國家資通安全研究院
National Institute of Cyber Security

112年網路攻防演練暨資安檢測重要發現事項

國家資通安全研究院
112年11月

【普通】

大綱

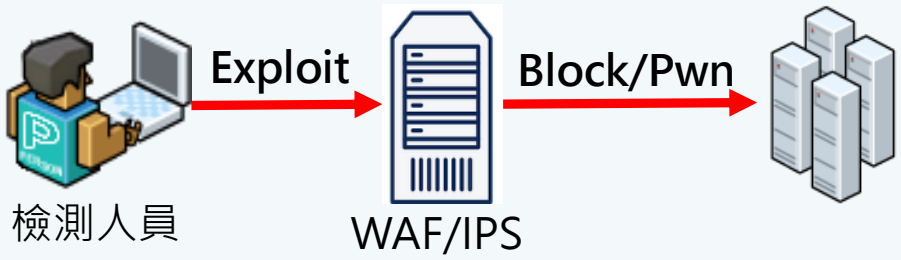
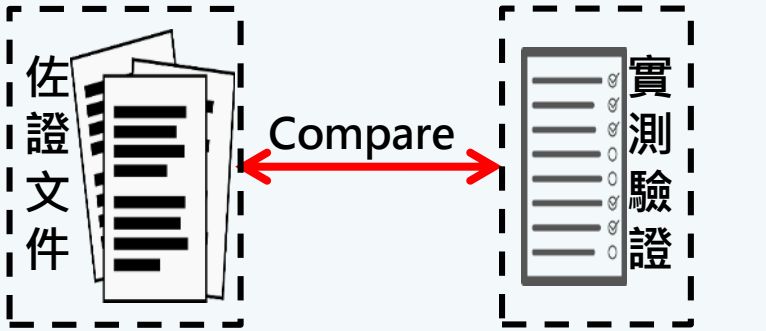
- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

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

- 資安院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	資安技術檢測
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	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，112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

網路攻防演練重要結果

國家資通安全研究院
National Institute of Cyber Security

- 本年度經由網路攻防演練，整理主要弱點類型、常見攻擊手法與可能危害如下

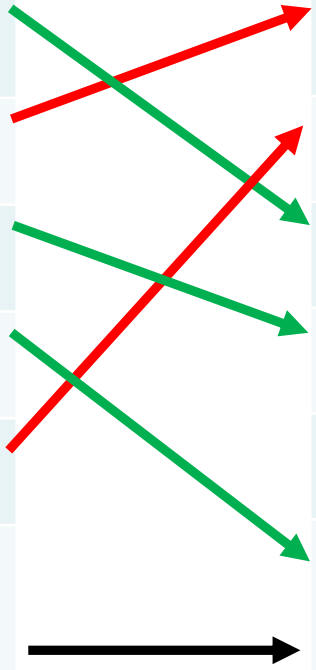
項次	弱點類型	常見攻擊手法	可能造成危害
1	認證及驗證機制失效	• 弱通行碼破解 • 透過系統手冊取得帳號通行碼資訊	• 取得系統管理權限或公開頁面修改權限 • 取得系統儲存之機敏資訊(如：個人資料)
2	注入攻擊	• 跨網站腳本攻擊 • SQL Injection攻擊	• 竊取使用者資訊 • 資料庫資訊外洩
3	無效的存取控管	• 利用開發人員工具修改原始碼，將隱藏功能顯示於網頁上 • 透過目錄掃描或路徑猜測攻擊	• 取得系統管理權限或公開頁面修改權限 • 取得系統儲存之機敏資訊(如：個人資料)
4	不安全的組態設定	• 使用預設之帳號密碼登入 • 繞過檔案上傳格式限制 • 透過安全設定不足取得攻擊資訊	• 取得系統管理權限 • 被植入後門程式
5	加密機制失效	透過網頁原始碼或以工具攔截封包取得帳號密碼	取得系統管理權限

網路攻防演練結果比較

國家資通安全研究院
National Institute of Cyber Security

- 依據弱點類型，比較111年類型之變化如下，其中認證及驗證機制失效、注入攻擊及無效的存取控管比例最高

排名	111年
1	無效的存取控管(26%)
2	認證及驗證機制失效(25%)
	不安全的組態設定(25%)
4	危險或過舊之元件(14%)
5	注入攻擊(9%)
6	不安全設計(1%)



排名	112年
1	認證及驗證機制失效(35.6%)
2	注入攻擊(25.8%)
3	無效的存取控管(19.3%)
4	不安全的組態設定(7.7%)
5	加密機制失效(6.9%) *NEW*
6	危險或過舊之元件(2.1%)
	不安全設計(2.1%)

網路攻防演練綜合發現

國家資通安全研究院
National Institute of Cyber Security

- 歸納上述弱點類型，挑選5項常見弱點樣態並分析其原因，建議參考下列9個案例，清查機關可能潛在弱點

項次	弱點類型	發現事項	案例
1	認證及驗證機制失效	**未落實通行碼強度檢查機制***	案例1-1 案例1-2
2	注入攻擊	**注入漏洞***	案例2-1 案例2-2
3	無效的存取控管	**限制存取功能失效***	案例3-1 案例3-2
4	不安全的組態設定	未確實限制檔案上傳類型	案例4
5	加密機制失效	帳號密碼外洩	案例5-1 案例5-2

*註：與111 年攻防演練發現事項相同

1.未落實通行碼強度檢查機制
(認證及驗證機制失效)

未落實通行碼強度檢查機制樣態

國家資通安全研究院
National Institute of Cyber Security

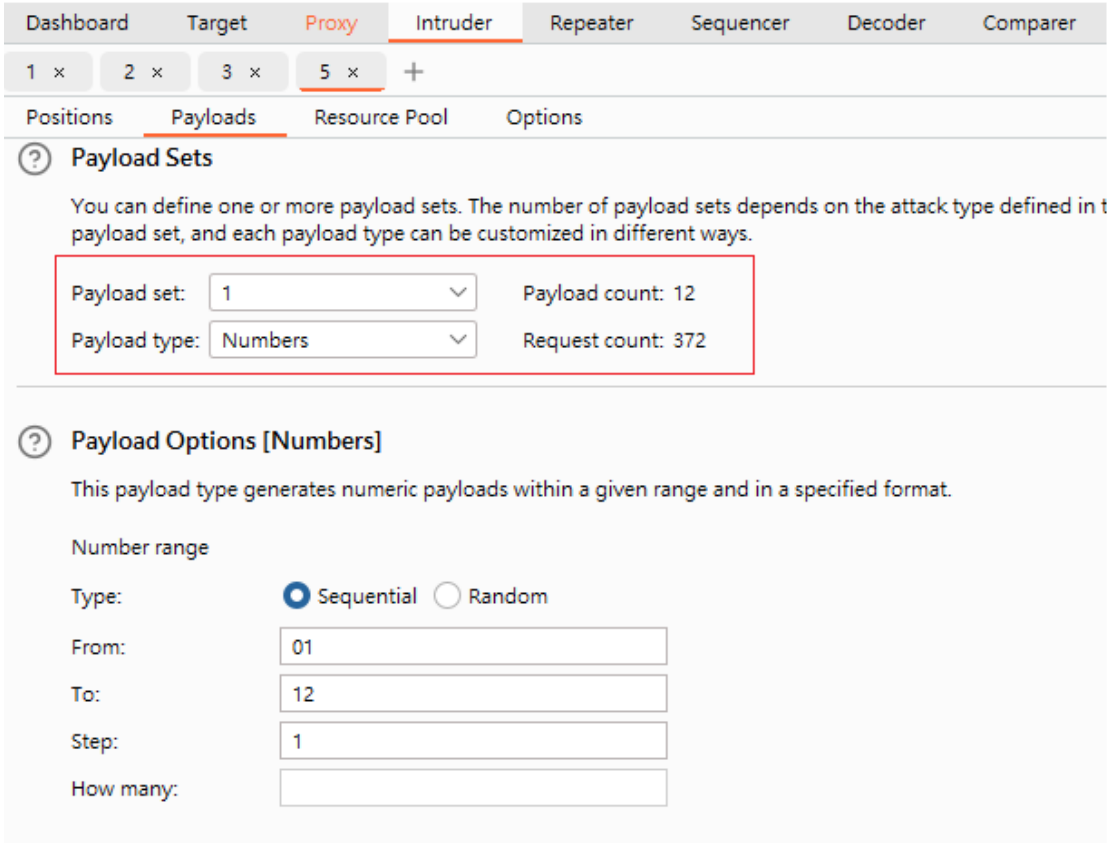
- 機關未強化通行碼設定原則
- 通行碼之提示內容(如生日年月或包含完整通行碼)，遭攻擊者利用暴力破解方式猜測成功
- 利用帳號與通行碼相同手法入侵系統複雜度極低，但受害輕則取得一般同仁權限，重則導致暴露內部往來信件或取得系統權限

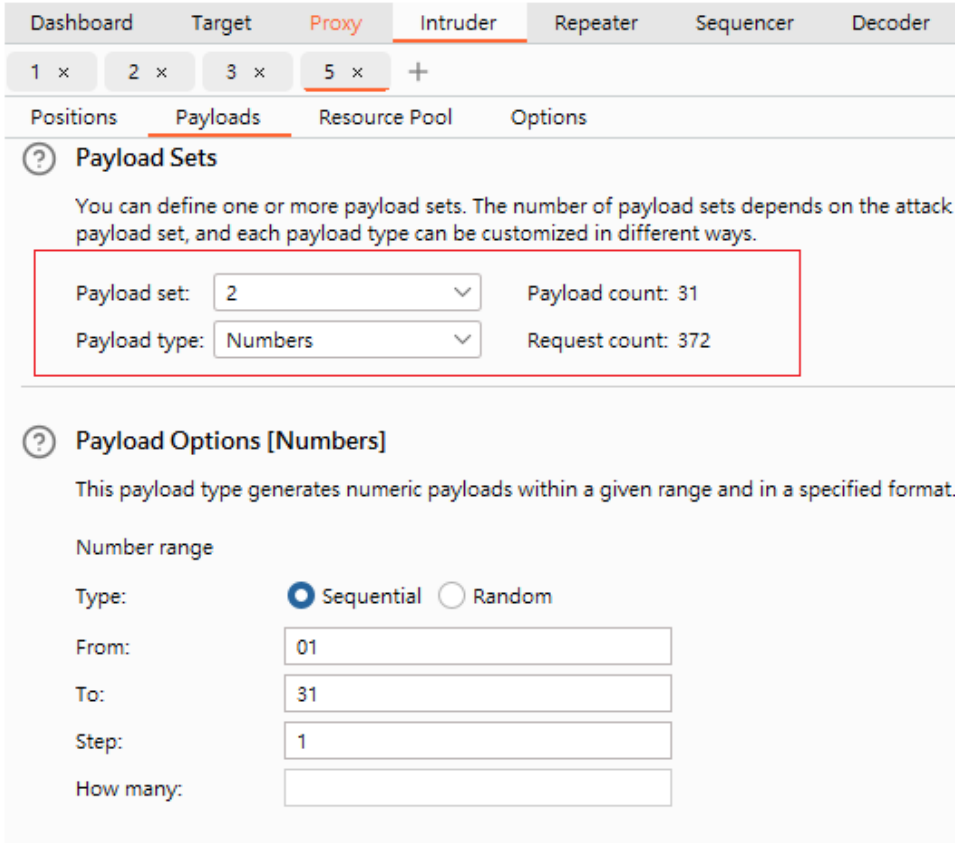
案例1-1 利用通行碼提示暴力破解(1/3)

- 瀏覽網頁會員登入頁面，發現通行碼提示為生日月日四碼

案例1-1 利用通行碼提示暴力破解(2/3)

- 利用Burp Suite攔截並竄改封包，以生日月01~12與生日天數01~31進行通行碼暴力破解

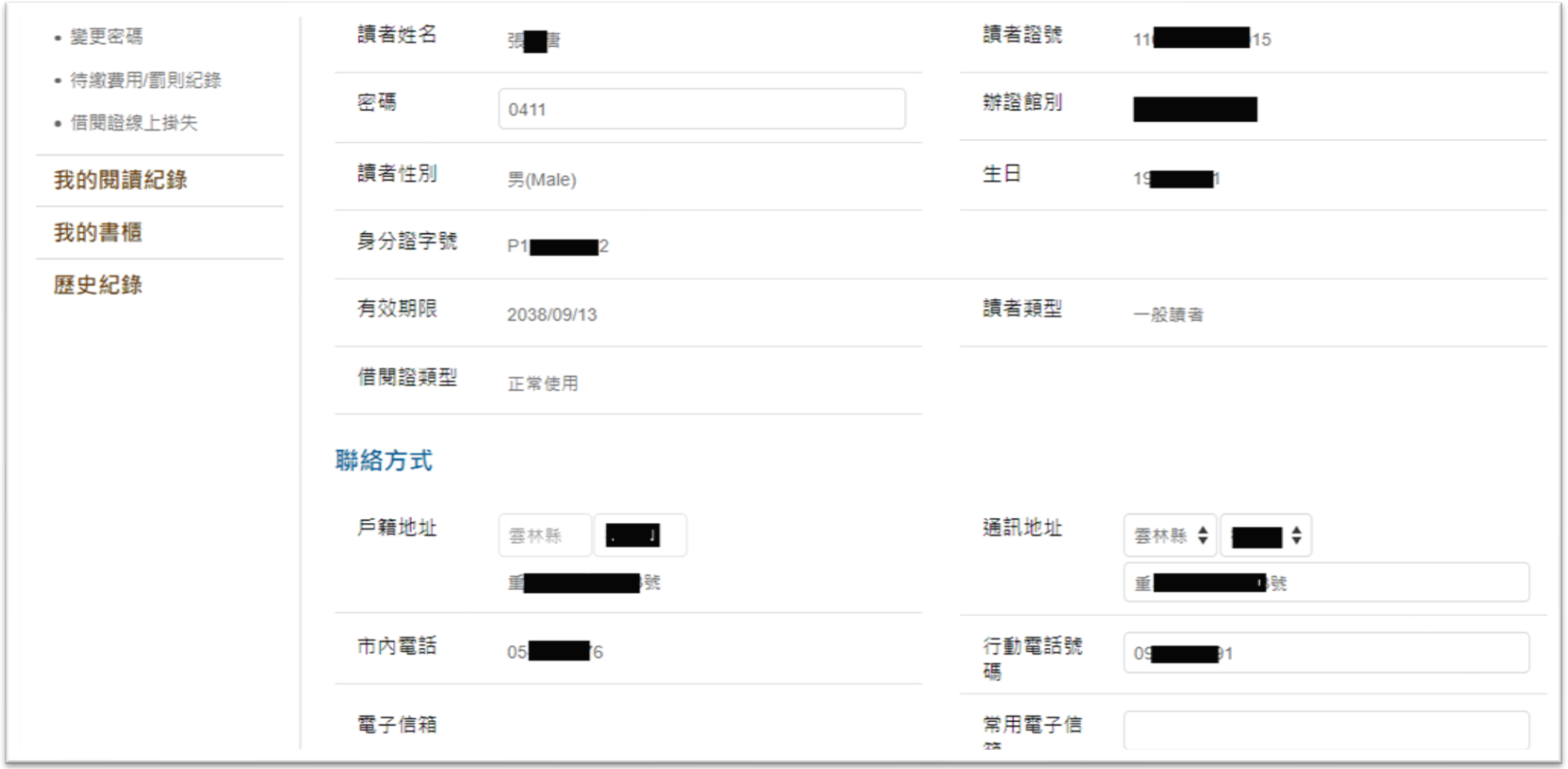




案例1-1 利用通行碼提示暴力破解(3/3)

國家資通安全研究院
National Institute of Cyber Security

- 成功登入後發現讀者個資

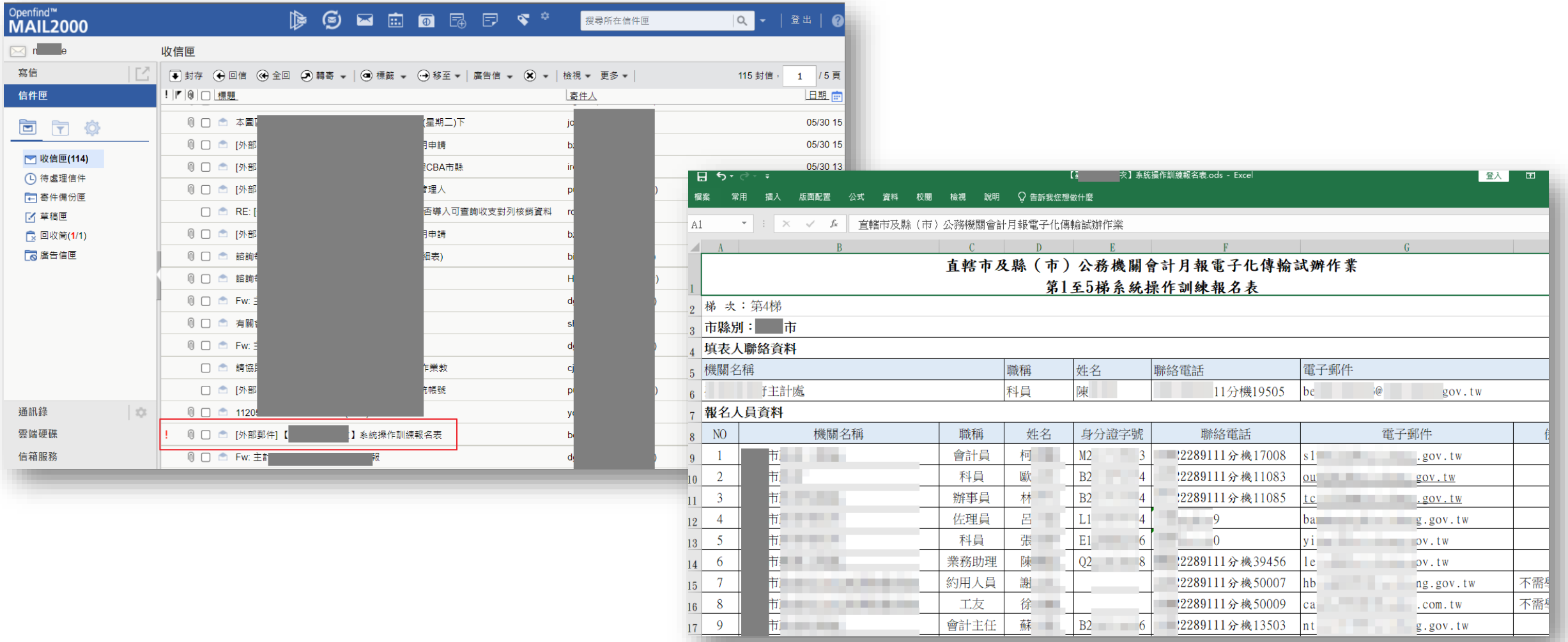


案例1-2 利用通行碼提示暴力破解(1/2)

- 瀏覽登入頁面，點選「忘記密碼」，發現密碼提示為「電話m09...」，嘗試以取得之密碼提示進行登入

案例1-2 利用通行碼提示暴力破解(2/2)

- 登入成功，並可檢視信件內容



未落實通行碼強度檢查機制改善建議

國家資通安全研究院
National Institute of Cyber Security

- 系統開發者
  - 通行碼設定應符合機關通行碼複雜度原則，以及設定密碼歷程紀錄等管控機制
  - 於登入頁面應使用圖形驗證碼等機制，避免受到暴力破解攻擊
- 系統使用者
  - 通行碼應避免使用公開易取得之資訊(如：廠商統一編號、E-mail帳號及學校代碼等)，易被攻擊者利用拼接方式猜測成功
  - 通行碼建議設定具備高複雜度，且避免使用字元過短與簡單英數字組合之通行碼

2.注入漏洞
(注入攻擊)

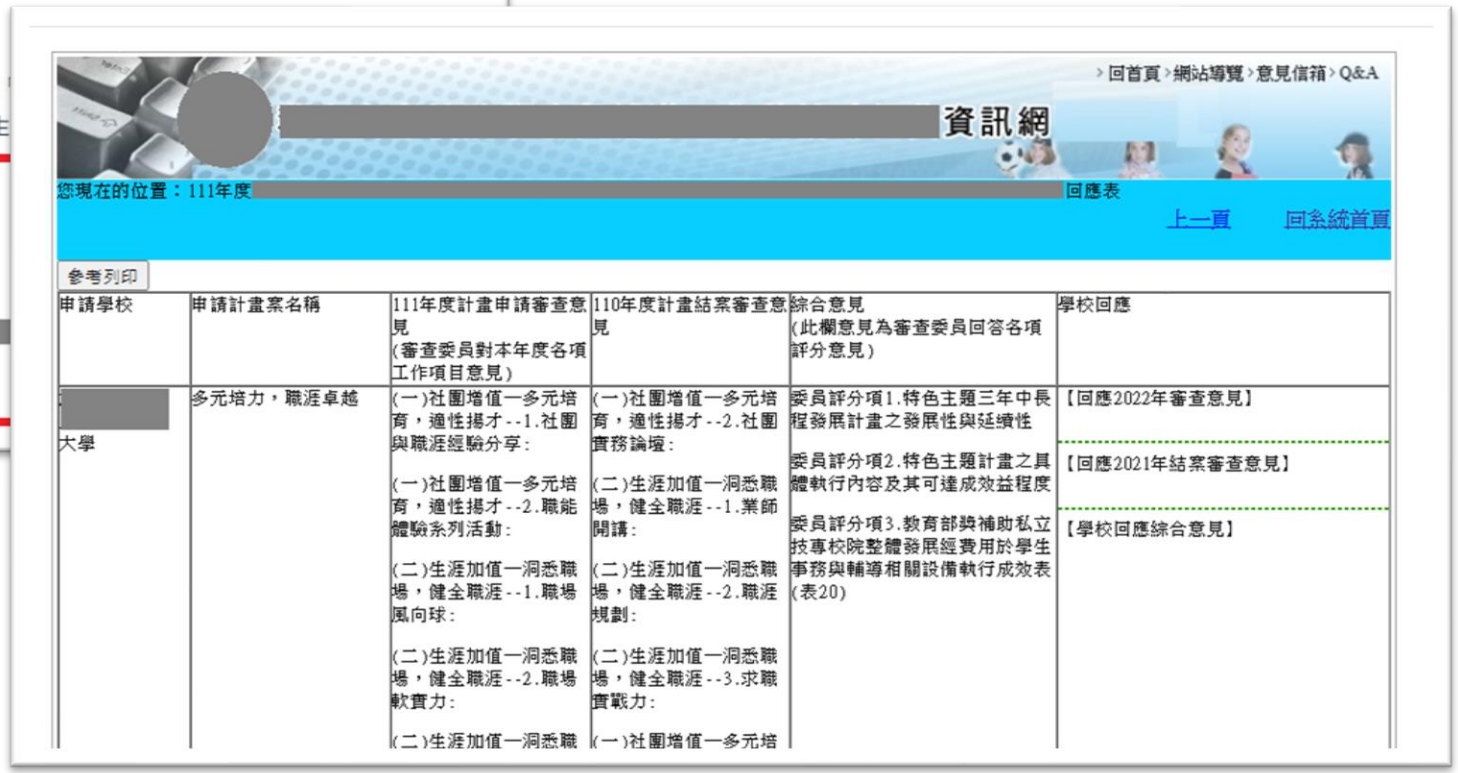
注入漏洞樣態

- 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2-1 注入漏洞(1/3)

國家資通安全研究院
National Institute of Cyber Security

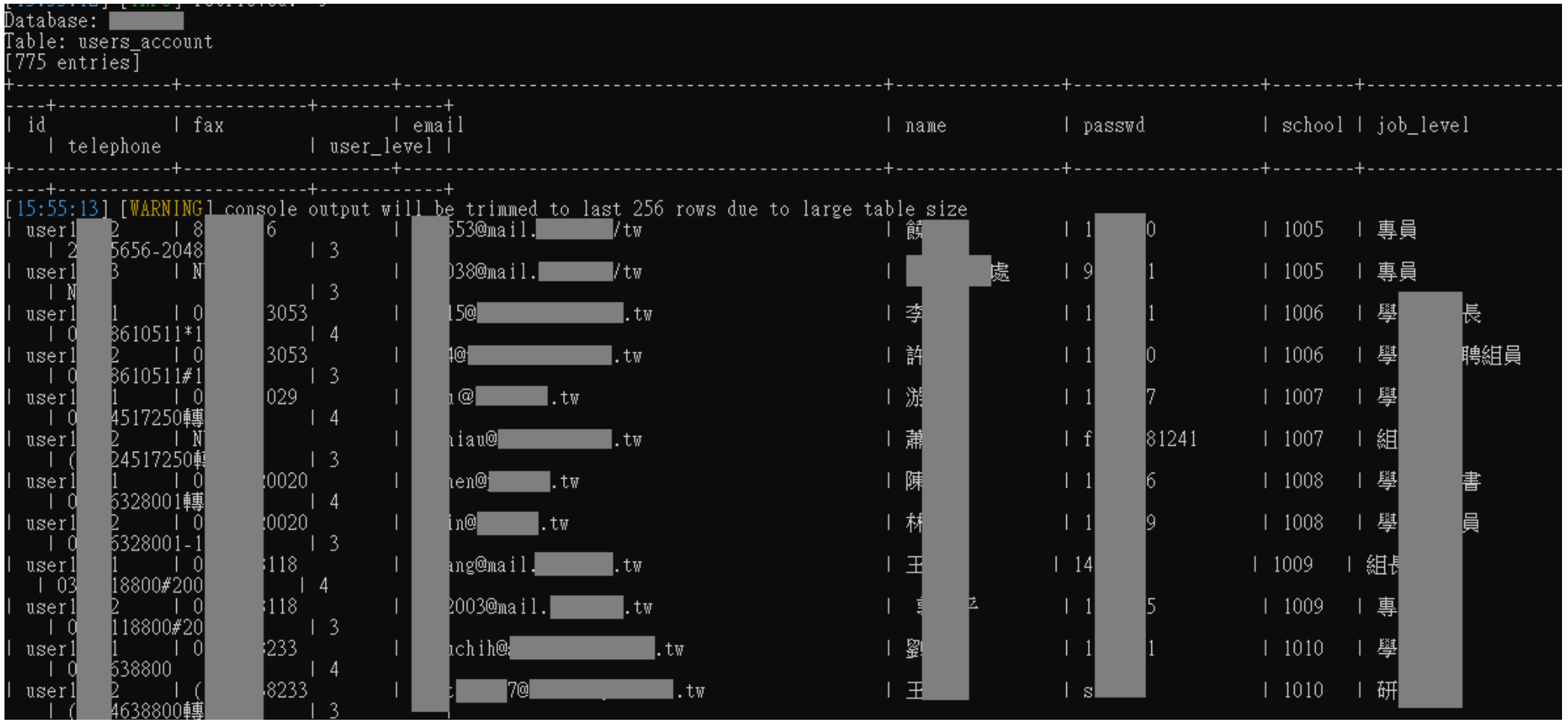
- 利用Google Hacking發現「無標題文件」網頁



案例2-1 注入漏洞(2/3)

國家資通安全研究院
National Institute of Cyber Security

- 使用SqlMap工具，取得資料庫名稱與資料表，並獲得帳號、明文密碼及Email等資訊



案例2-1 注入漏洞(3/3)

國家資通安全研究院
National Institute of Cyber Security

- 利用取得之帳號密碼成功登入，並取得系統管理者權限

案例2-2 注入漏洞(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 攻擊者使用Dirb工具掃描網站目錄，取得隱藏路徑/CDEC/，並利用攻擊語法成功繞過登入機制

案例2-2 注入漏洞(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 成功登入網站後，可取得特種個資

資料表 病史 發展衛籍 各科會診 家庭資料 報告書 結果報告 建議書一 二 三 四 五 六 診斷分類一 二 列印 複製 首頁

評估結果：發展遲緩

個案資料表

同意[redacted]

修改

姓名	蘇[redacted]晴	編號	13292	身分證字號	E22[redacted]
民國110年1[redacted]生		年齡	2歲3月	性別	女
住址1	高雄市湖[redacted]弄7號9樓之2			電話 手機	09877[redacted]
住址2					
病歷號碼	20218627	收案醫師	Dr. 余[redacted]豪	收案日期	民國112年4月6日
轉介者	☐家長(欲瞭解發展狀況) ☐醫師建議 ☐其他醫療院所 ☐轉介中心建議 ☐幼托園所老師 ☐社會、兒童福利或特教機構 ☑其他 早產兒追蹤				
就診問題	評估項目(或覺得哪些方面有發展遲緩)： ☐生理 ☐視力 ☐聽力 ☐粗大動作 ☐精細動作 ☑認知 ☐情緒 ☐行為 ☐學習 ☐社會適應 ☐人際互動 ☐感覺統合 ☑語言溝通 ☐注意力 ☐活動量 ☐衝動性 ☐日常活動功能(請註明) ☐遺傳諮詢 ☐學前鑑定 ☐開立(更新)手冊或證明 ☐輔具需求 ☑追蹤評估 ☐其他				
主訴	疑似認知、疑似語言				

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

3.限制存取功能失效
(無效的存取控管)

限制存取功能失效樣態

- 未限制存取來源或無權限控管，導致任一使用者皆可存取特定頁面
- 網站透過前端JavaScript語法進行限制，導致攻擊者可透過修改JavaScript繞過身分驗證

案例3-1 限制存取功能失效(1/4)

國家資通安全研究院
National Institute of Cyber Security

- 檢視網頁原始碼，將member之參數「display: none」刪除，可於網頁顯示「加入會員」功能

案例3-1 限制存取功能失效(2/4)

國家資通安全研究院
National Institute of Cyber Security

- 利用隱藏之功能建立帳號並成功登入

案例3-1 限制存取功能失效(3/4)

- 再次嘗試登入，利用Burp Suite攔截封包，嘗試修改伺服器回傳內容，將「Q0201S 」修改成「Q0108S 」

Pretty Raw Hex Render

```
</script>
<script type="text/javascript" src="/qanda/plugins/ech.multiselect/jquery.multiselect.filter.js">
</script>


<link rel="stylesheet" type="text/css" href="css/menulayout.css" />
<link rel="stylesheet" type="text/css" href="css/portlet.css" />
<link rel="stylesheet" type="text/css" href="css/MetroJs.css" />
<link rel="stylesheet" type="text/css" href="css/style.css" />
<link rel="stylesheet" href="/qanda/css/themes/start/jquery-ui.min.css" type="text/css" media="all" />

<script type="text/javascript">
  $(function(){
    var mo = $.evalJSON('[{"n":"news","o":"Q0108S"},{"n":"qa","o":"Q0204S"},{"n":"plus","o":"Q0208S"}]');
    if(mo.length){
      $.each(mo, function(i,o){
        $('<img src="images/'+o.n+'.'+(o.i||'gif')+'"/>').appendTo("#funcBar").css("cursor","pointer").click(function(){
          $("#content").html('').load(o.o+'_load.action',{
            session_key:'ac244a01-db5a-4c3d-8439-b546f3e68162'
          }
          );
        }
        )
      }
      )
    }
```

案例3-1 限制存取功能失效(4/4)

國家資通安全研究院
National Institute of Cyber Security

- 發現「管理員/客服人員基本資料」維護頁面，可新增具管理者權限之帳號，且登入後成功取得系統管理者權限

案例3-2 限制存取功能失效(1/3)

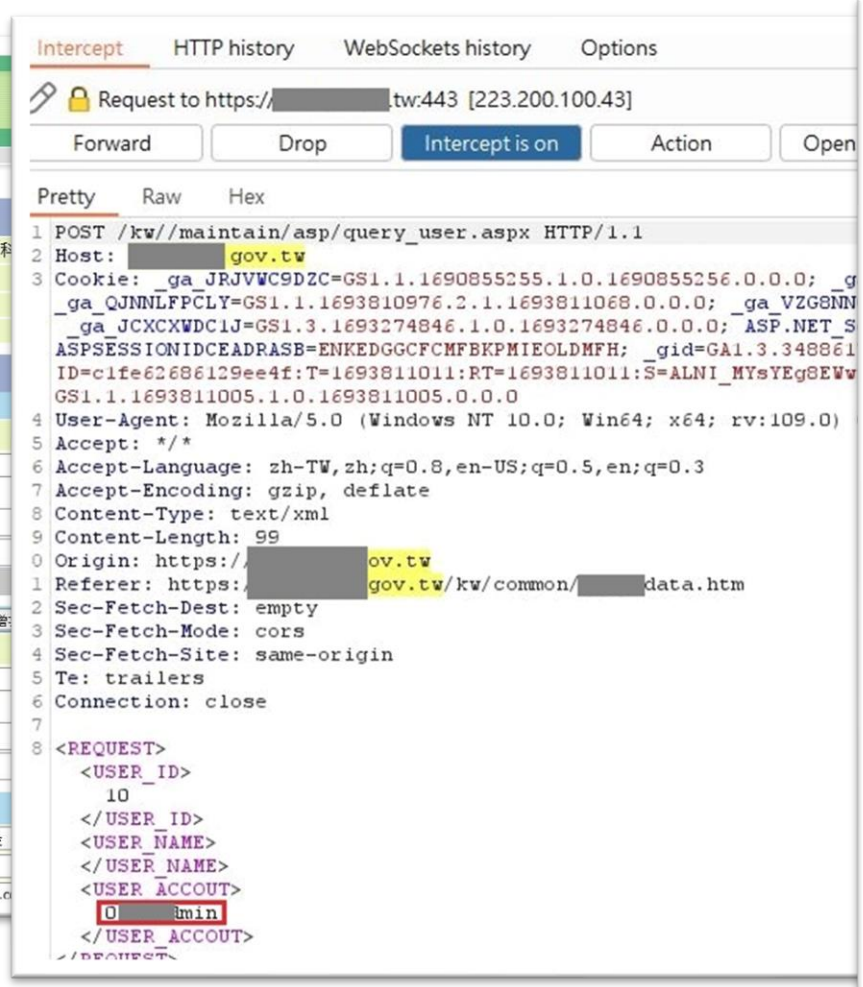
國家資通安全研究院
National Institute of Cyber Security

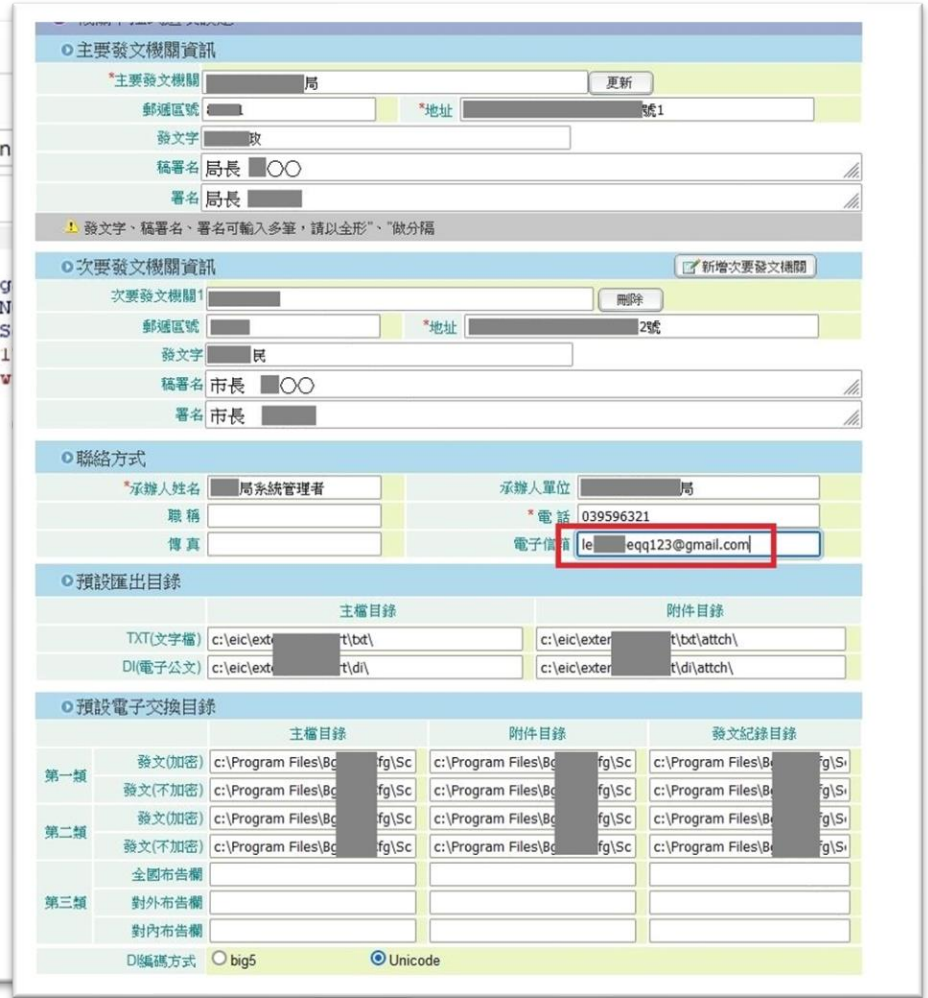
- 使用網頁正常功能新增帳號，並於帳號查詢欄位輸入「admin」，可查看管理者帳號

案例3-2 限制存取功能失效(2/3)

國家資通安全研究院
National Institute of Cyber Security

- 檢視基本資料設定，使用Burp Suite攔截封包，將使用者帳號修改成發現之管理者帳號，並將該管理者帳號之Email修改成攻擊者信箱





案例3-2 限制存取功能失效(3/3)

國家資通安全研究院
National Institute of Cyber Security

- 利用忘記密碼功能，將管理者密碼寄至攻擊者信箱，並成功登入系統

限制存取功能失效改善建議

- 系統開發者
  - 建議逐一頁面進行權限控管檢查，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
  - 避免僅利用前端JavaScript語法進行存取限制，以防遭攻擊者竄改，進而繞過檢查機制

4.未確實限制檔案上傳類型 (不安全的組態設定)

未確實限制檔案上傳類型樣態

國家資通安全研究院
National Institute of Cyber Security

- 針對網頁中之檔案上傳功能，僅以前端程式進行檔案類型控管，但未於後端伺服器進行再次確認，造成可透過攔截並竄改封包方式，成功上傳非預期之檔案類型

案例4 未確實限制檔案上傳類型(1/3)

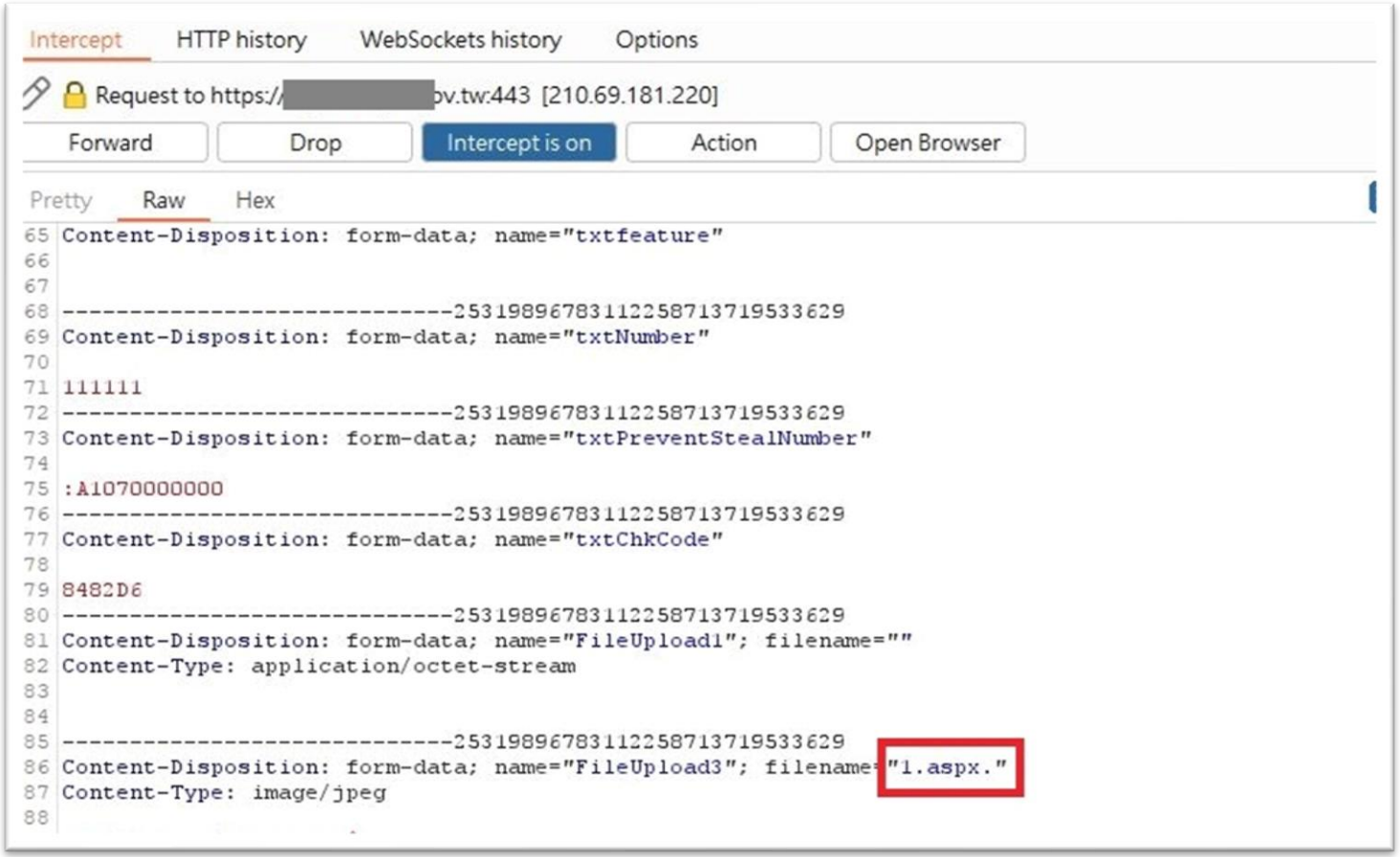
國家資通安全研究院
National Institute of Cyber Security

- 攻擊者創建新帳號，並利用其編輯圖片功能上傳檔案

案例4 未確實限制檔案上傳類型(2/3)

國家資通安全研究院
National Institute of Cyber Security

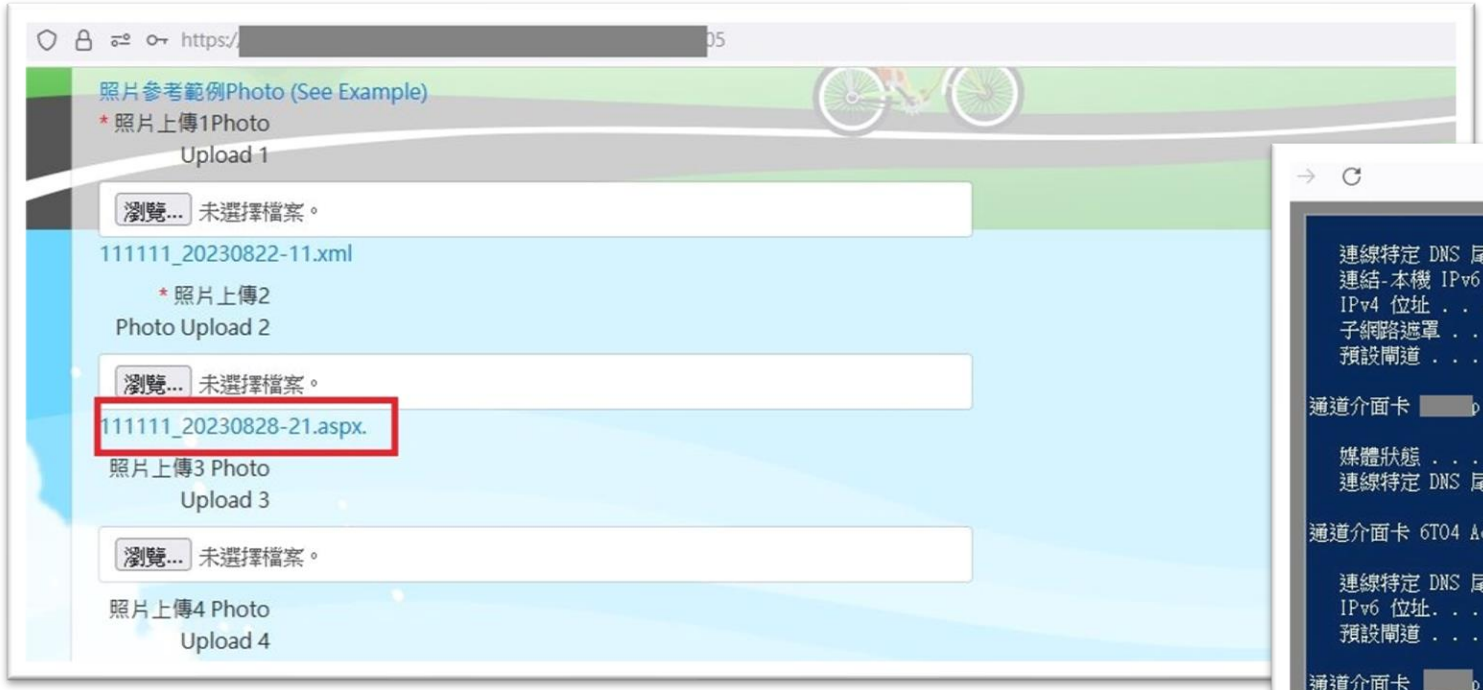
- 利用Burp Suite攔截封包，嘗試修改參數「filename」，將「.jpg」修改成「1.aspx」

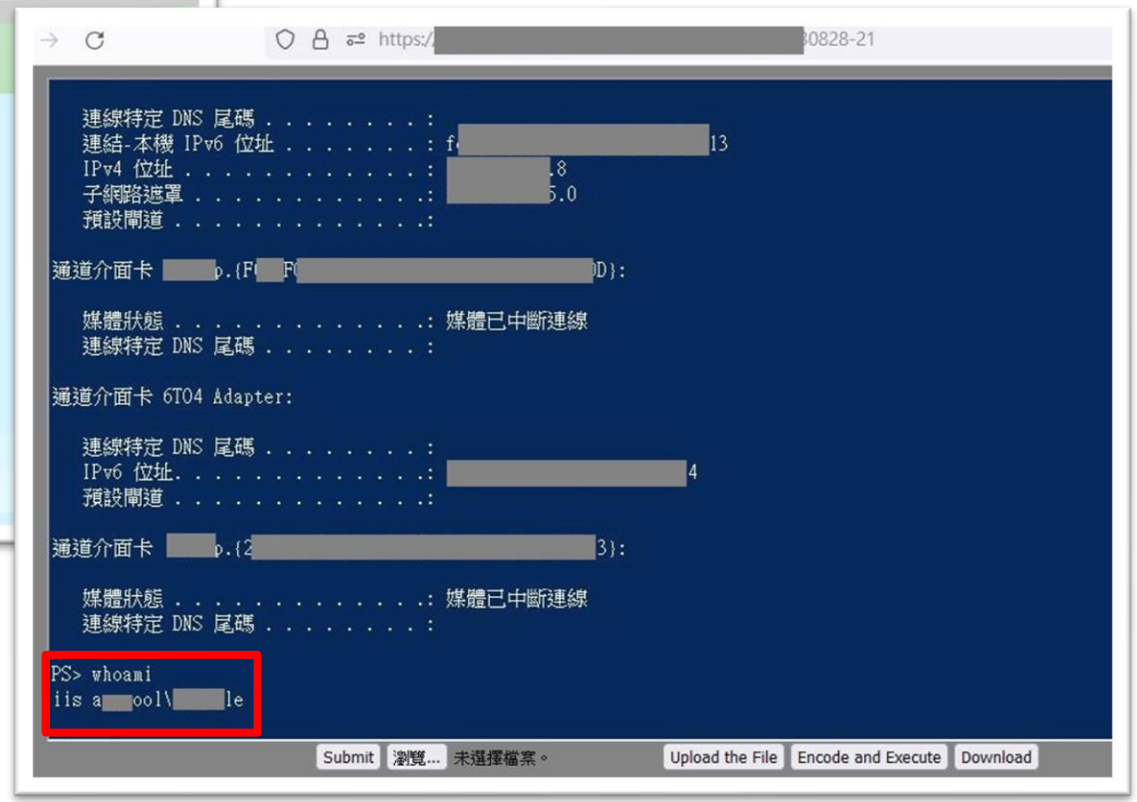


案例4 未確實限制檔案上傳類型(3/3)

國家資通安全研究院
National Institute of Cyber Security

- 點選檔案連結「111111_20230828-21.aspx.」，成功上傳Web shell，取得OS一般使用者權限





未確實限制檔案上傳類型改善建議

國家資通安全研究院
National Institute of Cyber Security

- 系統開發者
  - 針對透過網頁上傳檔案之副檔名進行嚴格限制，並於前端網頁應用程式與後端伺服器皆進行檢查，或可針對上傳檔案內容進行檢查與限制
- 系統管理者
  - 可透過網頁應用程式防火牆進行上傳檔案內容檢查，阻擋含有惡意程式之檔案上傳行為
  - Windows伺服器應安裝防毒軟體進行防護，透過即時檢查刪除惡意程式

5.帳號密碼外洩
(加密機制失效)

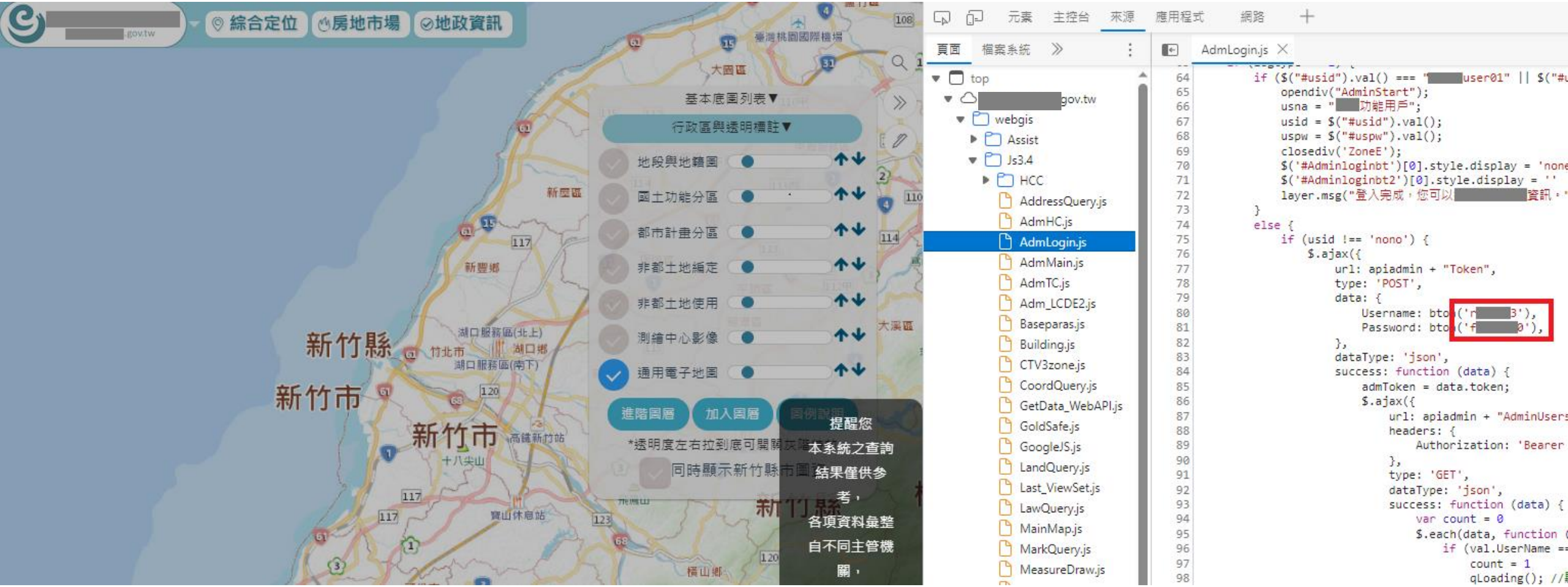
帳號密碼外洩樣態

- 於伺服器中針對密碼以明文方式或以不安全編碼方式進行儲存
- 將帳號密碼寫入網頁原始碼等容易遭外部使用者取得之位置，造成攻擊者可透過資訊蒐集取得帳號密碼

案例5-1 帳號密碼外洩(1/2)

國家資通安全研究院
National Institute of Cyber Security

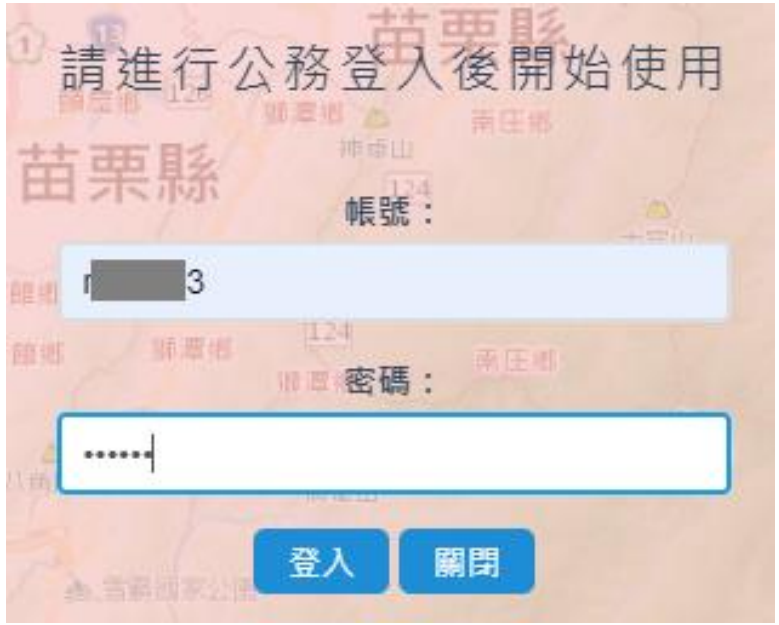
- 透過檢視網頁原始碼發現帳號密碼

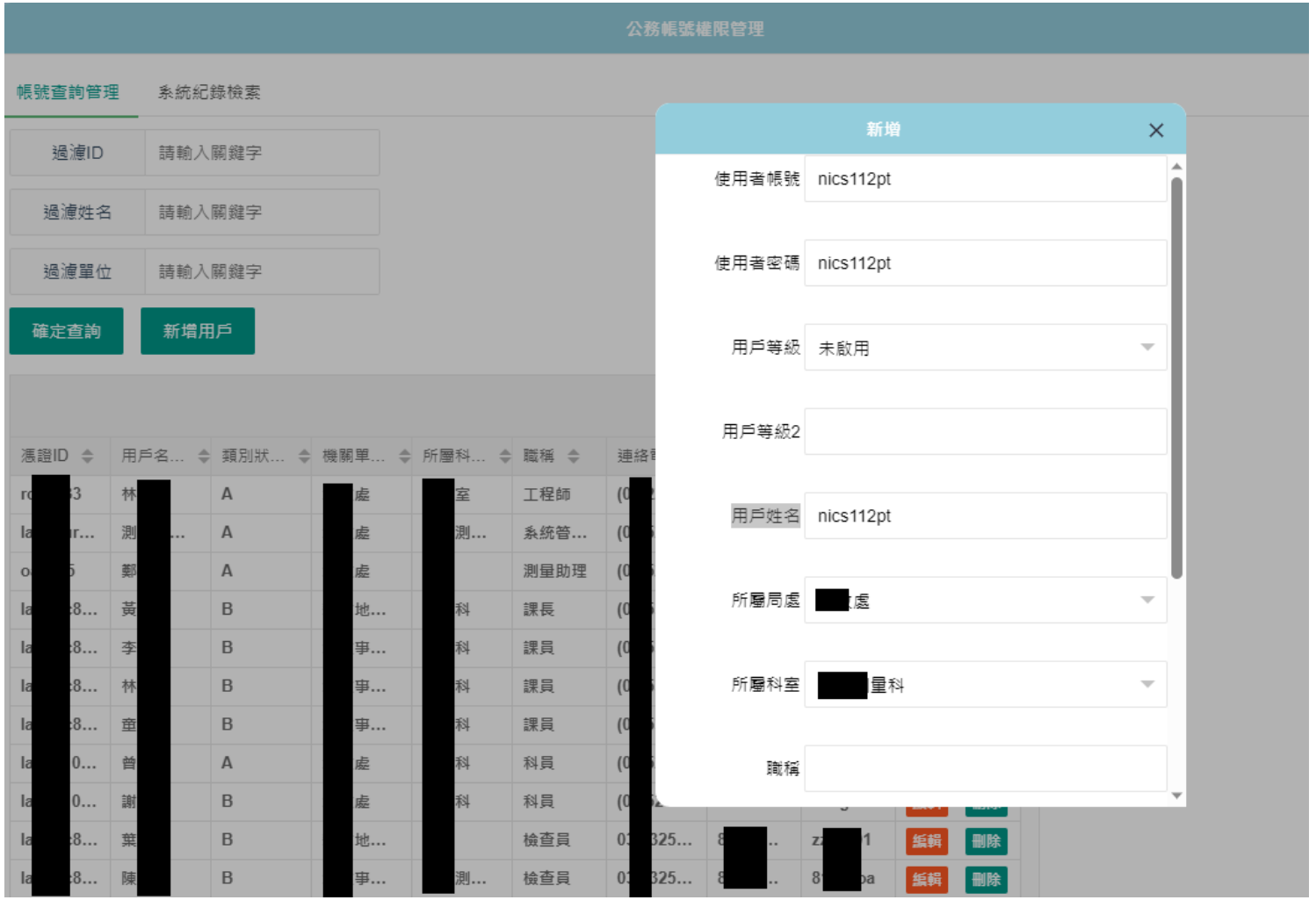


案例5-1 帳號密碼外洩(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 利用發現之帳號密碼登入網站後成功新增帳號，取得管理者權限

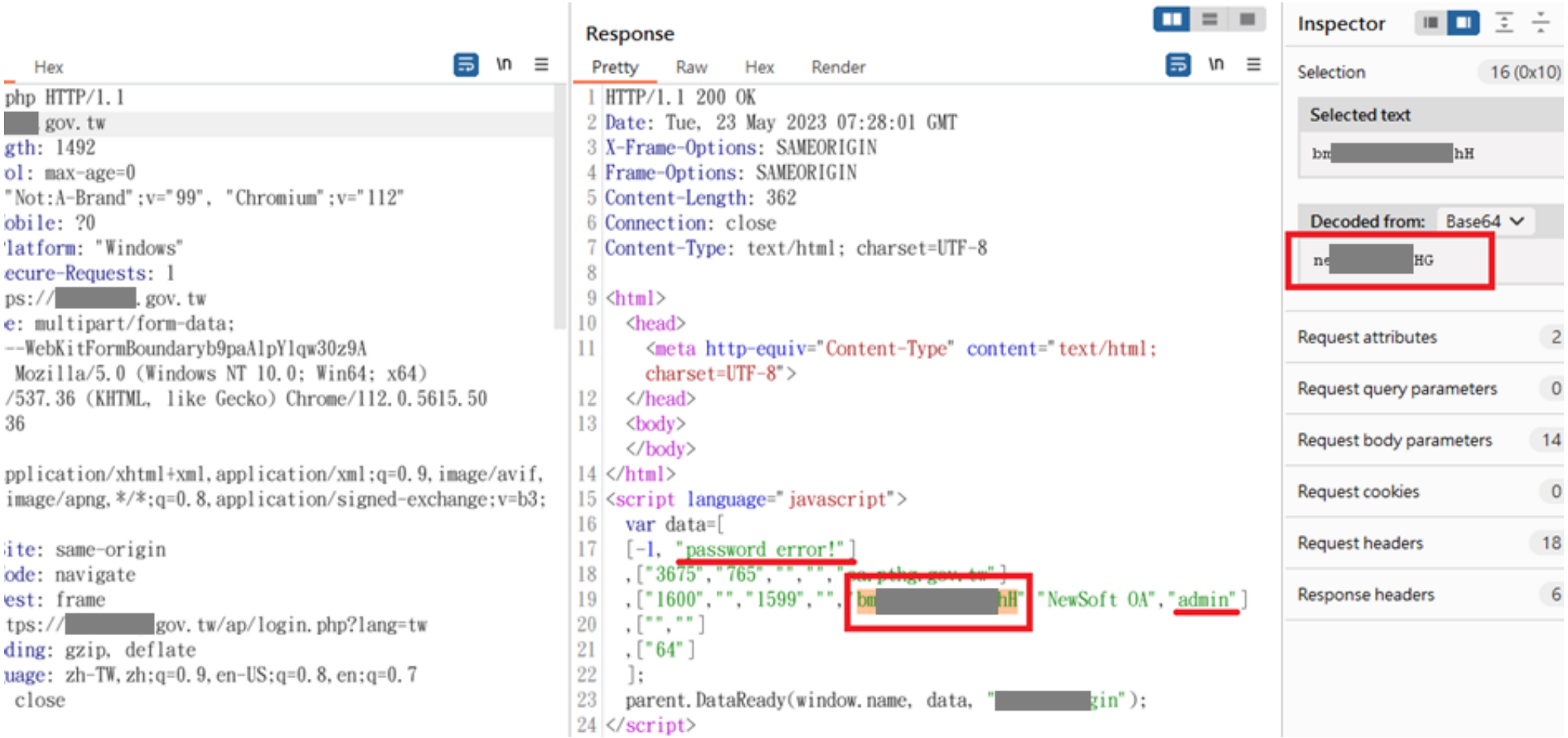




案例5-2 帳號密碼外洩(1/2)

國家資通安全研究院
National Institute of Cyber Security

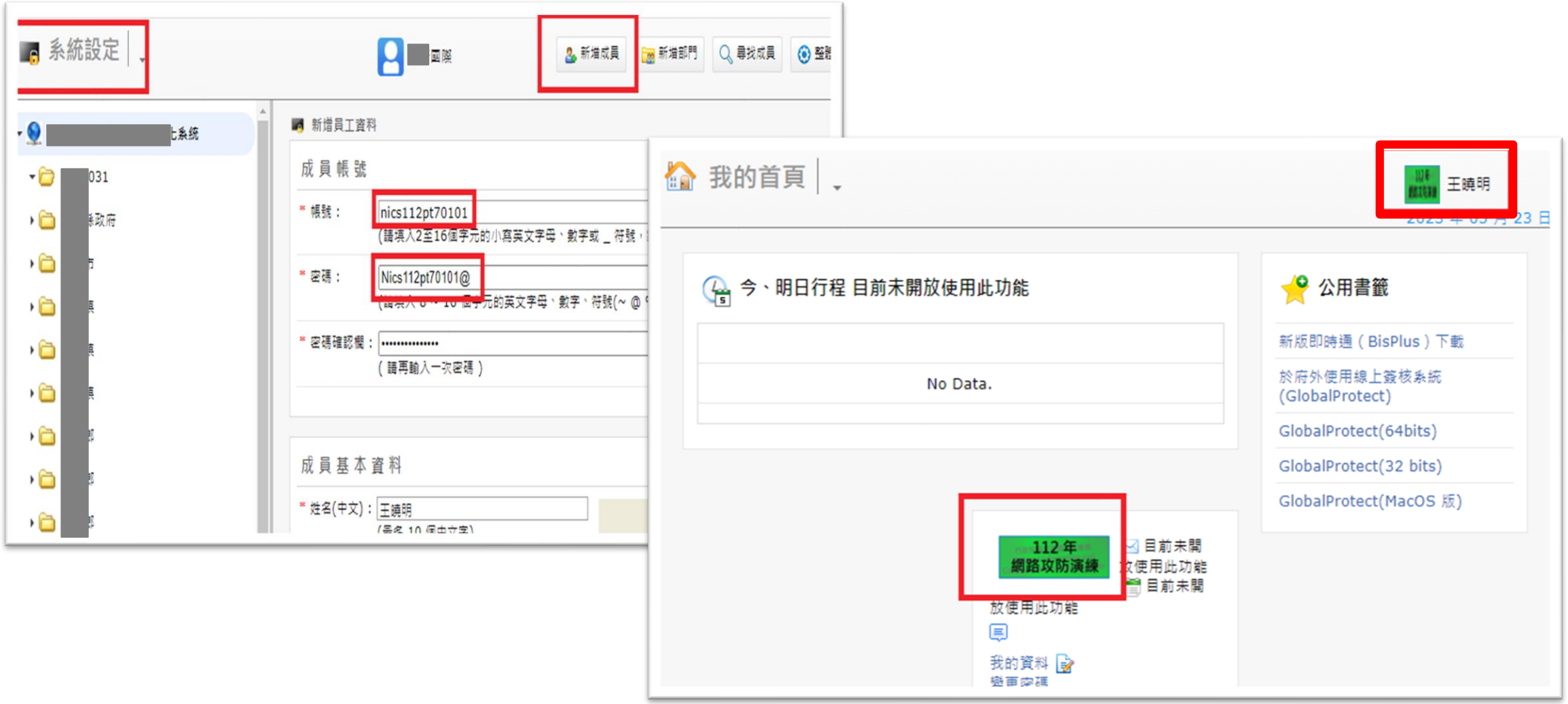
- 攻擊者使用Burp Suite工具攔截封包，查看回傳結果，發現當輸入任意錯誤密碼時，該網站會回傳正確密碼之Base64編碼結果



案例5-2 帳號密碼外洩(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 利用取得之密碼登入網站後成功新增管理者，取得管理者權限



帳號密碼外洩改善建議

國家資通安全研究院
National Institute of Cyber Security

- 系統開發者
  - 所有檢查應於伺服器端進行，僅回傳必要之檢查結果，避免將機敏資訊放入網頁回應封包當中
  - 程式開發完成應重新檢視網頁原始碼內容，避免將機敏資訊放於網頁原始碼之註解當中

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

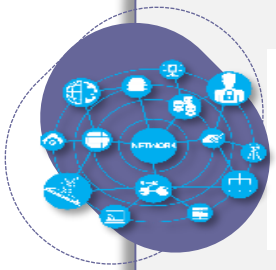
資安稽核技術檢測結果

國家資通安全研究院
National Institute of Cyber Security

使用者電腦安全檢測

- 使用者電腦弱點掃描共發現1,047個高風險與544個中風險弱點
- 使用者電腦安全防護檢測顯示電腦皆有更新病毒碼，且未發現惡意程式，惟發現46台電腦未落實安全性更新及23台電腦應用程式未更新

物聯網設備檢測



- 物聯網設備檢測結果共發現147項不符合項目，其中40.1%為「軟/韌體、作業系統及相關應用程式不得存在CVSS v3高於7分(含)之CVE漏洞」，31.3%為「管理介面身分鑑別不得使用預設帳號通行碼」

網域主機安全防護檢測

- 網域主機皆已部署與更新防毒軟體，且未發現惡意程式，惟發現8台未安裝所有安全性更新項目

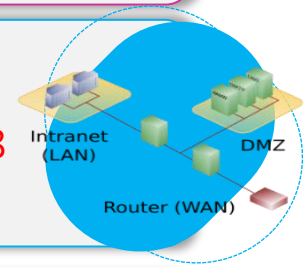
資料庫安全檢測

- 資料庫安全檢測結果共發現49項不符合項目，其中18.4%為「資料庫資料傳輸具有安全機制」，12.2% 為「啟用資料庫帳號登出/登入稽核」

核心資通系統安全檢測

- 核心資通系統內網滲透測試結果共發現75個高風險、16個中風險及24個低風險弱點，其中59.1%屬於「注入攻擊」弱點
- 核心資通系統防護基準檢測結果共發現82個不符合項目

網路架構檢測



- 網路架構檢測共發現30個高風險、50個中風險、8個低風險及12個建議項目

組態設定安全檢測

- 共發現230台使用者電腦組態設定有未符合之項目
- 共發現15台網域主機組態設定有未符合之項目
- 共發現28台網通設備組態設定有未符合之項目
- 共發現30台伺服器應用程式組態設定有未符合之項目

網路惡意活動檢視

- 共發現445筆IP與221筆DN中繼站名單未阻擋
- 皆未發現APT網路流量惡意行為

使用者電腦安全檢測共同發現事項(1/2)

國家資通安全研究院
National Institute of Cyber Security

發現事項同111年

1 電腦開啟之服務存在SSL使用安全性不足之加密演算法弱點(SWEET32)，防護強度不足有被破解風險

3 機關部分電腦仍未更新至最新，且仍存在使用停止支援之作業系統與應用程式(如Windows 7/8.1、Adobe Acrobat Reader及Flash Player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 電腦開啟之服務存在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

使用者電腦安全檢測共同發現事項(2/2)

國家資通安全研究院
National Institute of Cyber Security

改善建議

1.停止使用安全性不足之加密演算法，如DES、3DES及RC4等
2.採用更高安全性加密簽章方式，避免使用SHA1雜湊方式加密簽章
3.端點設備管理者建立安全性更新檢查機制並落實執行，以及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)

範例：修改Windows註冊檔以停止支援DES、3DES及RC4

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56" /f /v Enabled /t Reg_DWORD /d 0
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168" /f /v Enabled /t Reg_DWORD /d 0
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" /f /v Enabled /t Reg_DWORD /d 0
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128" /f /v Enabled /t Reg_DWORD /d 0
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128" /f /v Enabled /t Reg_DWORD /d 0
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128" /f /v Enabled /t Reg_DWORD /d 0
```

參考資料：https://kb.cybertecsecurity.com/knowledge/disabling-cipher-suites

物聯網設備檢測共同發現事項(1/2)

國家資通安全研究院
National Institute of Cyber Security

發現事項1與2同111年

1. 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

2. 設備之管理介面、Telnet及SNMP服務使用預設帳號通行碼，恐有資訊外洩與遭入侵疑慮

3. 設備管理介面未使用身分鑑別功能，恐有資訊外洩與遭入侵疑慮

物聯網設備

使用者

物聯網設備檢測共同發現事項(2/2)

國家資通安全研究院
National Institute of Cyber Security

改善建議

1. 常見高於7分(含)之CVE漏洞，如設備支援不安全加密演算法弱點(SWEET32)，或後台管理平台使用過舊軟體版本(如Apache Tomcat等)。建議設備管理者定期更新物聯網設備軟韌體版本，已停止支援設備應規劃汰換

2. 設備管理者應變更管理介面、Telnet及SNMP之預設帳號通行碼，關閉非必要服務，並強化存取控管，限制存取來源，例如SNMP預設之Community Name為「public」，設備管理者可透過管理介面變更為其他字串

3. 設備管理者建議啟用管理介面身分鑑別功能外，可設定通行碼複雜度與最小長度要求，以及啟用限制錯誤嘗試之機制

網域主機安全防護檢測共同發現事項

國家資通安全研究院
National Institute of Cyber Security

發現事項同111年

1 未安裝所有安全性更新項目

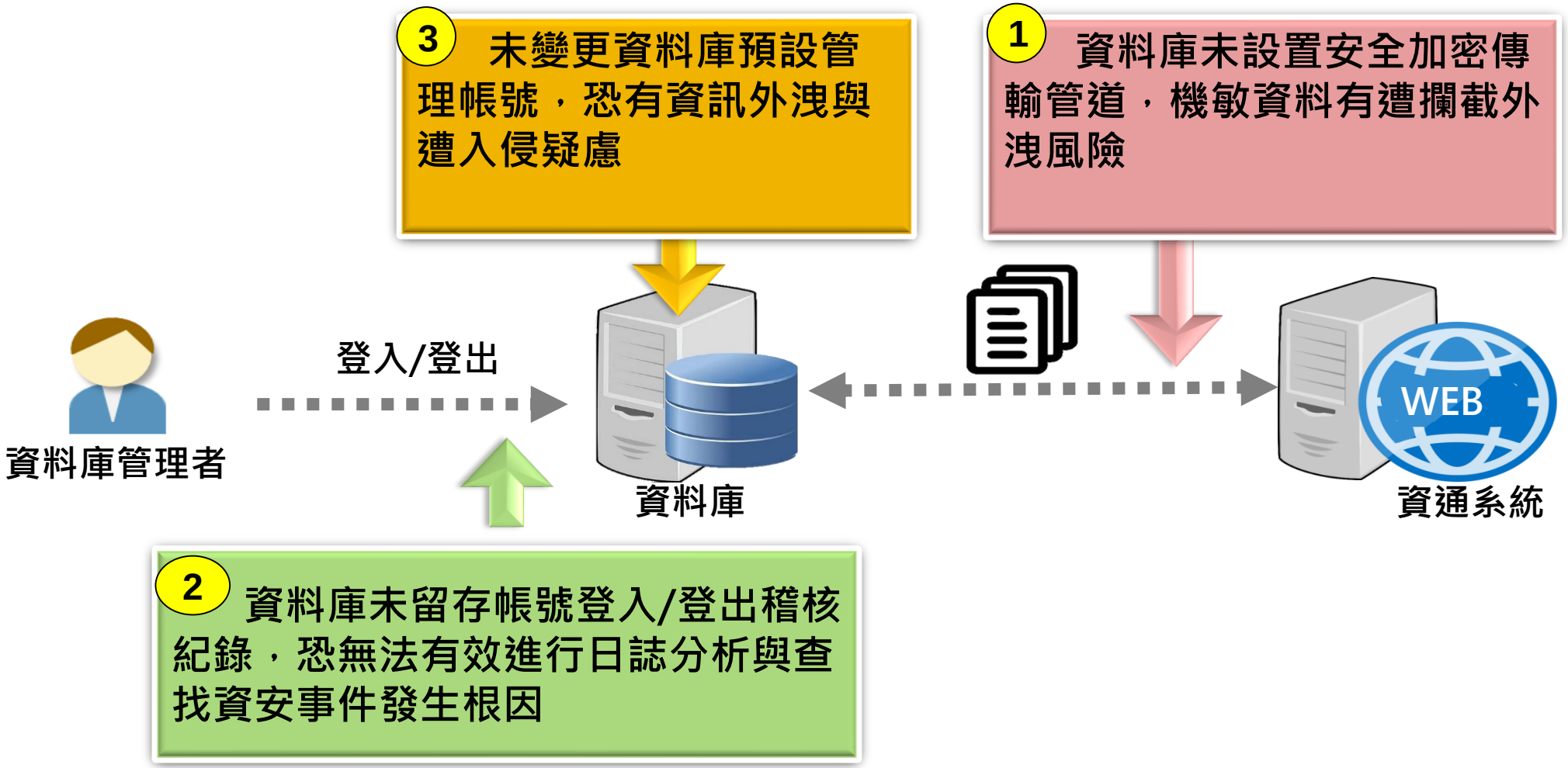
改善建議

1.重新檢視更新與確認相關機制，定期檢視網域主機更新情形，以提升防護能量

資料庫安全檢測共同發現事項(1/3)

國家資通安全研究院
National Institute of Cyber Security

發現事項1同111年



資料庫安全檢測共同發現事項(2/3)

國家資通安全研究院
National Institute of Cyber Security

改善建議

1.針對資料庫設置安全加密傳輸方式，如啟用TLS 1.2以上加密傳輸協定，以確保資料傳輸安全

2.啟用資料庫帳號登出/登入稽核，強化稽核紀錄完整性。建議啟用資料庫內建之稽核功能，或評估採購專業資料庫稽核管理工具

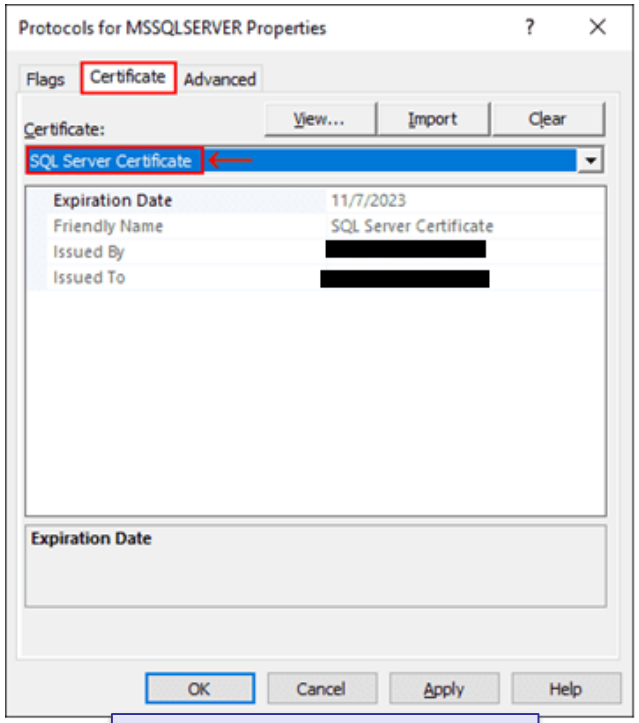
3.停用或變更資料庫預設管理帳號，降低駭客入侵風險，例如SQL Server變更預設管理帳號「SA」、Oracle變更預設管理帳號「SYSTEM」

資料庫安全檢測共同發現事項(3/3)

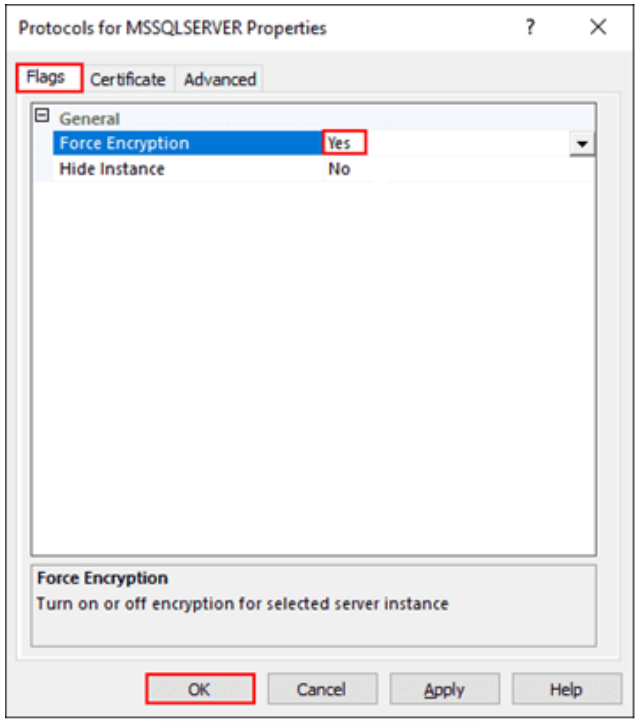
國家資通安全研究院
National Institute of Cyber Security

實作範例

- SQL Server 啟用TLS加密傳輸

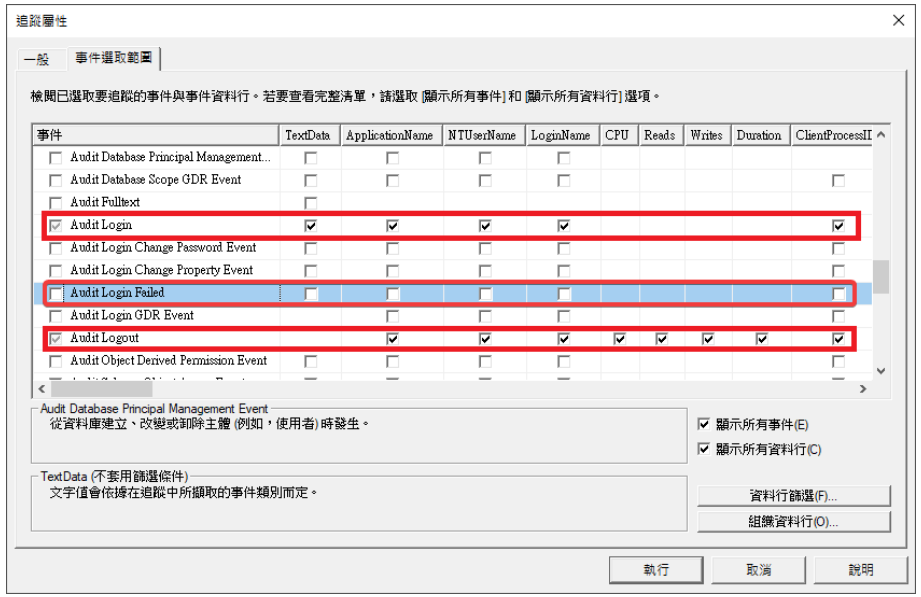


綁定站台加密憑證



設定強制加密

- SQL Server Profiler 啟用登入/登出稽核



- Audit Login
- Audit Login Failed
- Audit Logout

參考資料：https://learn.microsoft.com/zh-tw/mem/configmgr/core/plan-design/security/enable-tls-1-2-server

核心資通系統內網滲透測試共同發現事項(1/2)

國家資通安全研究院
National Institute of Cyber Security

發現事項1同111年

2 資通系統存在無效的存取控管弱點，使用者可跨權限存取非授權之資料

資通系統主機

3 資通系統存在不安全的組態設定弱點，恐有資訊外洩與遭入侵疑慮

1 系統存在注入攻擊弱點，使用者可輸入惡意指令並當成SQL語句執行，取得資料庫機敏資料，或利用JavaScript語法撰寫惡意程式，竊取使用者Cookie中機敏資料或將使用者自動引導至釣魚網站

核心資通系統內網滲透測試共同發現事項(2/2)

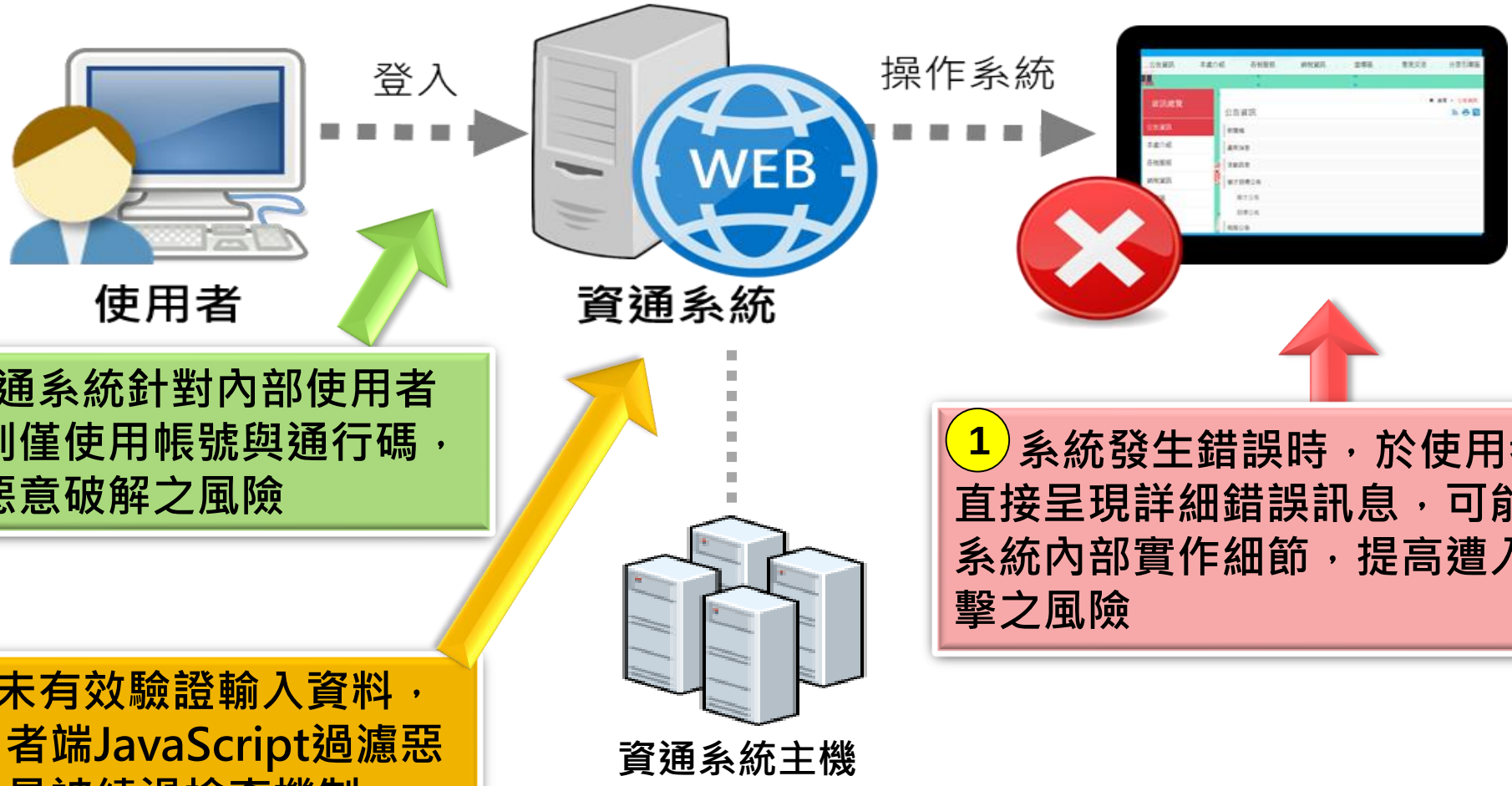
改善建議

1. 系統開發者對所有功能頁面過濾可能造成危害之符號及標籤輸入，或僅允許輸入特定格式語法。伺服器端網頁程式需對所有接收參數進行過濾或取代，例如僅能輸入數字型態之資料或者過濾或取代「= + - @」等符號，或限制使用者輸入任何與活頁簿相關語法等字眼

2. 應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。系統維運者依最小權限原則定期審查使用者權限

3. 確認系統安全組態設定之完整性與有效性，如移除非必要性預設頁面或限制頁面存取來源等

核心資通系統防護基準檢測共同發現事項(1/2)



2 高等級資通系統針對內部使用者之識別與鑑別僅使用帳號與通行碼，存在帳號被惡意破解之風險

1 系統發生錯誤時，於使用者頁面直接呈現詳細錯誤訊息，可能洩露系統內部實作細節，提高遭入侵攻擊之風險

3 資通系統未有效驗證輸入資料，或僅依賴使用者端JavaScript過濾惡意輸入字元，易被繞過檢查機制

核心資通系統防護基準檢測共同發現事項(2/2)

改善建議

1.實作客製化錯誤頁面，僅顯示簡短錯誤訊息及代碼，不可顯示程式碼錯誤堆疊等詳細訊息

2.對資通系統之存取採取多重認證技術，如使用帳號通行碼與OTP等

3.對使用者輸入資料，於應用系統伺服器端進行合法性檢查，例如建立白名單限制允許字元(防護效果較佳)或利用黑名單過濾惡意字元(可能會有漏網之魚)，且勿依賴使用者端之JavaScript檢查邏輯，避免被輕易繞過

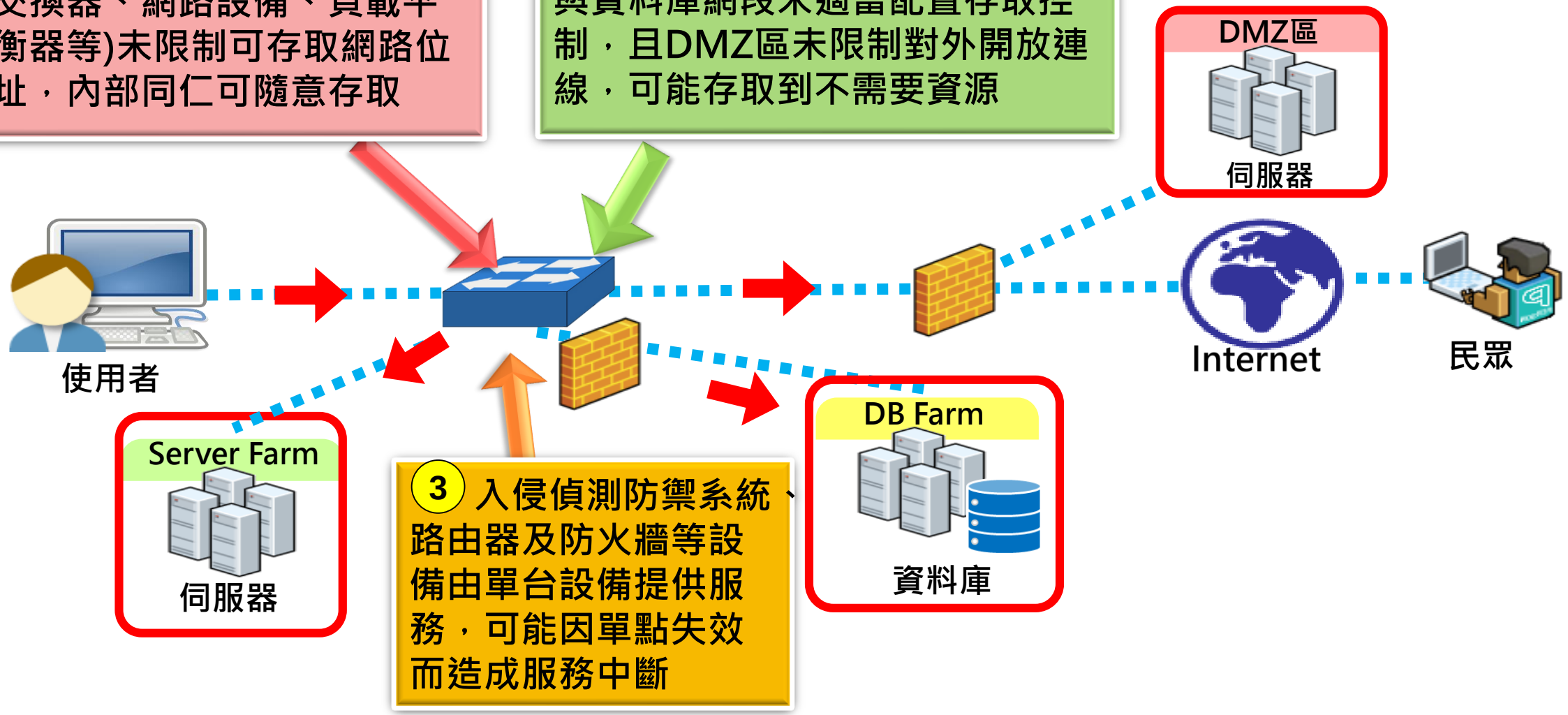
網路架構檢測共同發現事項(1/2)

國家資通安全研究院
National Institute of Cyber Security

發現事項1與2同111年

1 設備管理介面(如防火牆、交換器、網路設備、負載平衡器等)未限制可存取網路位址，內部同仁可隨意存取

2 機關使用者網段至伺服器網段與資料庫網段未適當配置存取控制，且DMZ區未限制對外開放連線，可能存取到不需要資源



3 入侵偵測防禦系統、路由器及防火牆等設備由單台設備提供服務，可能因單點失效而造成服務中斷

網路架構檢測共同發現事項(2/2)

國家資通安全研究院
National Institute of Cyber Security

改善建議

1.針對網路設備存取控制，建議設備管理者限制僅管理人員之IP可存取管理介面，避免非必要同仁連線至網路設備或將網路設備放置於獨立網段

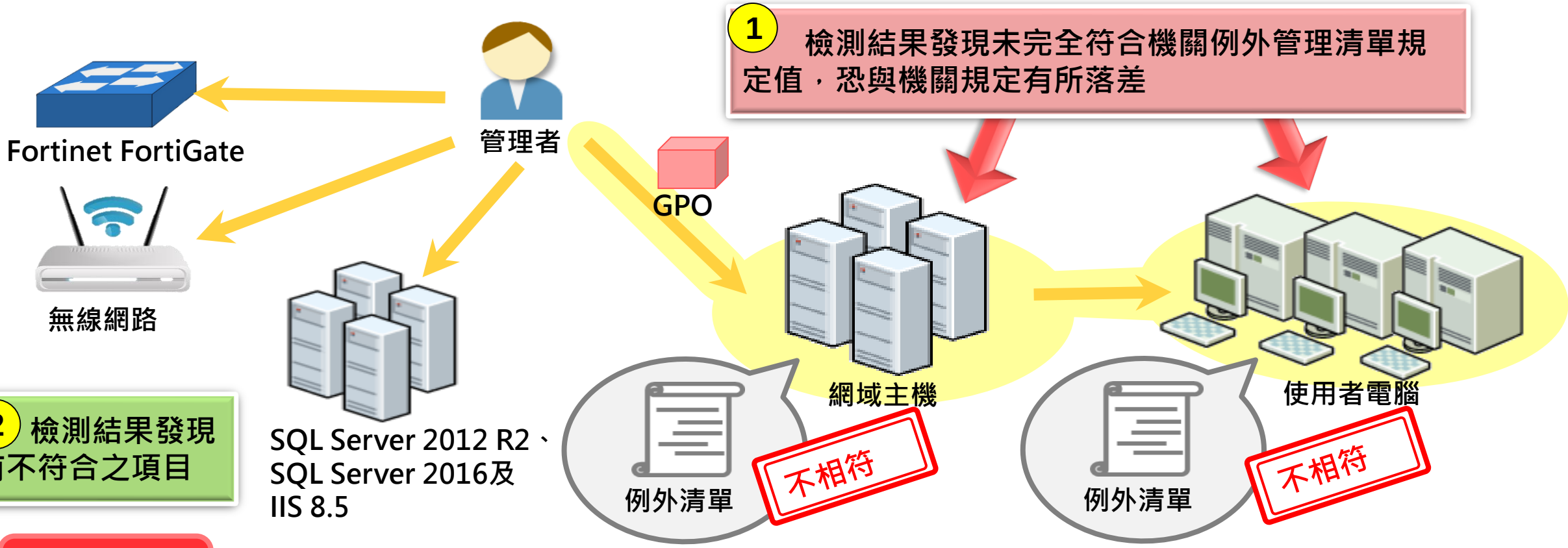
2.針對網路區域間之存取，建議網管人員重新檢視防火牆，依需求設定防火牆規則，並建立防火牆規則定期檢查機制，確認防火牆規則之合適性

3.建議核心設備(如防火牆、核心交換器及入侵偵測防禦系統等)可建立自動備援機制，提高服務可用性

組態設定安全檢測共同發現事項

國家資通安全研究院
National Institute of Cyber Security

發現事項同111年



改善建議

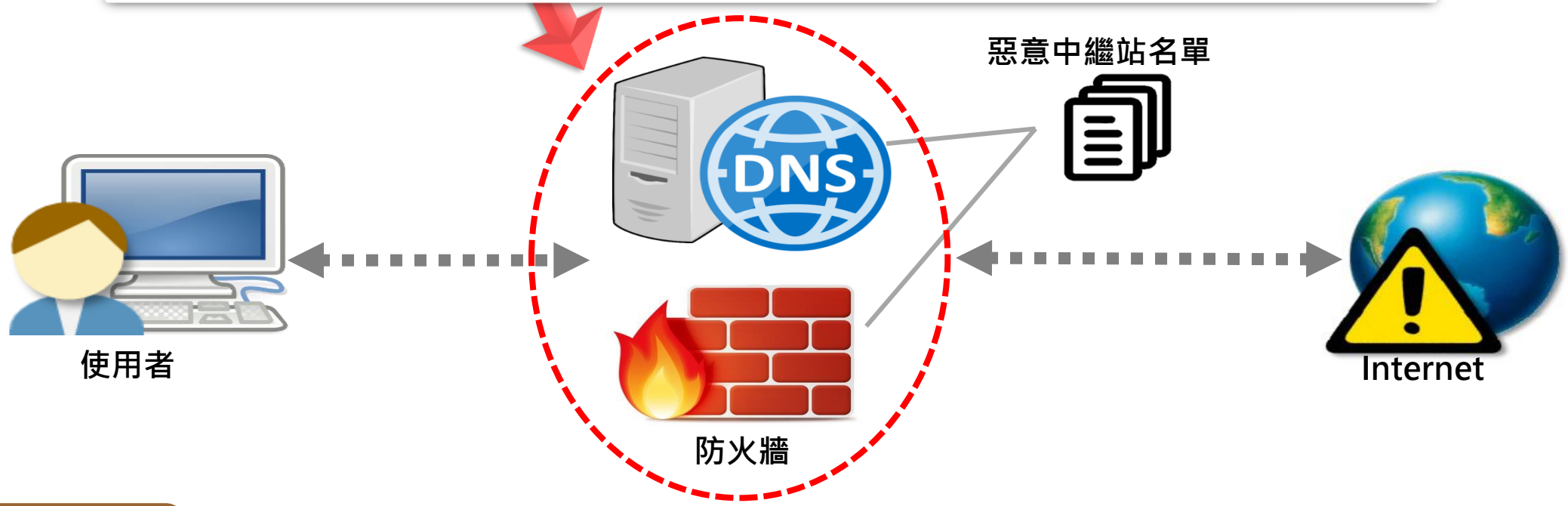
1. GCB導入人員定期審查例外管理清單正確性，確保例外項目設定值符合機關管理現況
2. GCB導入人員定期檢視部署情形，並抽檢組態設定內容，以確保組態設定正確性

網路惡意活動檢視共同發現事項

國家資通安全研究院
National Institute of Cyber Security

發現事項同111年

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. 網管人員應建立惡意中繼站名單部署與更新機制，並落實執行
2. 網管人員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

大綱

國家資通安全研究院
National Institute of Cyber Security

- 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，並於登入頁面加入驗證碼機制
- 落實執行安全性更新
  - 資通系統與物聯網設備之軟/韌體、作業系統及相關應用程式，應定期進行安全性更新，避免因版本過舊存在可利用之漏洞
- 強化使用者輸入內容檢查
  - 針對資通系統中所有使用者可輸入之欄位與上傳檔案等相關功能，應強化內容檢查，以防範惡意語法與檔案所造成之危害
- 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
- 落實部署政府組態基準
  - 除定期審查例外管理清單正確性，以及確保例外項目設定值符合機關管理規定外，建議建立部署結果檢查機制，確保組態設定正確性

國家資通安全研究院
National Institute of Cyber Security

報告完畢 敬請指教