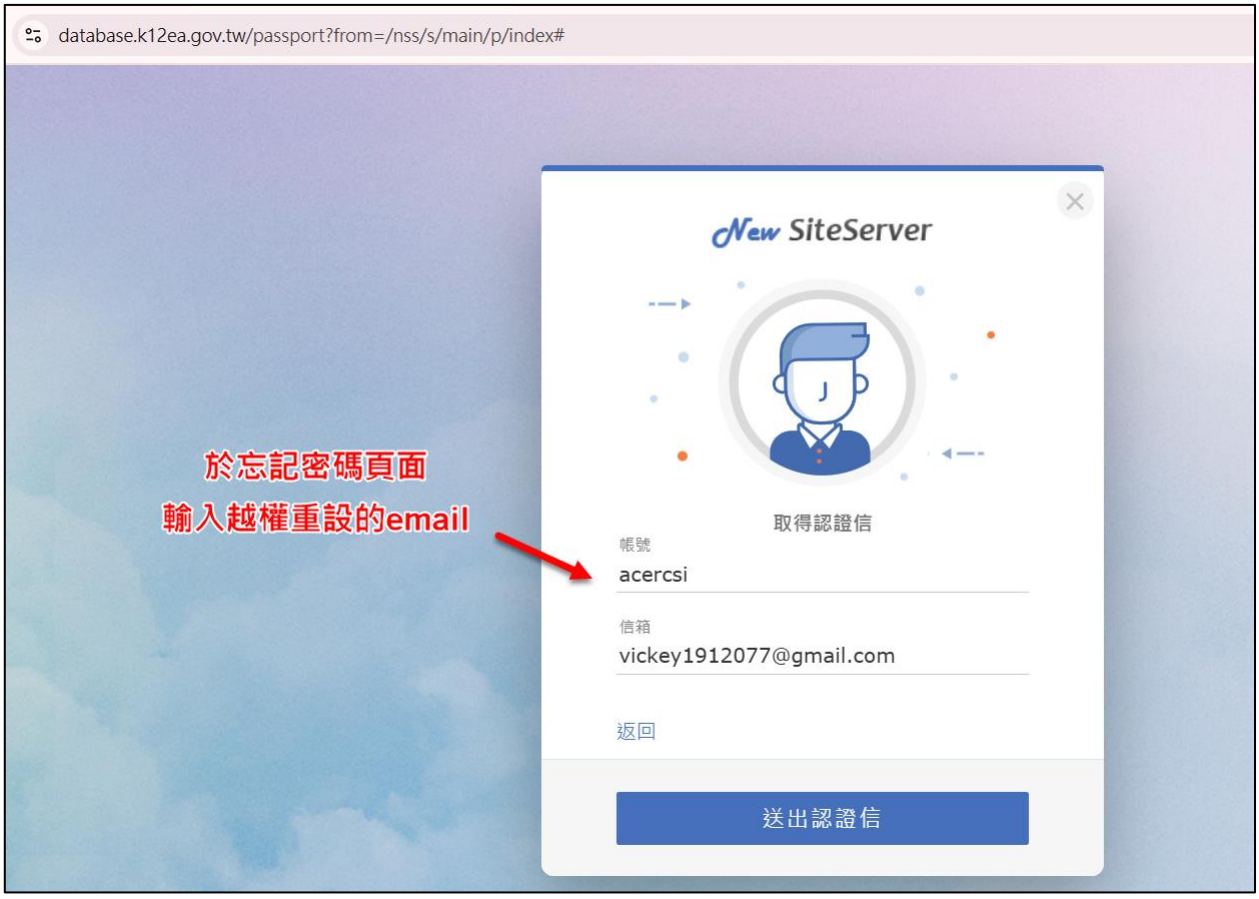

圖8　忘記密碼功能輸入重設資訊-7

（二） 弱點名稱：網頁回傳過多訊息

- 問題 URL 或 IP：
  - https://database.k12ea.gov.tw/nss/site/main/getsiteuser
- 問題參數：
  - _id
  - username
  - name
  - email
- 測試語法：無
- IP 或網域名稱：database.k12ea.gov.tw
- 風險等級：中
- CVE 編號：無
- 弱點分類：使用者授權
- 弱點說明：網頁回傳值內容包含太多技術訊息或機敏資訊，例如：伺服器內部實體路徑、SQL 語法、身分證字號等。攻擊者可以藉由獲取這些資訊，推測與了解後端所使用的網頁技術或得到機敏資訊。
- 修補建議：伺服器只應回傳必要資訊，避免回傳過多包含機敏資訊之回應。詳細修補建議請參考附件。
- 檢測說明：檢測發現使用進階資料查詢功能，可看到網頁回應過於詳細的使用者資訊。
- 檢測畫面與測試截圖：（續下頁）

圖9　進階管理頁面查詢使用者-1

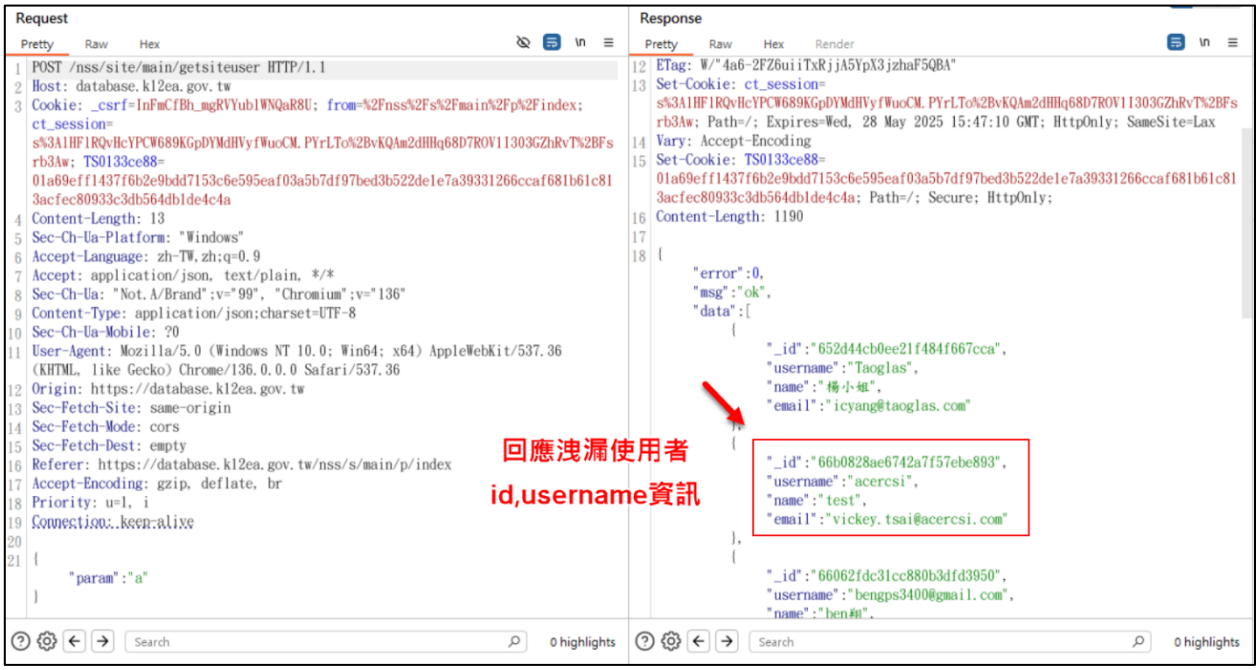

圖10　查詢回應過多使用者資訊-2

（三） 弱點名稱：上傳檔案格式未妥善驗證

- 問題 URL 或 IP：
  - https://database.k12ea.gov.tw/nss/ext/upfile
- 問題參數：上傳檔案功能
- 測試語法：無
- IP 或網域名稱：database.k12ea.gov.tw
- 風險等級：中
- CVE 編號：無
- 弱點分類：邏輯漏洞
- 弱點說明：網頁允許使用者上傳資料，但並未妥善針對檔案格式（副檔名）進行限制或驗證，使攻擊者可以直接上傳惡意程式或網頁木馬，或是透過代理伺服器繞過前端限制，進而取得網站權限。
- 修補建議：建議詳細驗證上傳檔案格式。詳細修補建議請參考附件。
- 檢測說明：檢測發現，弱點頁面並未於前端針對上傳檔案格式做限制，可成功上傳較具風險之檔案格式。
- 檢測畫面與測試截圖：（續下頁）

圖11　上傳檔案格式未限制-1

圖12　成功上傳較具風險之檔案格式-2

（四） 弱點名稱：錯誤訊息非客製化結果而夾帶太多技術訊息

- 問題 URL 或 IP：
  - https://database.k12ea.gov.tw/nss/main/feeder/5a9759adef37531ea27bf1b0/UcWBxIZ7223?f=normal&vector=private&static=false
- 問題參數：無
- 測試語法：無
- IP 或網域名稱：database.k12ea.gov.tw
- 風險等級：中
- CVE 編號：無
- 弱點分類：設定管理
- 弱點說明：當對網站進行某些不當操作時，網路應用系統可能會將許多底層 API 顯示的錯誤資訊，未經解讀與妥善翻譯，直接傳送到前端讓使用者閱讀，例如：完整或部分路徑、變數與檔名、表格中的資料行與資料欄名稱等。攻擊者可以藉由獲取這些技術細節，推測與了解後端所使用的網頁技術或得到機敏資訊。
- 修補建議：網頁錯誤訊息若不必要，建議不用給一般使用者看。詳細修補建議請參考附件。
- 檢測說明：本次檢測，輸入以下網址，系統即回傳錯誤訊息，其中包含過多技術細節。
- 檢測畫面與測試截圖：（續下頁）

圖13　錯誤訊息含太多技術細節

（五） 弱點名稱：Robots.txt 網站結構曝光

- 問題 URL 或 IP：
  - https://database.k12ea.gov.tw/robots.txt
- 問題參數：Disallow: /admin
- 測試語法：無
- IP 或網域名稱：database.k12ea.gov.tw
- 風險等級：中
- CVE 編號：無
- 弱點分類：設定管理
- 弱點說明：Web Robots 是搜尋引擎在編製網站索引時，自動遍訪網站的程式。Robots.txt 為網站管理者指示 Robot 不應造訪哪些部分的方法。

  當 Robot 試圖存取網站時，會先搜尋該網站的 Robots.txt（例如：www.site.com/robots.txt），如果找到這份文件，便會分析它的記錄內容，以便確認是否允許它擷取文件。由於所有 Web 使用者都能存取 Robots.txt，因此，不應利用它來隱藏 Web 伺服器上的檔案或目錄。
- 修補建議：Robots.txt 不應用來保護或隱藏資訊，建議使用正面表列。詳細修補建議請參考附件。
- 檢測說明：檢測發現禁止攀爬的網站目錄。
- 檢測畫面與測試截圖：

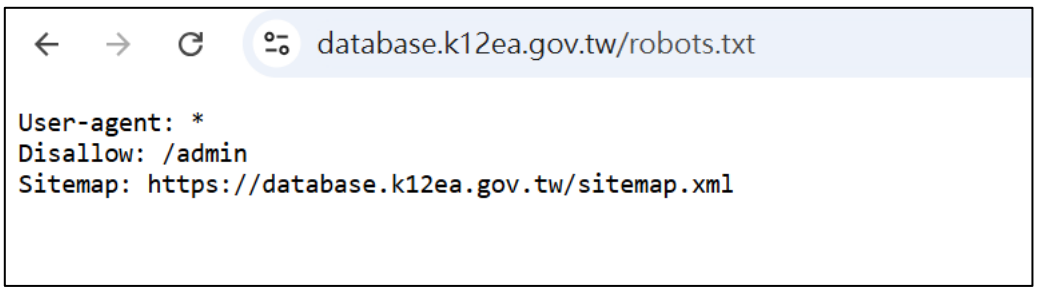

圖14　Robots.txt 網站結構曝光

伍、 結論

本次滲透測試共發現 1 個嚴重風險及 4 個中風險弱點。建議徹查網站，將頁面設定妥善權限。伺服器只應回傳必要資訊，避免回傳過多包含機敏資訊之回應。建議設計安全的文件上傳功能，應於後端伺服器檢查檔案格式。網頁錯誤訊息若不必要，建議不用給一般使用者看。Robots.txt 不應用來保護或隱藏資訊，建議使用正面表列。若貴單位網站仍有修改更新時，須持續自我檢查，注意是否有可能產生的新漏洞。

陸、 附件

一、 Robots.txt 網站結構曝光

（一） 弱點說明

Web Robots 是搜尋引擎在編製網站索引時，自動遍訪網站的程式。Robots.txt 為網站管理者指示 Robot 不應造訪哪些部分的方法。

當 Robot 試圖存取網站時，會先搜尋該網站的 Robots.txt（例如：www.site.com/robots.txt），如果找到這份文件，便會分析它的記錄內容，以便確認是否允許它擷取文件。由於所有 Web 使用者都能存取 Robots.txt，若用來保護或隱藏資訊，只會將原本隱藏的目錄情報公開，讓攻擊者取得資訊，因此，不應利用它來隱藏 Web 伺服器上的檔案或目錄。

（二） 修補建議

Robot.txt 應採用正面表列的方式（先允許可存取的，再禁止所有的）進行設定，範例如下：

```
User-Agent:*
Allow: /user/
Allow: /report/
Allow: /sales/
Disallow:/
```

二、 上傳檔案格式未妥善驗證

（一） 弱點說明

網頁允許使用者上傳資料，但並未妥善針對檔案格式（副檔名）進行限制或驗證，使攻擊者可以直接上傳惡意程式或網頁木馬，或是透過代理伺服器繞過前端限制，進而取得網站權限。

（二） 修補建議

應設計安全的文件上傳功能，詳細的設置建議如下：

1. 保存上傳檔的目錄，設置為不可執行（重要設置）
   只要 Web 伺服器無法解析該目錄下的檔，即使攻擊者上傳了指令檔，伺服器本身也不會受到影響。

2. 判斷檔案類型
   在判斷檔案類型時，可以結合使用 MIME-Type、尾碼檢查等方式。檔案類型檢查時，強烈建議採用白名單的方式。此外，若上傳的檔案為圖片，可使用壓縮方式破壞圖片結構，如此一來，在處理圖片的同時亦可破壞圖片中可能包含的惡意程式碼。

3. 使用亂數改寫檔案名稱、副檔名、以及存放路徑
   攻擊者要執行代碼，需將檔案上傳後訪問檔案路徑，若採用亂數改寫檔名和路徑，將極大地增加攻擊成本。與此同時，像 webshell.asp;1.jpg 這種惡意程式，將因檔名被改寫而無法成功實施攻擊。

三、 不完整的存取控管

（一） 弱點說明

網站開發者於處理程式功能時，應更加嚴格的驗證身分權限，避免攻擊者利用漏洞存取未經授權的功能，或更改使用者權限。

常見的存取控制缺失問題如下：

1. 未登入的使用者可使用登入後之功能

   未經授權的使用者存取登入後的功能頁面，即可使用該網頁之功能，讓使用者任意查看他人隱私或是存取檔案，可能導致資訊遭竊、功能遭濫用。

   以下範例中，應用程式在存取帳號訊息的 SQL 語法中，並未驗證欄位資料：

```
pstmt.setString（1, request.getParameter（"acct"））;
ResultSet results = pstmt.executeQuery（ ）;
```

   攻擊者僅需在瀏覽器中修改 acct 欄位之數值，即可要求網站回應相關帳號訊息：

```
http://example.com/app/accountInfo?acct=notmyacct
```

   若伺服器於後端未正確驗證該數值資料，則攻擊者可以存取任意帳號資料。

2. 低權限使用者可執行高權限功能

   已登入之低權限使用者，若得知管理功能完整網址或 API 路徑，即可直接發送要求到後端。

   以下範例中，攻擊者強制瀏覽管理功能目標 URL，該 URL 需管理者權限存取：

http://example.com/app/getappInfo （已登入使用者才可存取）
http://example.com/app/admin_getappInfo （管理者才可存取）

若未獲授權使用者可存取以上任一功能，或一般使用者可存取管理功能（admin_getappinfo），則此網站含有設計瑕疵。

3. 使用者可新增、刪除、查詢、修改其他使用者之資料
已登入的使用者修改基本資料時，嘗試修改他人資料，但伺服器並未驗證該組 Session 是否正確，則可以修改其他使用者之個人資料。

（二） 修補建議

針對網站環境中的權限控管相關設定，進行妥善的了解與設定調整。讓使用者無法直接瀏覽、存取未獲授權的頁面，只能透過網頁所設計的權限與流程讀取應得的資訊。當使用者嘗試修改個人資料時，應確認是否有權限修改該筆資料，避免使用者修改其他使用者之資料。

針對以上幾點問題，建議徹查網站，將頁面設定妥善權限，不應給非授權人員存取瀏覽，或使用該功能：

1. 確認使用者是否已登入
2. 確認使用者是否具備此功能之操作權限
3. 確認使用者是否有權限修改他人資料

四、 錯誤訊息非客製化結果而夾帶太多技術訊息

（一） 弱點說明

當對網站進行某些不當操作時，網路應用系統可能會將許多底層 API 顯示的錯誤資訊，未經解讀與妥善翻譯，直接傳送到前端讓使用者閱讀，例如：完整或部分路徑、變數與檔名、表格中的資料行與資料欄名稱等。攻擊者可以藉由獲取這些技術細節，推測與了解後端所使用的網頁技術或得到機敏資訊。

（二） 修補建議

詳細的系統技術性錯誤訊息，主要為提供程式設計人員除錯或測試用，不應直接呈現在網頁上供一般使用者存取。呈現給使用者的錯誤訊息，應是能了解操作錯誤的原因、或判斷邏輯錯誤等客製化訊息。

此弱點建議用以下方式進行全面性修補，而非僅針對特定頁面進行移除或權限設定，以確保攻擊者無法引導錯誤訊息顯示重要的資訊：

1. 技術性的錯誤訊息建議存入後端主機的記錄檔（Log File）或資料庫中。完整或部分路徑、變數與檔名、表格中的資料行與資料欄名稱，以及特定的資料庫錯誤，永遠不得顯示與透露。
2. 應針對網頁與欄位所輸入之字串進行驗證與過濾，避免系統出現錯誤資訊。
3. 系統錯誤所回傳之網頁，應導向首頁，或客製化的錯誤頁面。網頁標頭也應由原本 HTTP 500（內部伺服器錯誤）調整成 HTTP 200（正常回應），以混淆攻擊者的判斷。

以下為常見程式語言或 Framework 關閉錯誤訊息之方式，除此之外，應確保所有功能都進行錯誤及例外處理。

1. IIS

   建議可於 IIS 站台中自訂 HTTP 錯誤回應，不將伺服器內部路徑甚或是 SQL 錯誤訊息呈現給使用者看。

   詳細設置方式請參考：

   https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731570(v=ws.10)?redirectedfrom=MSDN

2. PHP

   將 php.ini 的 display_errors 參數設定為 off，以避免整個網站都有機會顯示錯誤訊息，範例如下：

```
<?php
ini_set('display_errors','off');      # 關閉錯誤輸出
# ini_set('display_errors','on');       # 開啟錯誤輸出（若有需要可加入這行）
 error_reporting(E_ALL & ~E_NOTICE)   # 設定輸出錯誤類型
?>
```

   詳細設置方式請參考：

   https://www.php.net/manual/en/errorfunc.configuration.php

   https://www.opencli.com/php/php-enable-disable-error-reporting

3. ASP.NET

   修改 Web.config，建議設定 customerrors mode 為 RemoteOnly 或 on，範例如下：

```
<configuration>
    <system.web>
        <customErrors mode="RemoteOnly"
```

```
defaultRedirect="Error.htm">
            <error statusCode="500" redirect="Error.htm"/>
        </customErrors>
    </system.web>
</configuration>
```

詳細設置方式請參考：

https://docs.microsoft.com/zh-tw/previous-versions/dotnet/netframework-3.0/h0hfz6fc(v=vs.85)?redirectedfrom=MSDN

4. Java

將 server.xml 的 showReport 及 showServerInfo 參數設定為 false，範例如下：

```
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false" showServerInfo="false"/>
```

詳細設置方式請參考：

https://tomcat.apache.org/tomcat-7.0-doc/config/valve.html

五、 網頁回傳過多訊息

（一） 弱點說明

網頁回傳值內容包含太多技術訊息或機敏資訊，例如：伺服器內部實體路徑、SQL 語法、身分證字號等。攻擊者可以藉由獲取這些資訊，推測與了解後端所使用的網頁技術或得到機敏資訊。

（二） 修補建議

伺服器只需回傳必要資訊，應避免回傳過多包含機敏或技術資訊之回應。