110年網路攻防演練暨資安技術檢測重要發現事項

行政院國家資通安全會報技術服務中心

110年12月

大綱

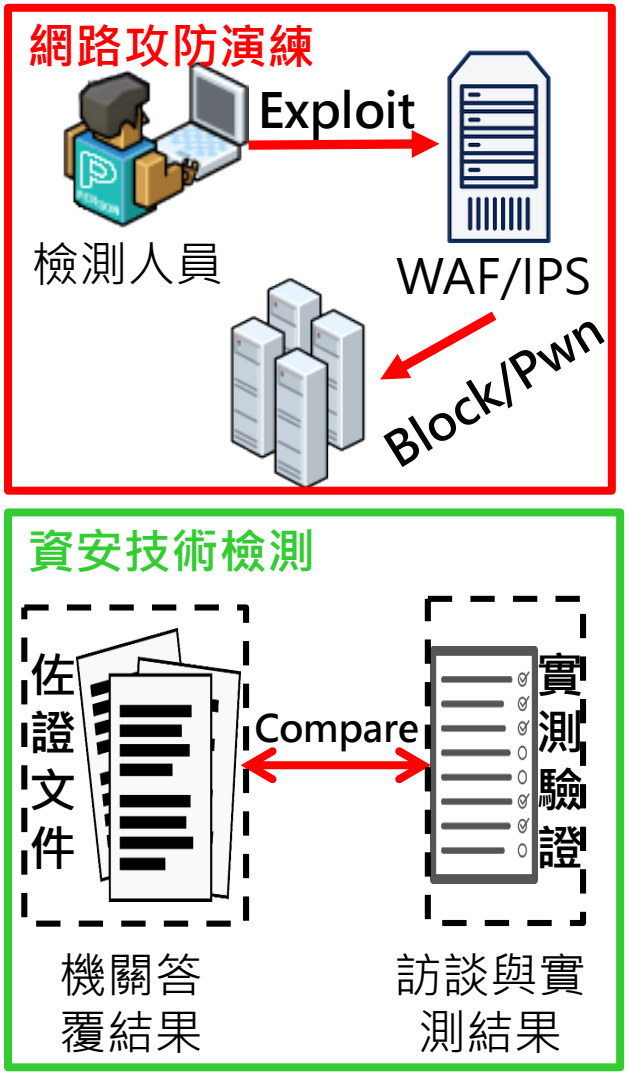
- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

大綱

- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

前言

- 技服中心透過網路攻防演練與資安技術檢測，驗證政府機關資安防護成效
  - 網路攻防演練：遠端模擬駭客入侵手法，檢測政府機關與所轄對外系統之資安防護，強化政府機關在資安事件發生時之緊急應變、系統復原及協調管控等能力
  - 資安技術檢測：透過現場訪談與實測，檢視政府機關資安防護措施落實程度，110年檢測項目包含使用者電腦安全檢測、網路惡意活動檢視及核心資通系統安全檢測等8項防護作為



大綱

- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

網路攻防演練弱點類型分布

- 綜整110年網路攻防演練攻擊紀錄，其中無效的身分認證與無效的存取控管比例最高

排名	109年
1	不安全的組態設定(0.48)
2	無效的身分認證(0.26)
3	無效的存取控管(0.10)
4	跨網站腳本攻擊(0.09)
5	注入攻擊(0.04)
6	機敏資料外洩(0.02)
7	使用已知漏洞元件(0.01)

排名	110年
1	無效的身分認證(0.49)
2	無效的存取控管(0.21)
3	不安全的組態設定(0.19)
4	跨網站腳本攻擊(0.08)
5	注入攻擊(0.02)
6	使用已知漏洞元件(0.01)
7	機敏資料外洩(0.00)

網路攻防演練綜合發現

- 歸納上述弱點類型，可彙整為下列6項根因，建議參考下列7個案例，清查機關潛在弱點

項次	弱點類型	發現事項	案例
1	無效的身分認證	**未落實通行碼強度檢查機制***	案例1
2	無效的存取控管	參數猜測	案例2-1 案例2-2
3	無效的存取控管	**資料庫未限制存取來源***	案例3
4	無效的存取控管	**不當的轉導設計***	案例4
5	跨網站腳本攻擊	跨網站腳本攻擊	案例5
6	注入攻擊	注入漏洞	案例6

*註：與109年攻防演練發現事項相同

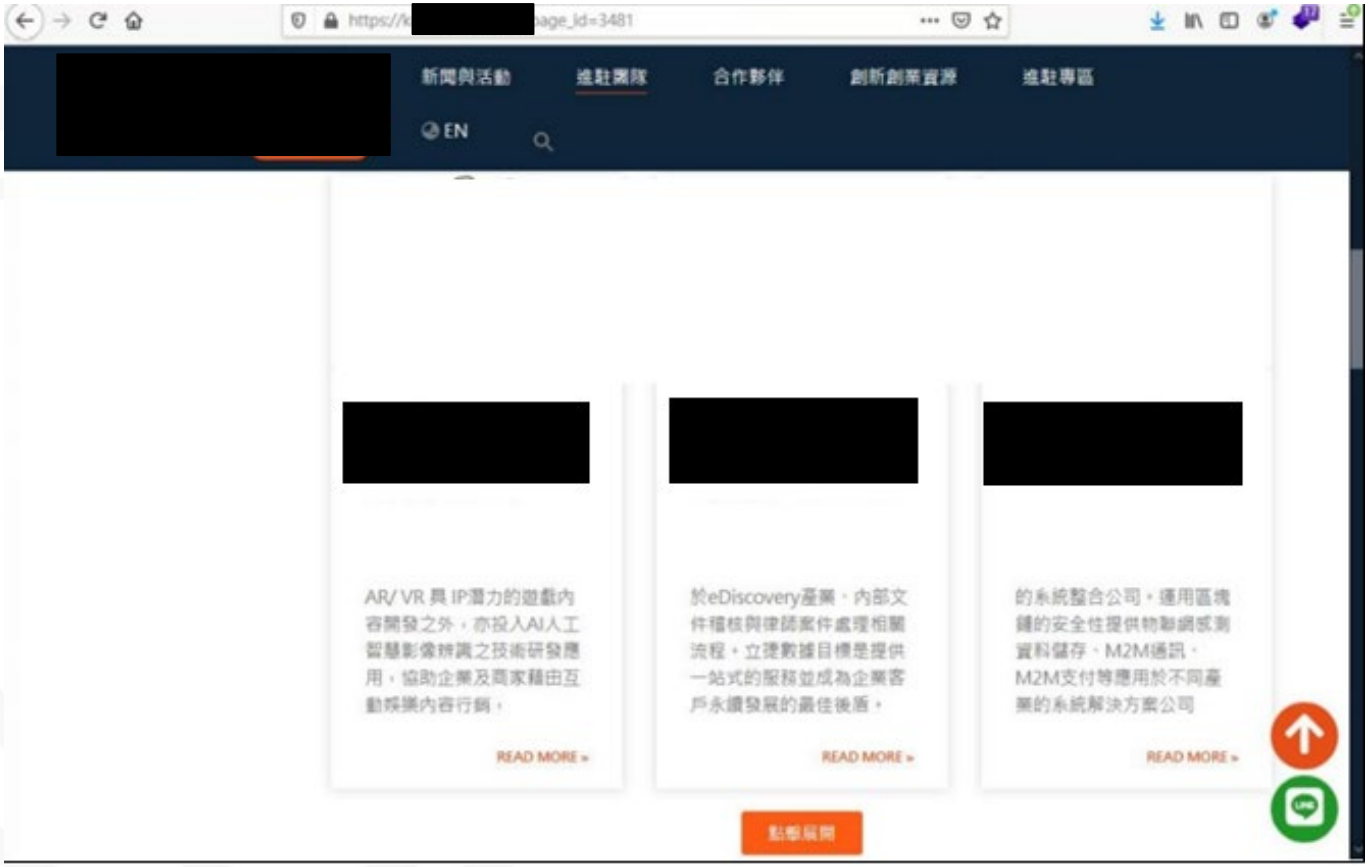
1.未落實通行碼強度檢查機制

未落實通行碼強度檢查機制樣態

- 機關未強化通行碼設定原則
- 使用通行碼內容含公開資訊，易被攻擊者利用拼接方式猜測成功
- 利用帳號與通行碼相同手法入侵系統複雜度極低，但影響範圍輕取得一般同仁權限，重則導致暴露內部往來信件或取得系統權限

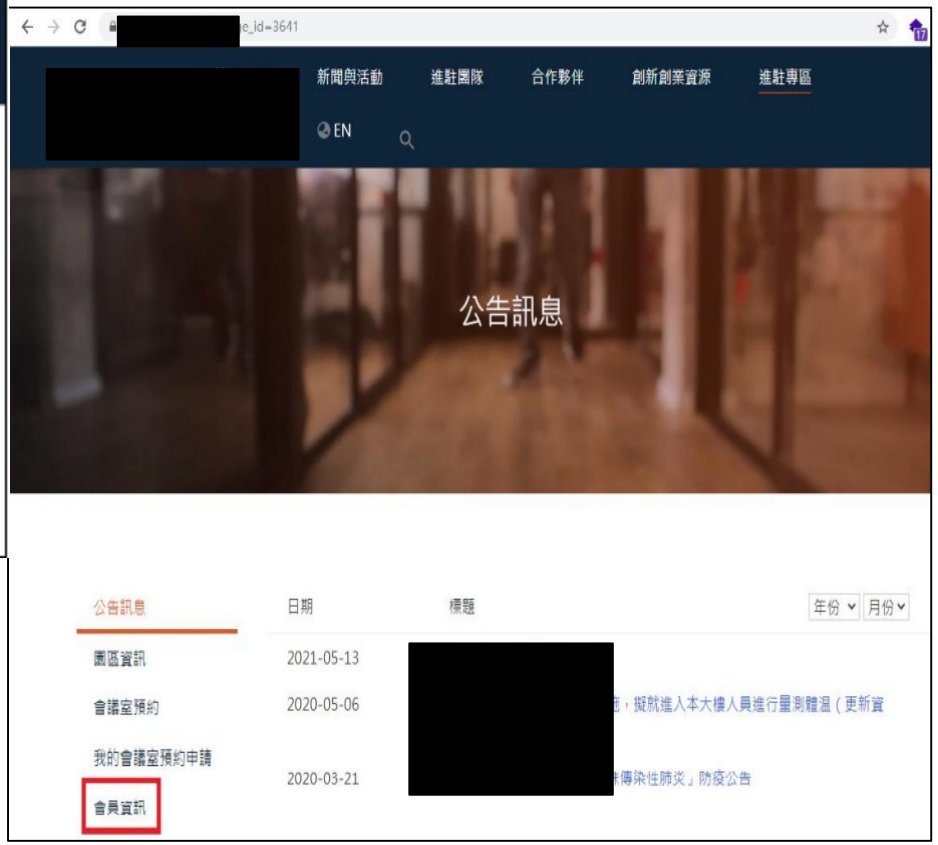
案例1 帳號與通行碼相同(1/3)

- 攻擊手瀏覽網頁，使用Google搜尋進駐廠商統一編號



案例1 帳號與通行碼相同(2/3)

- 帳號與通行碼輸入統一編號後成功登入，試圖編輯公開資訊



案例1 帳號與通行碼相同(3/3)

- 確認成功修改公開頁面之公司簡介

未落實通行碼強度檢查機制改善建議

- 通行碼符合機關通行碼複雜度原則，但內容包含公開資訊，則易被攻擊者利用拼接方式猜測成功
- 通行碼建議具備高複雜度，且避免使用公開資訊拼湊而成之通行碼

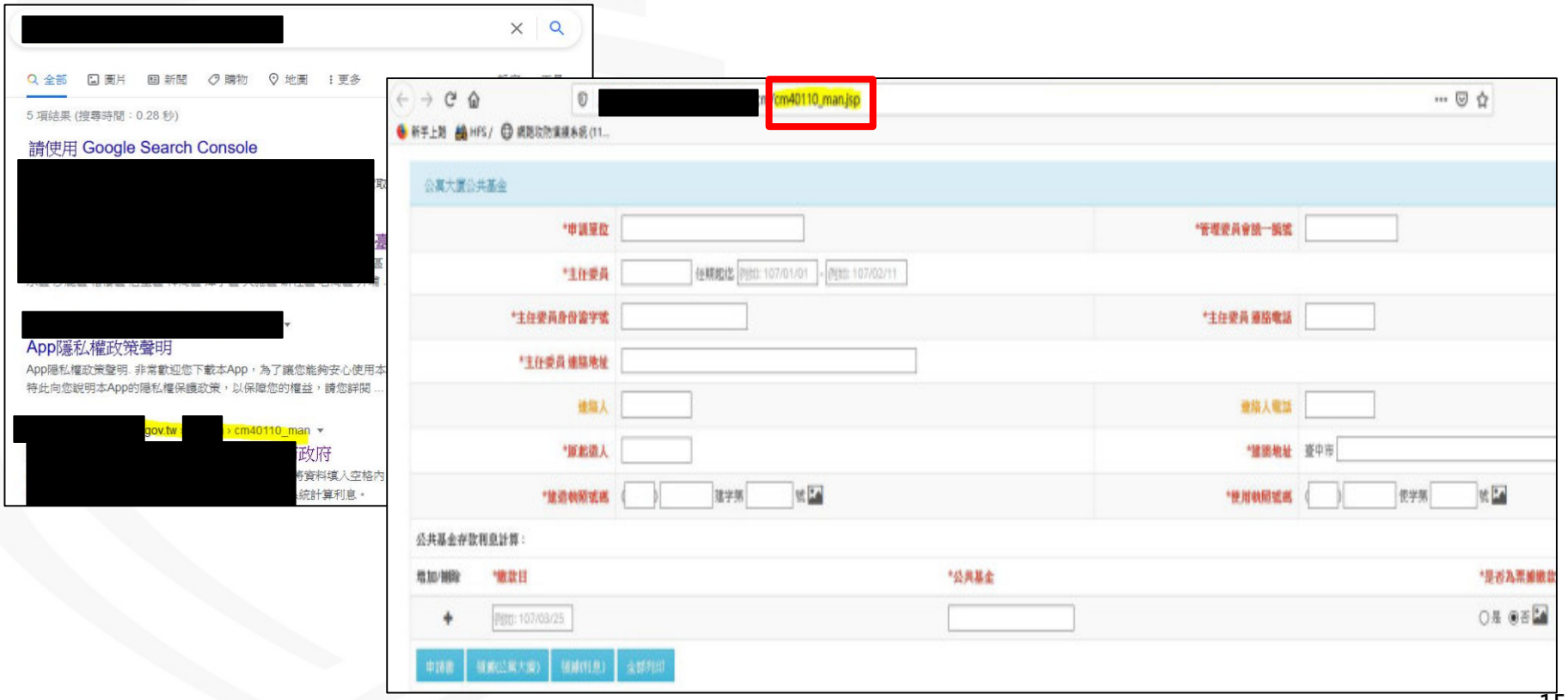
2.參數猜測

參數猜測樣態

- 以有規律數字或名稱命名系統功能頁面，針對頁面未限制存取來源且權限控管不當
- 帳戶權限控管參數為遞增/遞減數字或可識別參數值，於封包傳送過程中，攻擊者可竄改參數值，因系統未檢查使用者身分，成功異動帳戶權限

案例2-1 功能參數猜測(1/2)

- 攻擊手利用Google Hacking尋找系統可存取路徑，發現疑似功能頁面，得知路徑命名規則

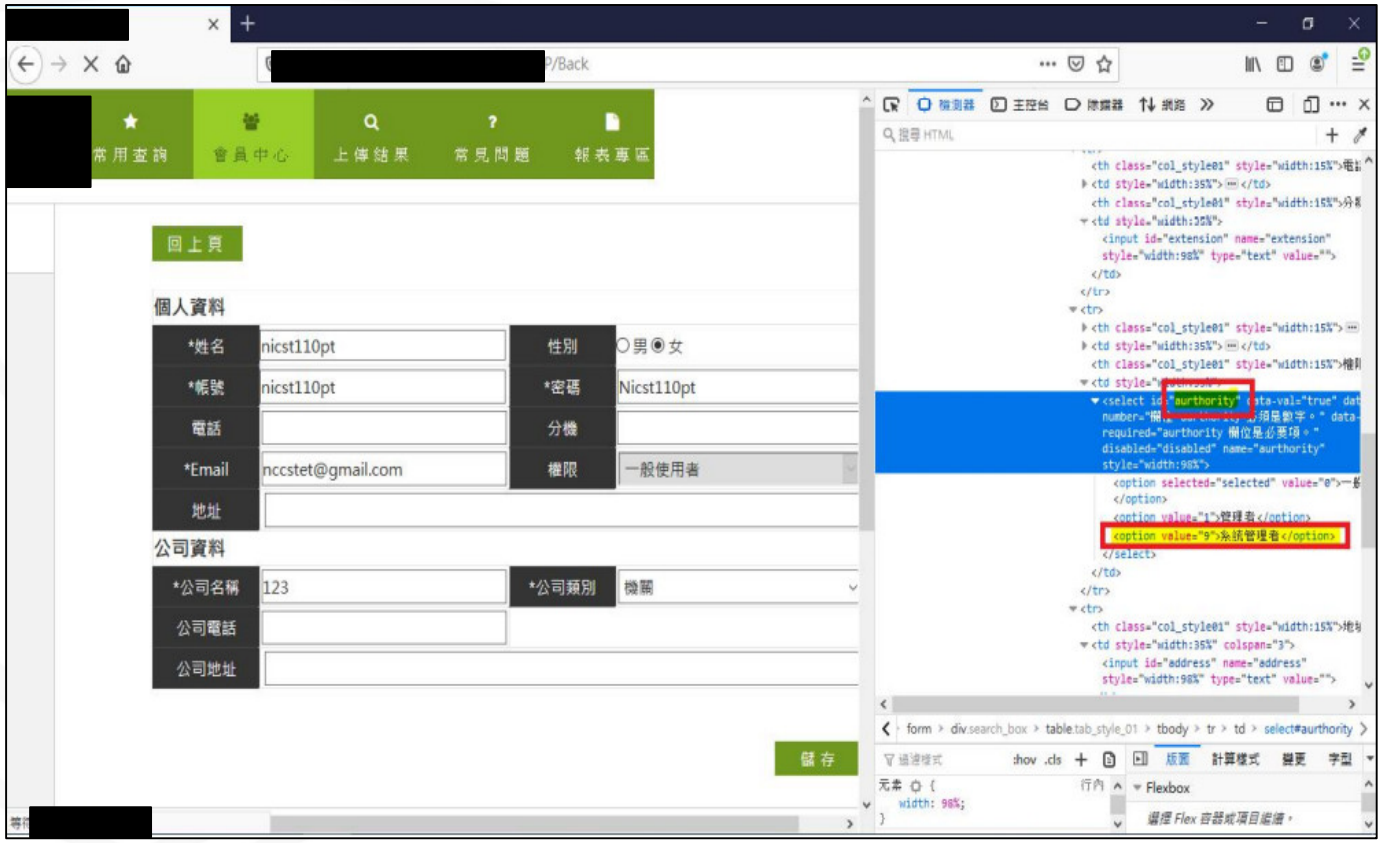


案例2-1 功能參數猜測(2/2)

- 進行路徑猜測，發現使用者資料維護頁面，嘗試新增使用者並設定新增帳號具備系統管理者身分

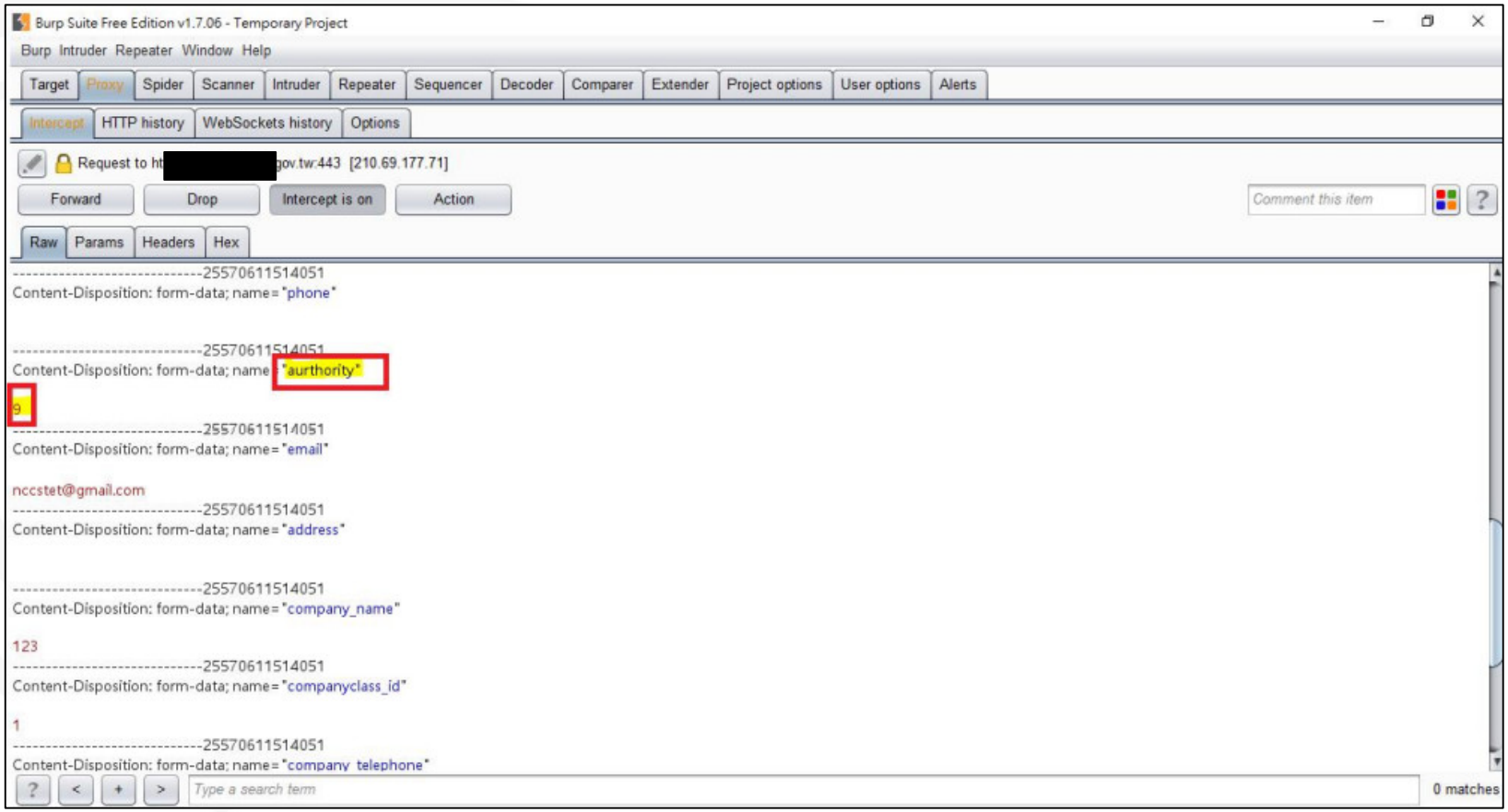
案例2-2 帳號權限參數猜測(1/3)

- 攻擊手於網頁註冊帳號，並在個人資料頁面原始碼發現權限欄位「id」為「aurthority」且「系統管理者」對應值為「9」



案例2-2 帳號權限參數猜測(2/3)

- 使用Burp Suite攔截封包，將註冊帳號「權限」參數名稱修改為「aurthority」，同時將參數值設為「9」



案例2-2 帳號權限參數猜測(3/3)

- 發現註冊帳號已從「一般使用者」提升為「系統管理者」

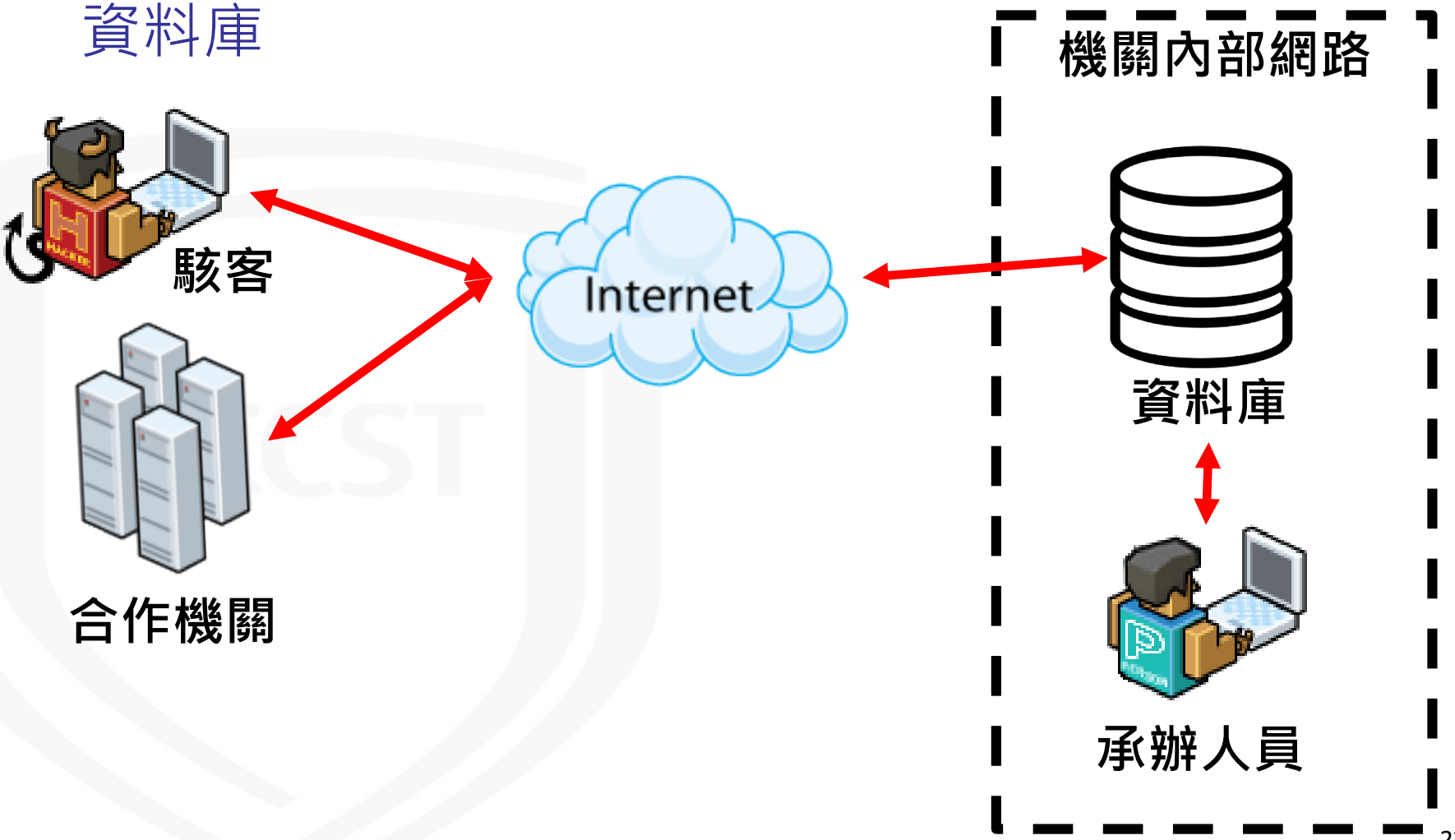
參數猜測改善建議

- 針對系統功能頁面與參數，應檢查對應權限，並控管各帳號權限存取範圍，降低使用者跨越權限存取功能

3.資料庫未限制存取來源

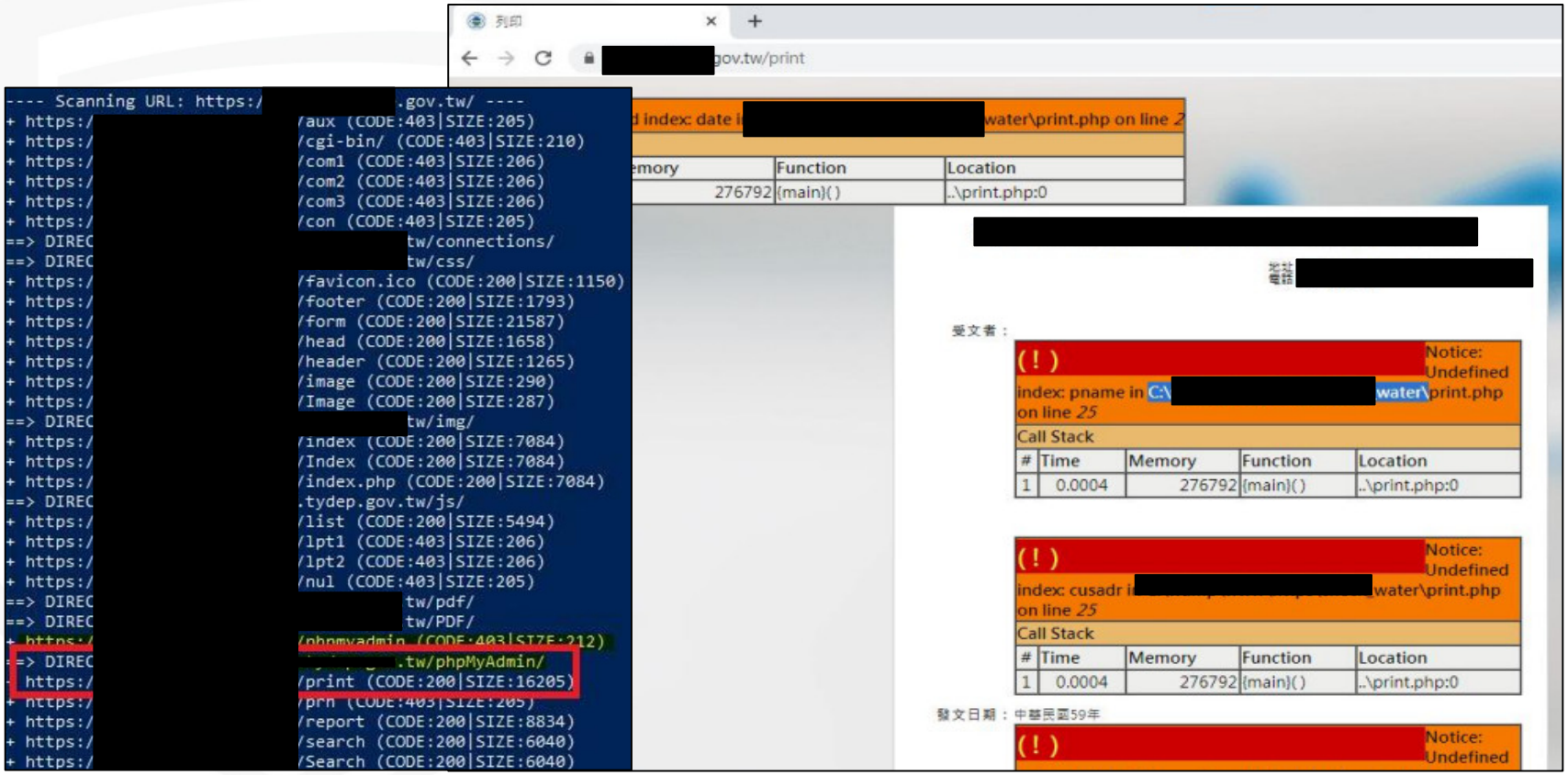
資料庫未限制存取來源樣態

- 取得資料庫登入頁面，允許外網來源直接存取資料庫



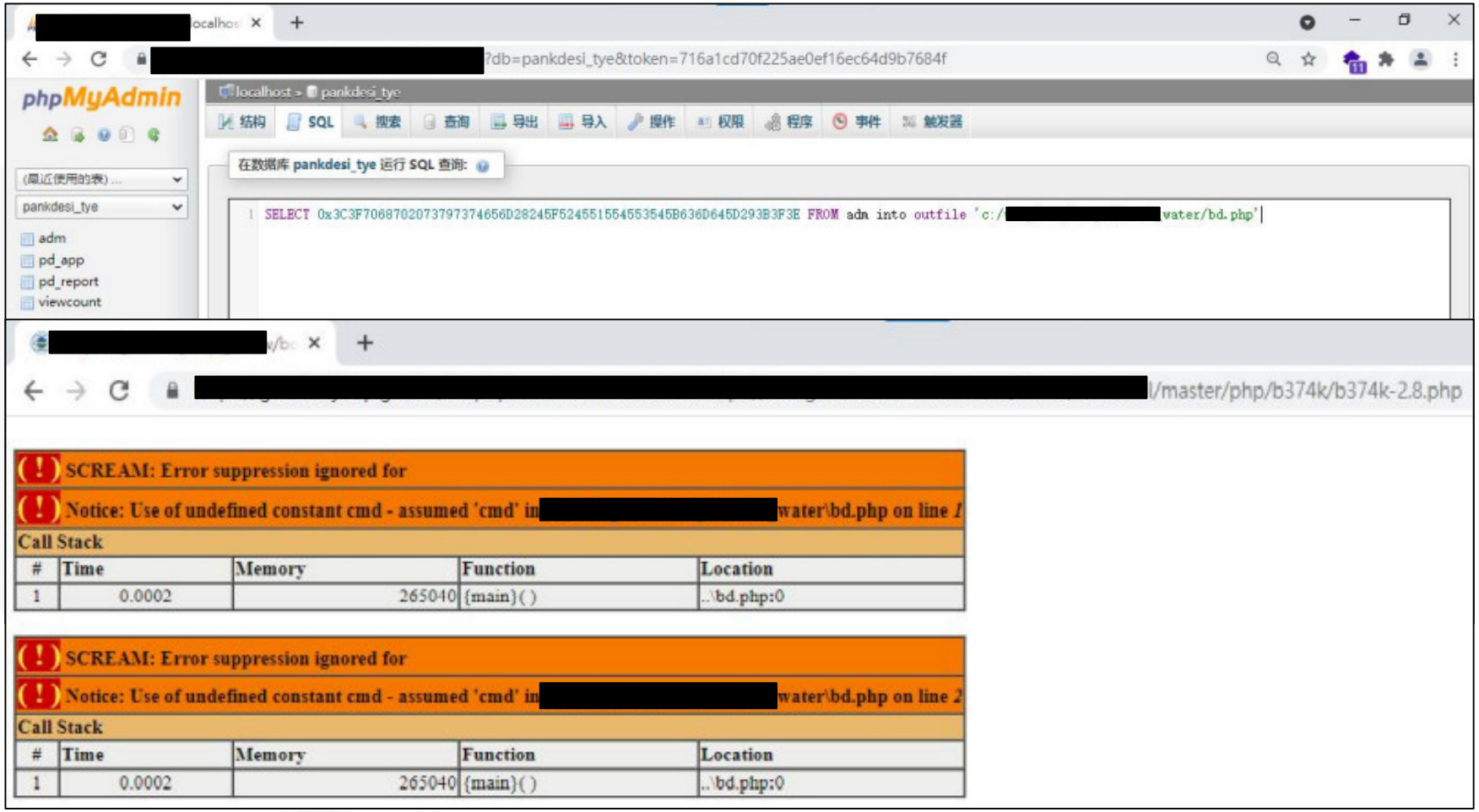
案例3 資料庫未限制存取來源(1/3)

- 攻擊手利用掃描目錄，發現系統phpMyAdmin網頁路徑與某頁面內含有絕對路徑



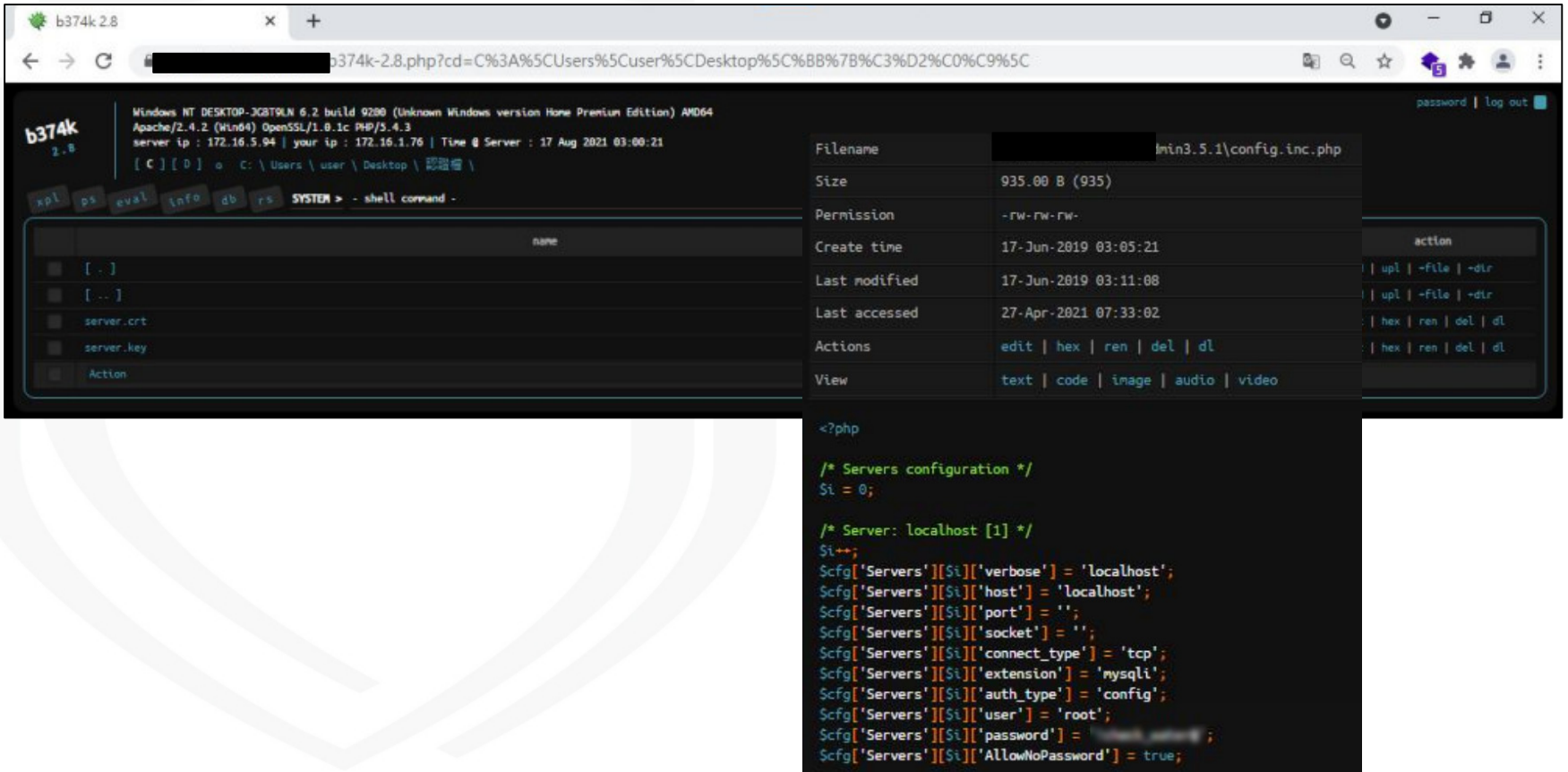
案例3 資料庫未限制存取來源(2/3)

- 瀏覽phpMyAdmin網頁，執行SQL語法將Webshell寫入至網站目錄



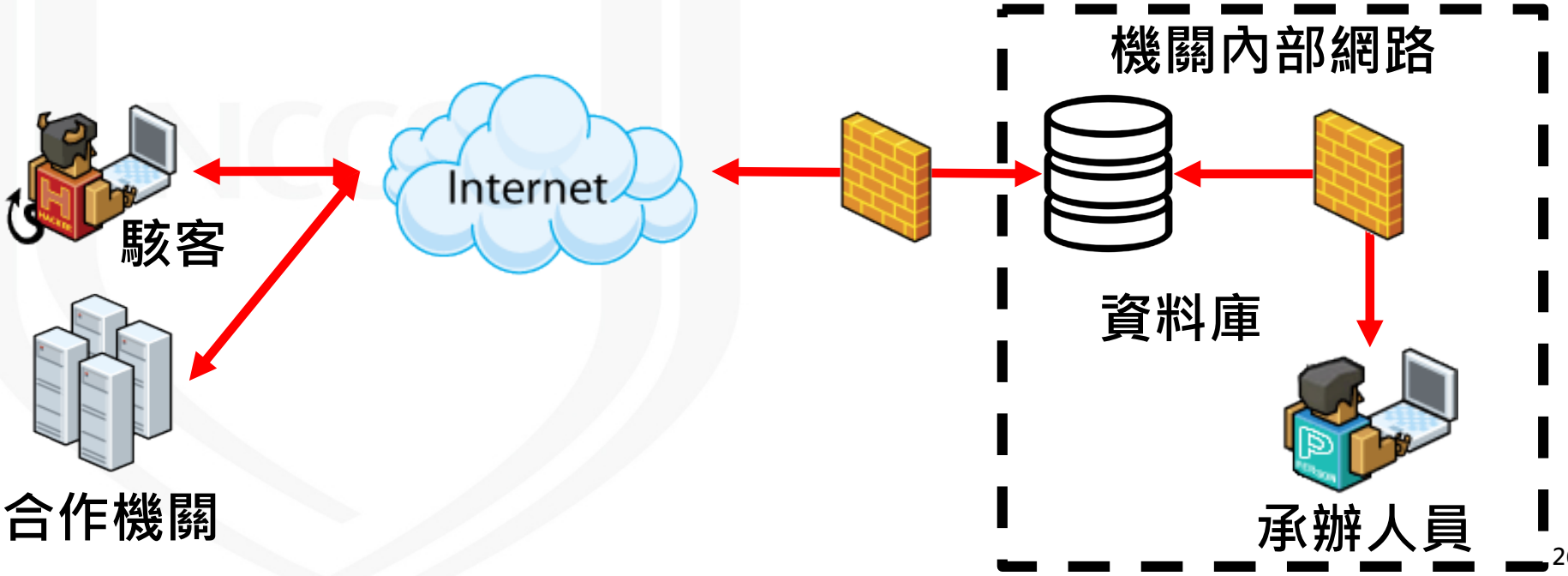
案例3 資料庫未限制存取來源(3/3)

- 利用上傳之Webshell下載遠端管理工具至網站中，再使用工具瀏覽主機檔案，發現MySQL資料庫之root帳號密碼



資料庫未限制存取來源改善建議

- 資料庫應管控於內部網段，不可直接暴露於外網
- 若有資料交換需求，應於防火牆或伺服器設定存取控制，僅允許特定來源IP存取資料庫
- 避免使用root與sa等高權限帳號進行登入與執行AP程式，其餘帳號須限縮存取範圍



4.不當的轉導設計

不當的轉導設計樣態

- 多數系統權限檢查失敗時，會透過特定方式進行轉導
- 網站透過前端JavaScript語法進行轉導，因回應封包夾帶過多資訊，導致攻擊者可修改JavaScript繞過身分驗證

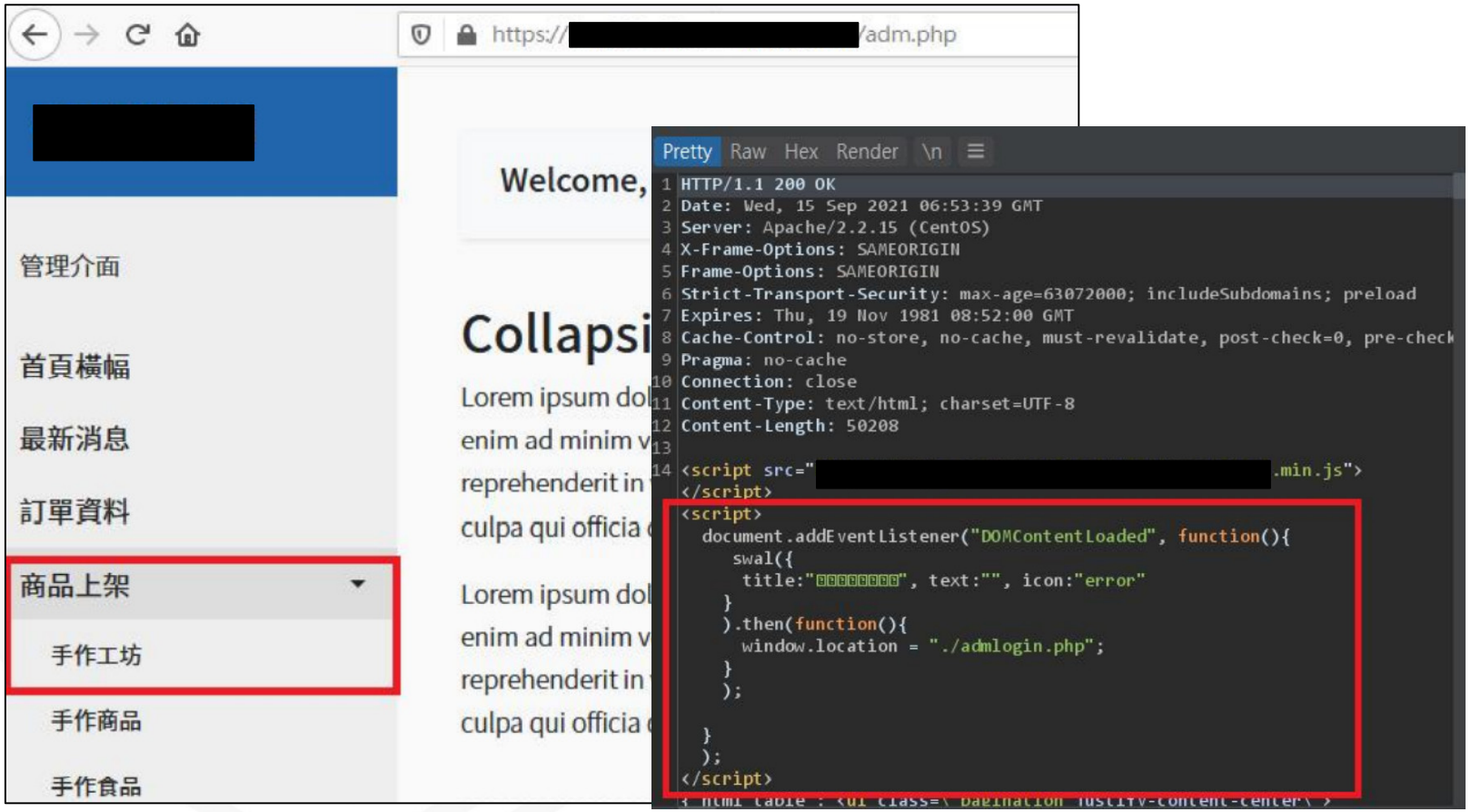
案例4 轉導設計不當(1/3)

- 攻擊手利用掃描目錄，發現系統後台頁面

```
┌──(nccst07㉿kali09)-[~]
└─$ dirb https:                                  .tw/ ./elist.txt -X.php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Sep 15 14:48:53 2021
URL_BASE: https://                               tw/
WORDLIST_FILES: ./elist.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 4477

---- Scanning URL: https:                                .tw/ ----
+ https:/                                  /adm.php (CODE:200|SIZE:13155)
+ https:/                                  /about.php (CODE:200|SIZE:8293)
+ https:/                                  /cart.php (CODE:302|SIZE:14944)
+ https:/                                  /check.php (CODE:302|SIZE:16773)
+ https:/                                  /conn.php (CODE:200|SIZE:0)
+ https:/                                  /contact.php (CODE:200|SIZE:10361)
+ https:/                                  /function.php (CODE:200|SIZE:0)
```

案例4 轉導設計不當(2/3)

- 使用Burp Suite工具將回傳封包內具轉導功能之JavaScript語法刪除



案例4 轉導設計不當(3/3)

- 嘗試新增資料，並確認成功新增於公開頁面

不當的轉導設計改善建議

- 建議逐一頁面進行權限控管，依系統角色差異，明確區分存取來源為訪客(未登入)、一般使用者及管理者等權限
- 所有檢查應於伺服器端進行，僅回傳必要檢查結果，避免將未授權或不必要功能頁面併入檢查結果回傳，以防遭攻擊者竄改，進而繞過檢查機制

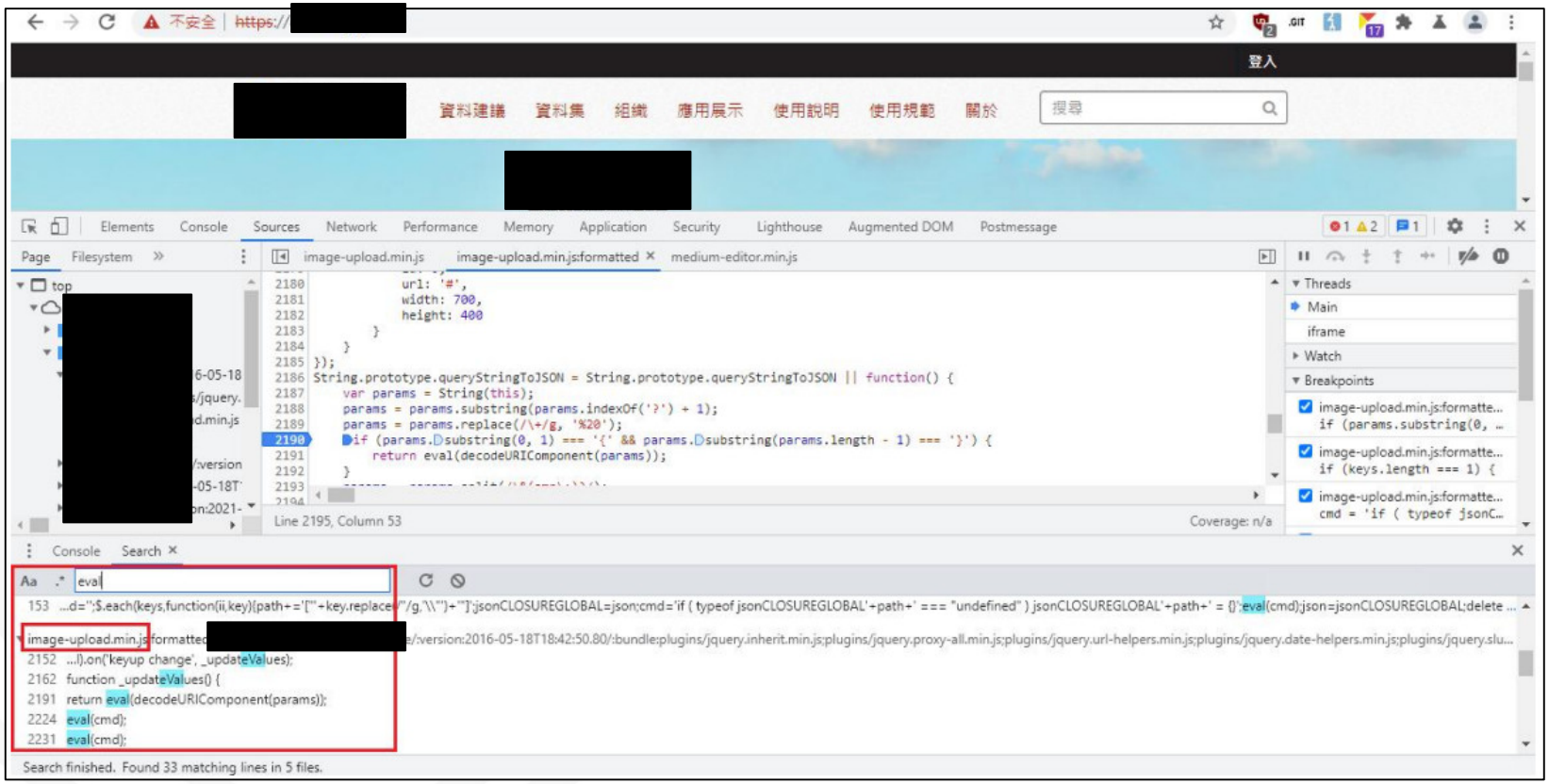
5.跨網站腳本攻擊

跨網站腳本攻擊樣態

- 跨網站腳本攻擊允許攻擊者將惡意語法注入至網頁，使用者點選含有惡意語法頁面或連結時觸發攻擊語法
- 攻擊者透過含有惡意程式碼URL，利用網頁使用之JavaScript執行，造成DOM-based跨網站攻擊

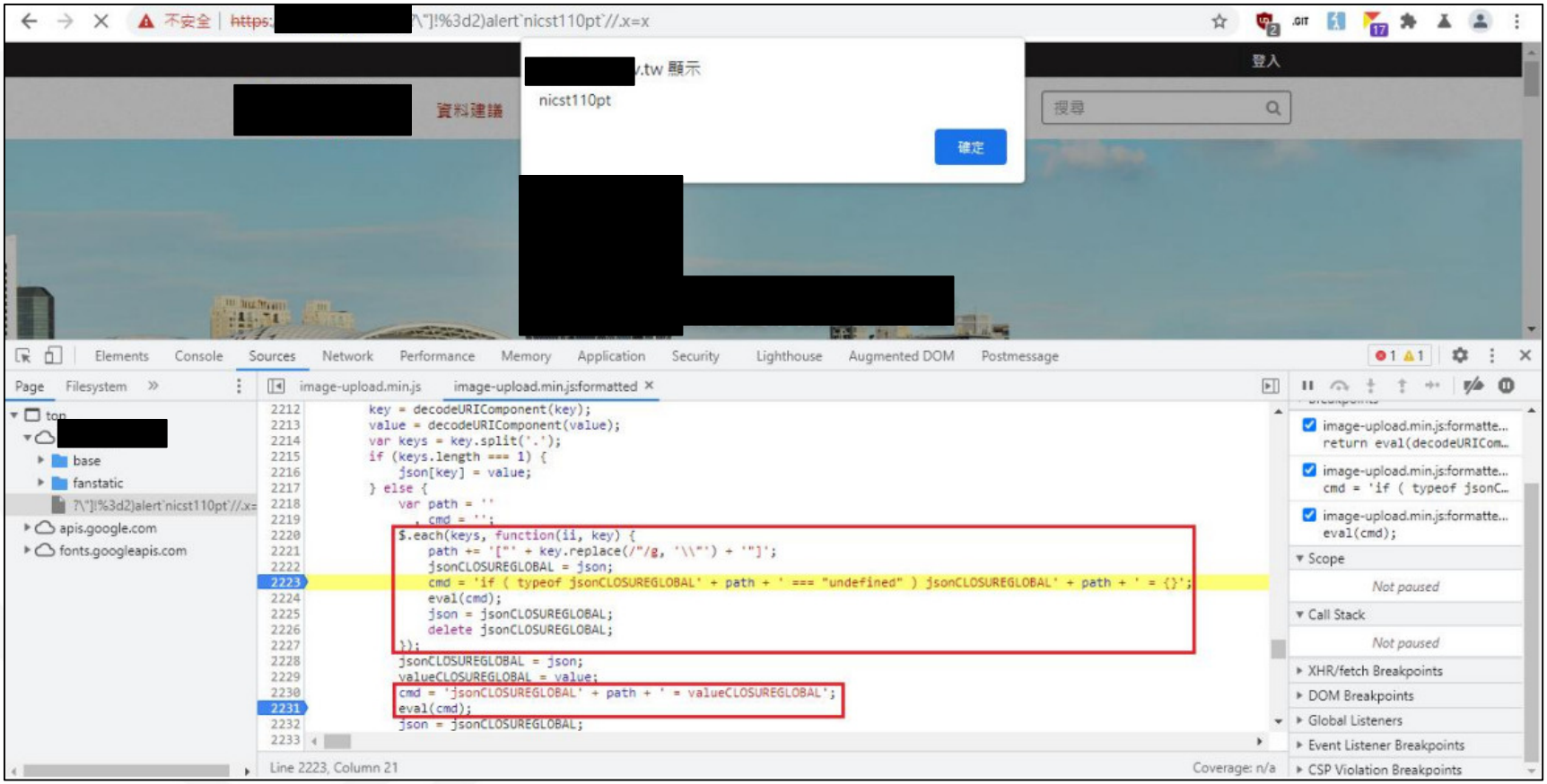
案例5 跨網站腳本攻擊(1/3)

- 攻擊手檢視系統原始碼，發現image-upload.min.js檔案使用eval()



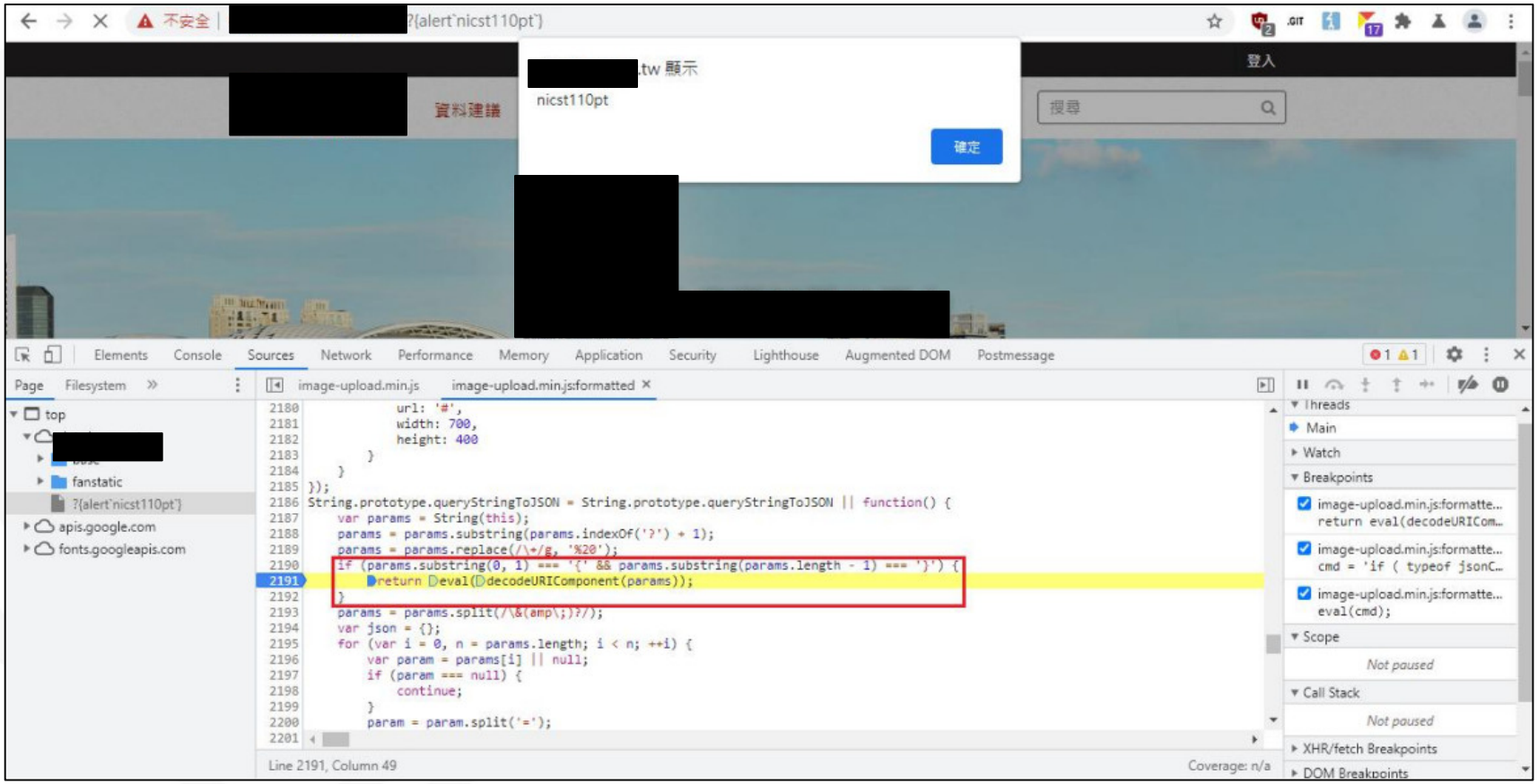
案例5 跨網站腳本攻擊(2/3)

- 攻擊手輸入攻擊語法1，成功顯示彈跳視窗
  - –攻擊語法：?\"]!%3d2)alert`nicstXXXXpt`//.x=x



案例5 跨網站腳本攻擊(3/3)

- 攻擊手輸入攻擊語法2，成功顯示彈跳視窗
  - –攻擊語法：?{alert`nicstXXXXpt`}



跨網站腳本攻擊防護建議

- 白名單
  - 限定輸入內容[a~z][A~Z][0~9]
  - 限定輸入長度
- 字串內容編碼
  - 範例：< 轉成 <、" 轉成 "
- 不信任任何來源輸入內容
- 引用JavaScript需詳細檢查資料，避免操作DOM過程被帶入惡意指令

6.注入漏洞

注入漏洞樣態

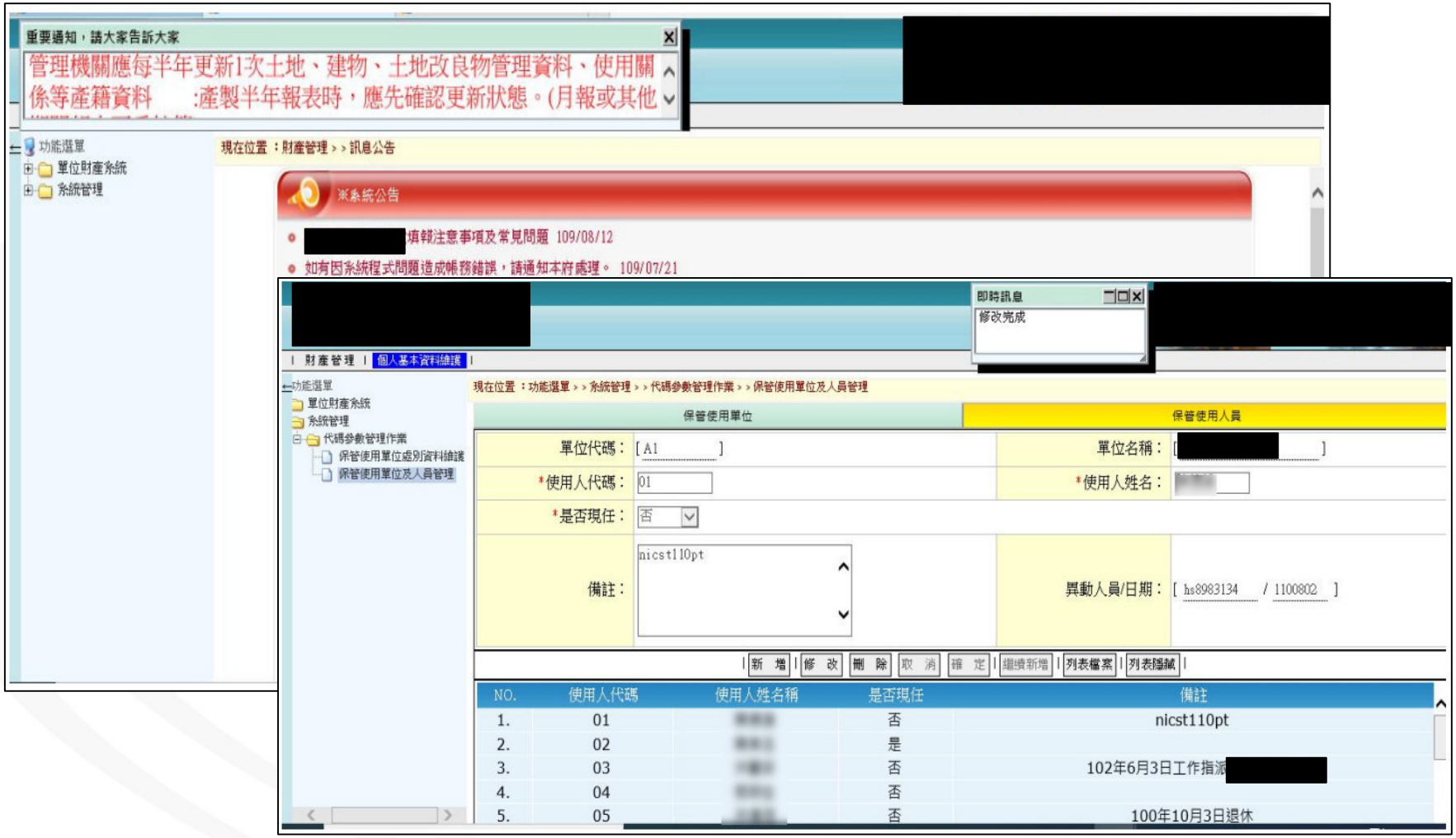
- 網站未妥善處理輸入內容，可輸入惡意指令並當成SQL語句執行
- 使用者內容以黑名單形式過濾，但過濾字串未周全，導致攻擊者以特定形式繞過

案例6 注入漏洞(1/2)

- 攻擊手於系統網頁輸入攻擊語法，嘗試繞過登入驗證

案例6 注入漏洞(2/2)

- 成功登入，取得使用者權限且可修改個人資訊



注入漏洞改善建議

- 對使用者輸入內容進行嚴格過濾，或採用白名單機制過濾使用者輸入內容
- 改以參數化形式傳值，避免SQL語句被竄改或截斷

大綱

- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

資安稽核技術檢測結果

使用者電腦安全檢測

- 使用者電腦弱點掃描共發現61個中風險弱點
- 使用者電腦安全防護檢測共發現1台電腦未更新病毒碼、9台電腦未落實安全性更新及4台電腦應用程式未更新

網路惡意活動檢視

- 共發現3筆IP中繼站名單未阻擋
- 共發現1筆DN中繼站名單未阻擋

核心資通系統安全檢測

- 核心資通系統內網滲透測結果共發現5個高風險與2個中風險弱點，其中85.7%屬於「無效的存取控管」弱點
- 核心資通系統防護基準檢測結果共發現17個不符合項目

網路架構檢測

- 網路架構檢測共發現5個高風險、7個中風險及3個建議項目

網域主機安全防護檢測

- 網域主機皆已部署防毒軟體並安裝所有安全性更新項目

物聯網設備檢測

- 物聯網設備檢測結果共發現21個不符合項目，其中47.6%為「軟/韌體、作業系統及相關應用程式存在CVSS v3高於7分(含)之CVE漏洞」，42.9%為「管理介面身分鑑別使用預設帳號密碼」

組態設定安全檢測

- 共發現9台使用者電腦組態設定未符合
- 共發現5台網域主機組態設定未符合
- 網通設備與伺服器應用程式組態設定皆符合

資料庫安全檢測

- 資料庫安全檢測結果共發現15個不符合項目，其中資料庫資料未具有適當保護機制」與「資料庫傳輸未具有安全機制」最多，各佔20%

使用者電腦安全檢測共同發現事項

1 機關所使用服務功能存在SSL利用中強度之加密演算法弱點，防護強度不足有被破解風險

3 仍有機關使用停止支援之作業系統與應用程式(如Windows 7、Adobe Flash Player、Office 2007等)，恐因漏洞無法修補而發生資安風險

非法使用者

資通系統

使用者

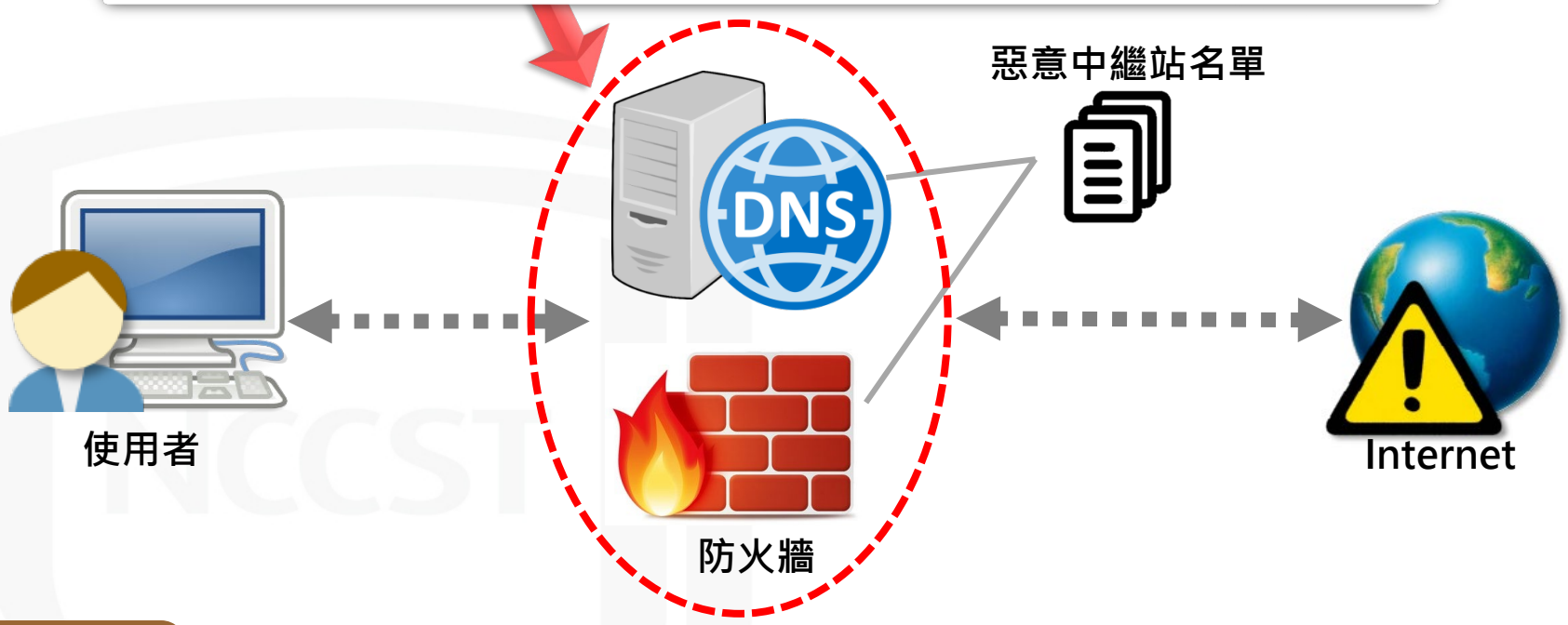
2 機關所使用服務存在SSL簽章使用不安全之Hash演算法弱點，連線資訊可能遭受破解而洩漏

改善建議

1. 使用更高強度加密演算法
2. 使用具有更高安全性加密簽章方式
3. 停用已終止支援之作業系統與應用程式，或採取其他管控措施(如限制存取與版本升級等)

網路惡意活動檢視共同發現事項

機關未確認惡意中繼站名單部署完整性與正確性，無法阻擋使用者電腦對惡意中繼站連線，可能導致機敏資訊外洩



改善建議

1. 應建立惡意中繼站名單部署與更新機制並落實執行
2. 建議定期進行惡意中繼站連線阻擋測試，確認惡意中繼站名單部署完整性與有效性

核心資通系統安全檢測共同發現事項

2 於部署環境中未針對相關資通安全威脅進行更新與修補，並開啟不必要服務與埠口(如8080、21、22等未使用之埠口)

1 系統存在無效存取控管弱點，使用者可藉由修改網頁路徑、頁面參數、HTML語法等方式，存取機關未授權功能頁面或下載檔案等

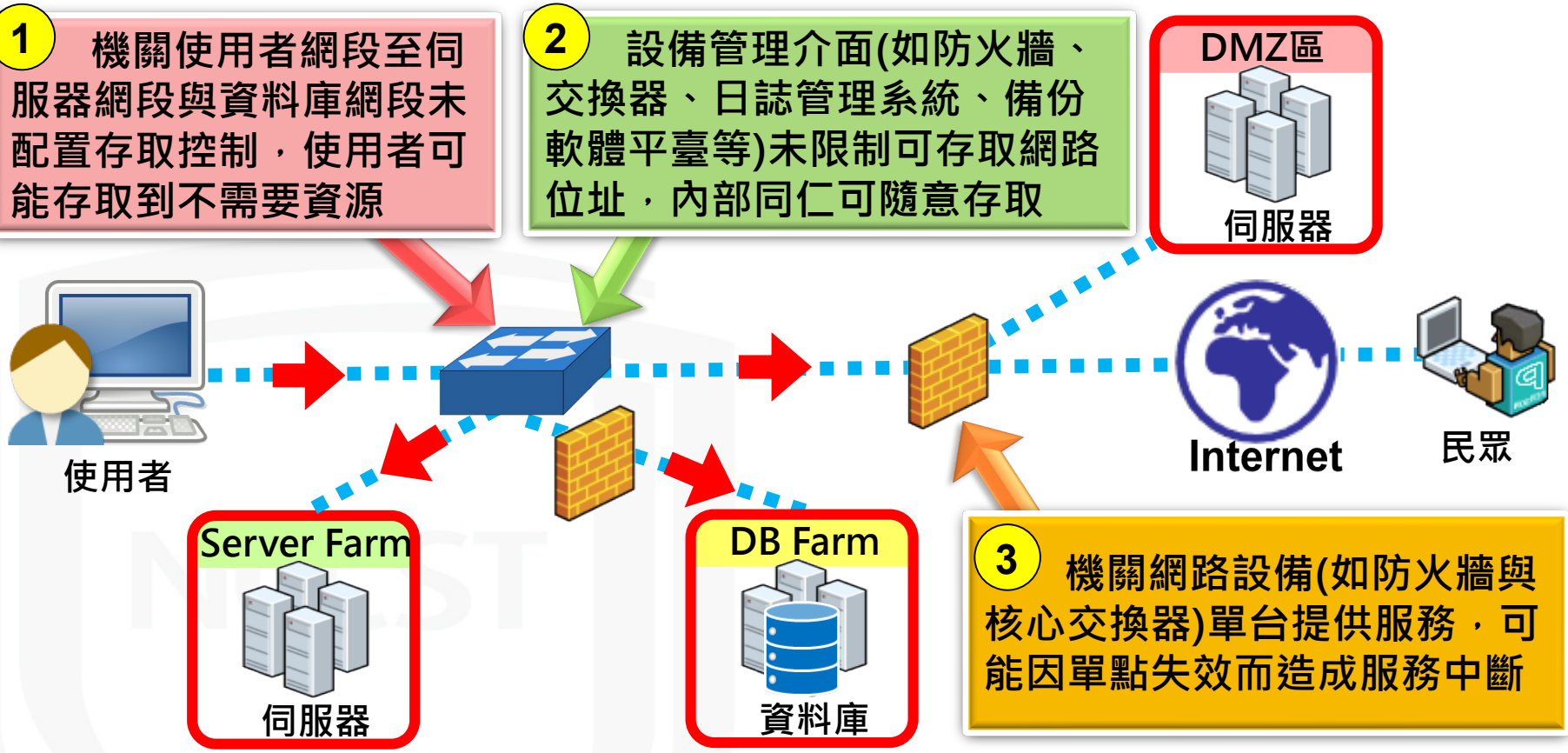
改善建議

1. 建議對所有功能頁面進行適當權限控管，避免僅在單一特定頁面進行權限檢查
2. 建議定期執行弱點掃描與修補作業，並關閉不必要服務與埠口

網路架構檢測共同發現事項

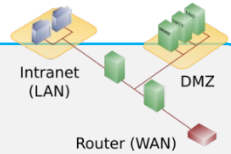
1 機關使用者網段至伺服器網段與資料庫網段未配置存取控制，使用者可能存取到不需要資源

2 設備管理介面(如防火牆、交換器、日誌管理系統、備份軟體平臺等)未限制可存取網路位址，內部同仁可隨意存取



改善建議

1. 針對網路區域間之存取，建議重新檢視防火牆，並設定存取控制規則
2. 針對網路設備存取控制，建議限制僅管理人員之IP可存取管理介面
3. 建議核心設備可建立自動備援機制，提高服務可用性



物聯網設備檢測共同發現事項

1. 設備的管理介面、Telnet及SNMP服務使用預設帳號密碼，恐有資訊外洩與遭受入侵疑慮

3. 設備管理介面面臨不正當輸入時，出現非預期異常行為或存在SQL Injection及XSS弱點

2. 軟/韌體、作業系統及相關應用程式存在CVSS v3高於7分(含)之CVE漏洞

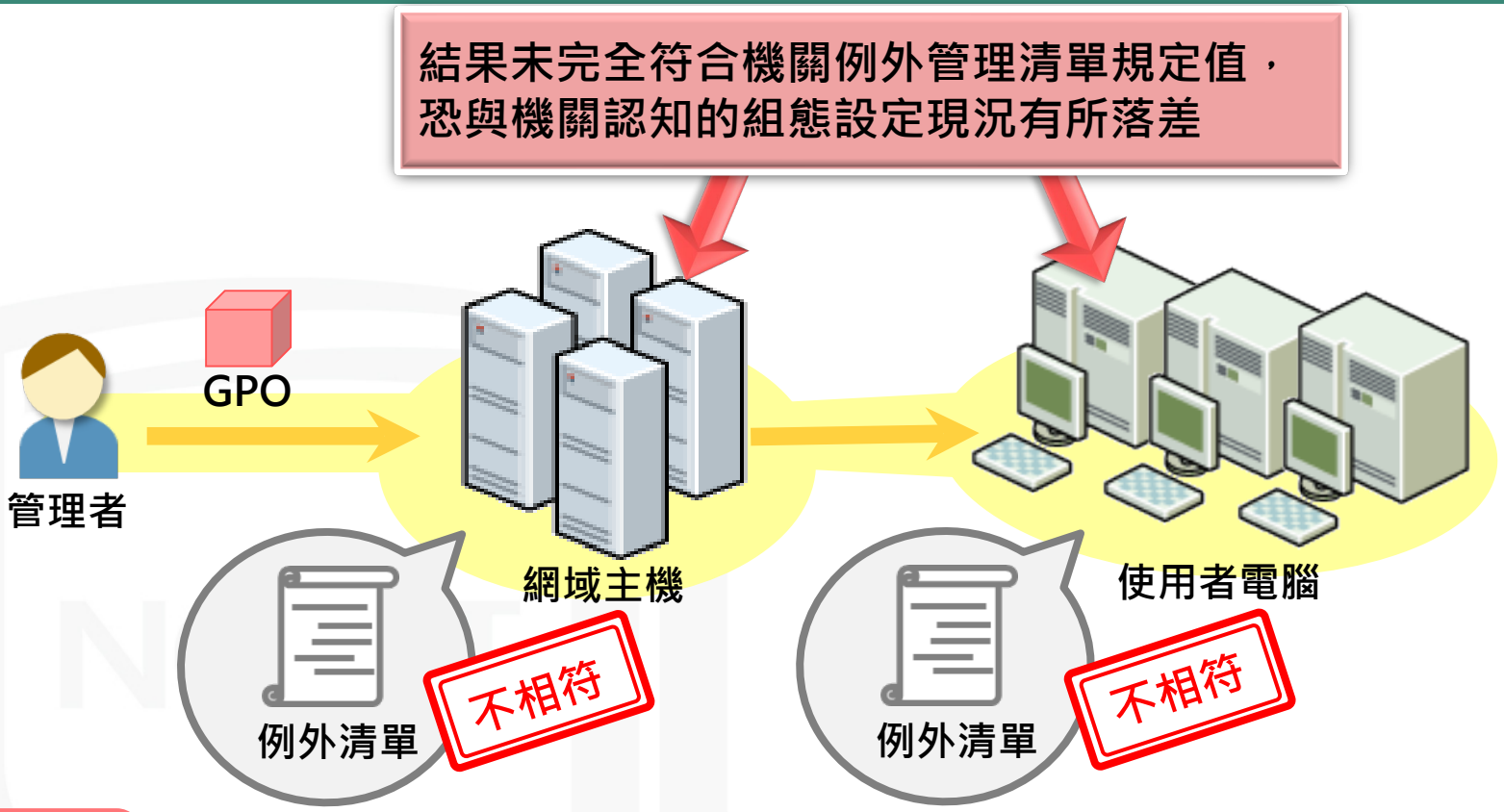
使用者

物聯網設備

改善建議

1. 設備管理介面應禁止使用預設帳號密碼，並關閉非必要服務
2. 建議定期針對物聯網設備韌體與後端服務器主機作業系統進行更新
3. 建議設備管理介面僅限定管理員可連線存取，降低不正常操作風險

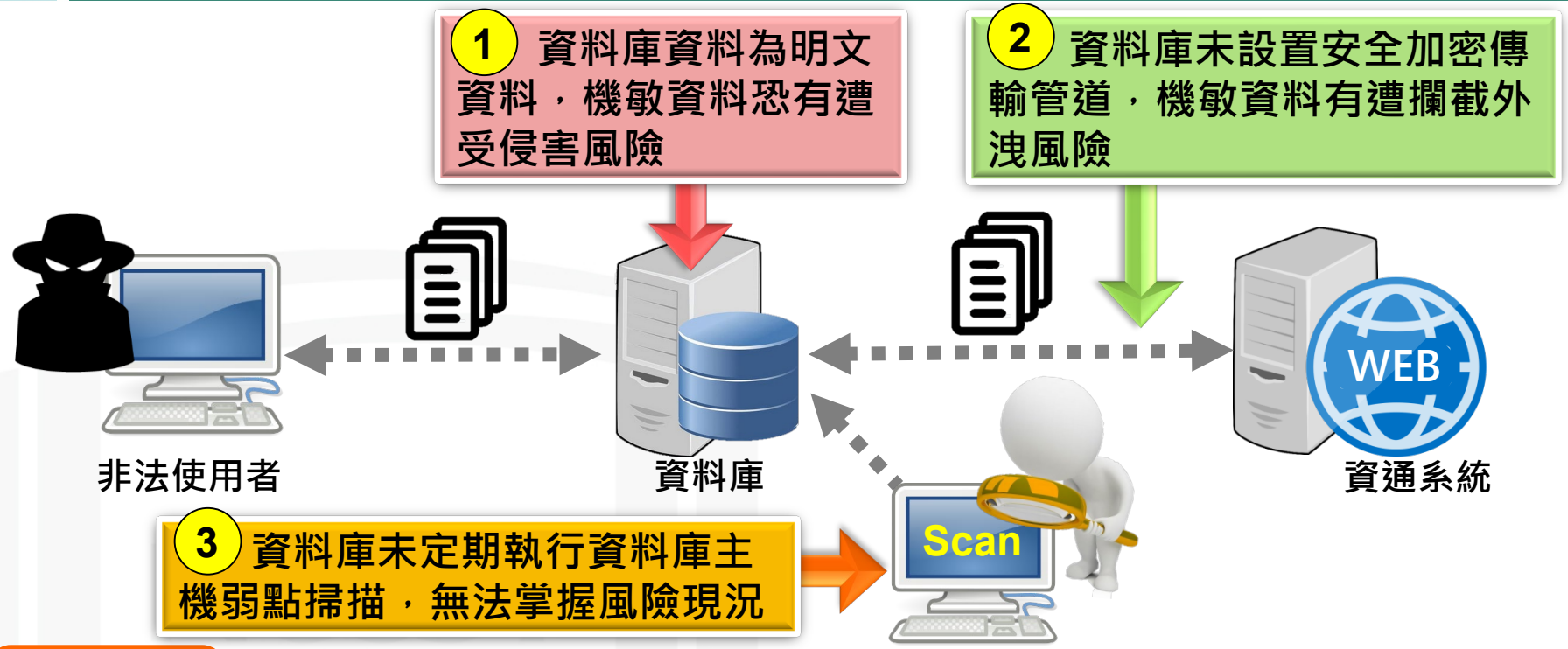
組態設定安全檢測共同發現事項



改善建議

1. 建議定期檢視網域主機群組原則部署情形，並抽檢使用者電腦組態設定內容，以確保組態設定正確性
2. 定期審查例外管理清單正確性，確保例外項目設定值符合機關管理現況

資料庫安全檢測共同發現事項



改善建議

1. 建議針對資料庫中機敏資料採取適當保護機制(如加密、不可識別處理等)強化資料儲存安全性
2. 建議資料庫應設置安全加密傳輸方式，以確保資料傳輸安全性
3. 建議定期執行資料庫主機弱點掃描，並依弱點掃描結果確實修補弱點，無法修補之弱點項目應採行其他風險控管措施，以降低未修補所導致資安風險

大綱

- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

結論與建議

- 強化通行碼防護政策
  - 針對資通系統與物聯網設備應建立完善通行碼規則，避免使用預設帳號與通行碼或帳號與通行碼相同
- 資訊揭露最小化
  - 資通系統頁面應避免洩漏過多系統資訊，減少有心人士成功利用造成系統危害
- 強化重要系統功能與設備存取控制
  - 針對資通系統重要功能頁面、資料庫及機關防火牆，應強化存取來源與存取權限
- 完備資料保護機制
  - 傳輸協定與機敏資料儲存，建議使用加密方式處理，同時啟用高強度協定或演算法

報告完畢
敬請指教