109年網路攻防演練暨資安檢測重要發現事項

行政院國家資通安全會報技術服務中心

109年12月

大綱

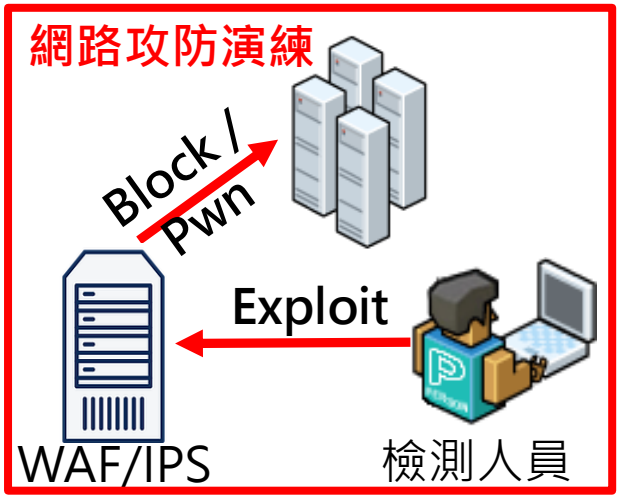
- 前言
- 網路攻防演練發現與建議
- 資安檢測發現與建議
- 結論與建議

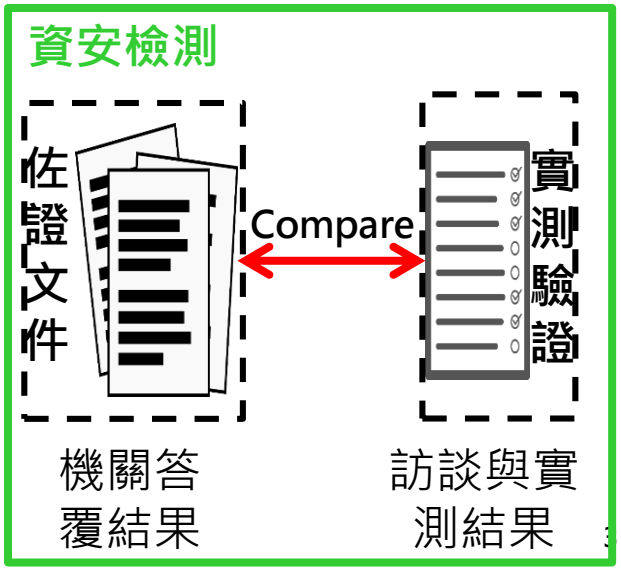
大綱

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

前言

- 技服中心持續透過網路攻防演練與資安檢測，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，109年以核心資料庫技術檢測為重點，檢測項目包含資料庫安全、網路安全、系統安全及主機安全等防護作為



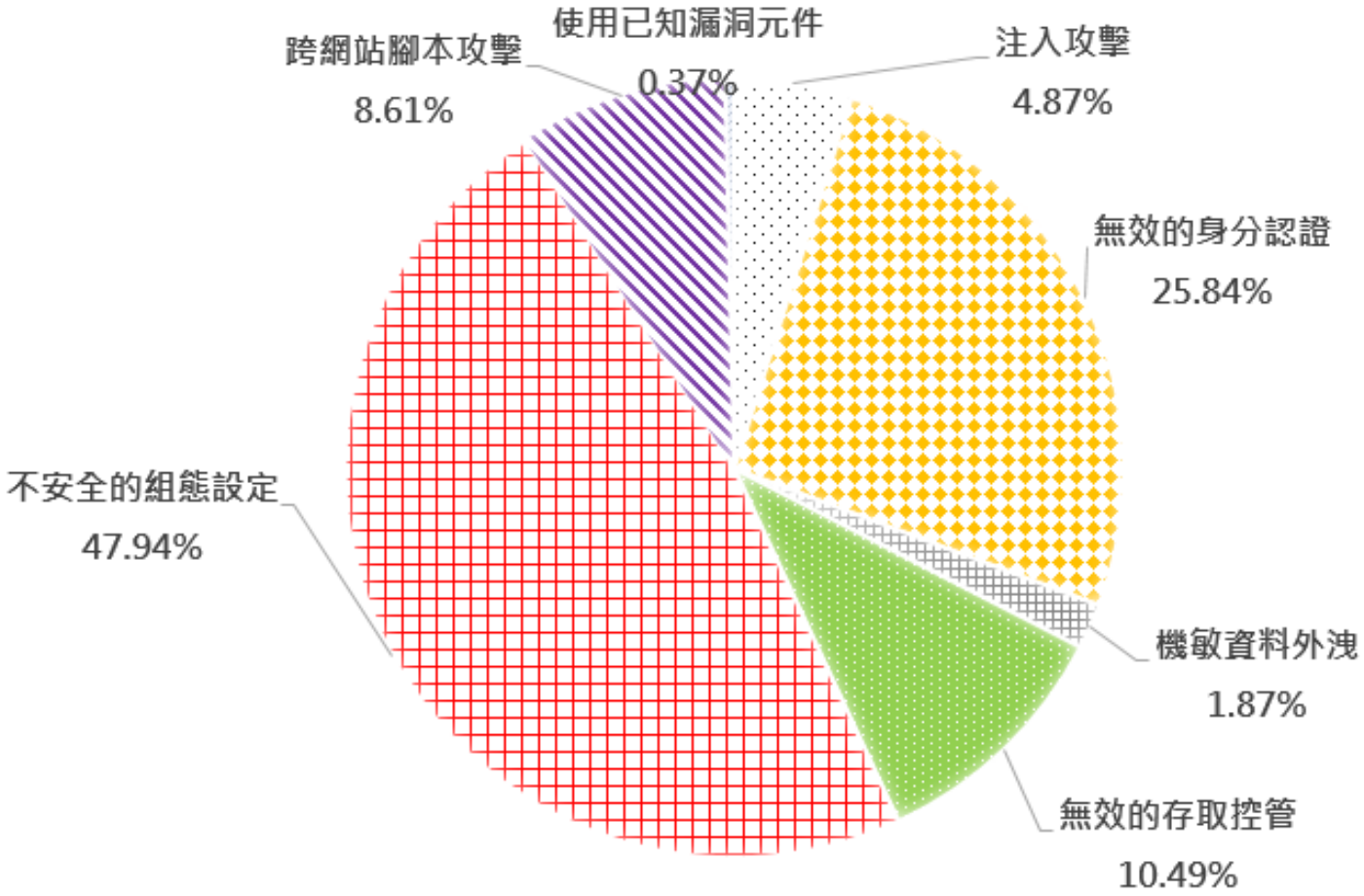


大綱

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

網路攻防演練弱點類型分布

- 綜整109年網路攻防演練攻擊紀錄，其中不安全的組態設定與無效的身分認證筆數比例最高



網路攻防演練綜合發現

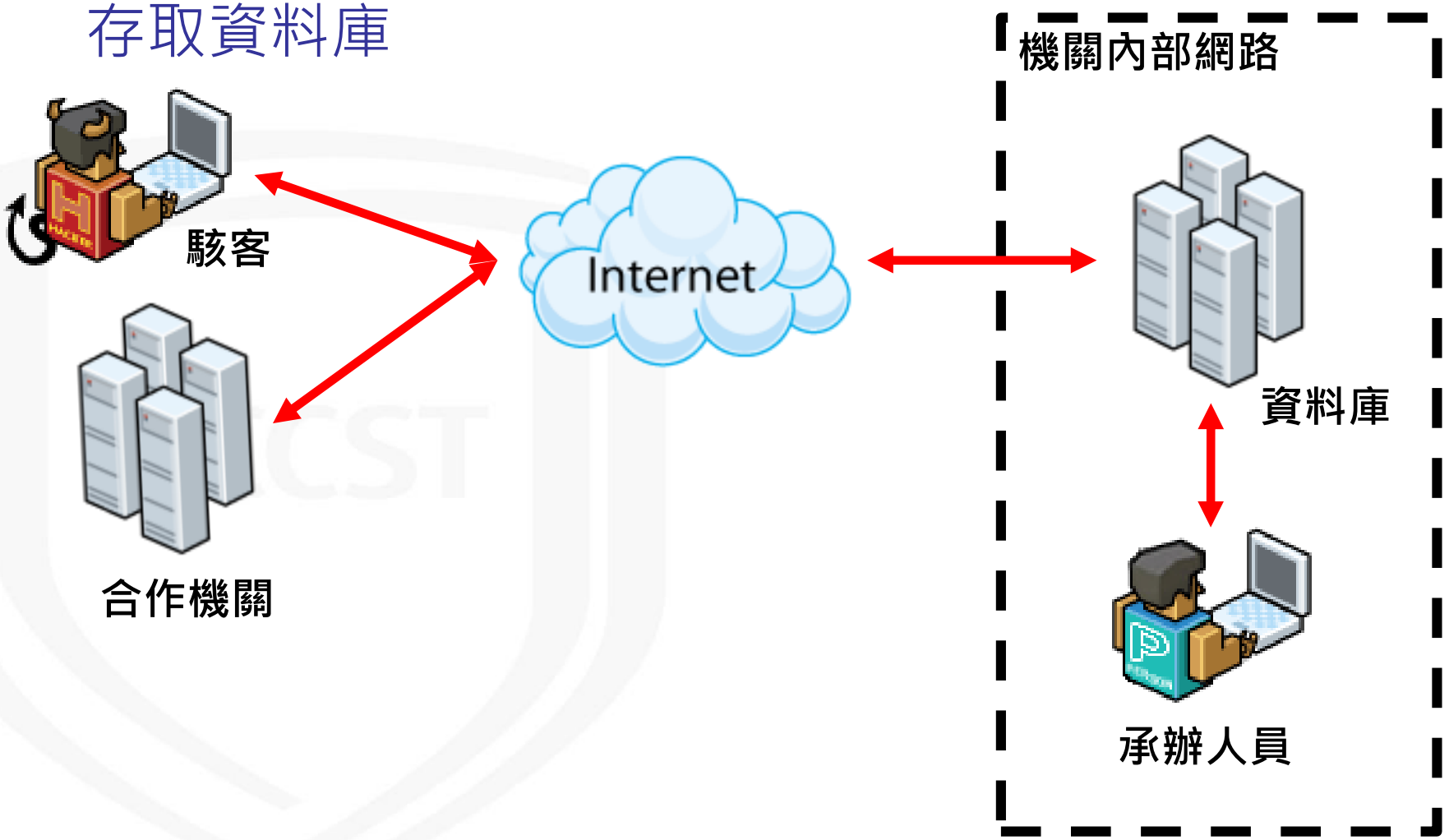
- 歸納上述弱點類型，其根因可彙整為下列4項，建議參考以下7個案例介紹，清查機關潛在弱點

項次	發現事項	案例
1	資料庫未限縮存取來源	案例1
2	上線前未落實安全設定檢查	案例2-1至2-3
3	公開預設帳號與通行碼原則	案例3
4	未落實權限檢查	案例4-1至4-2

1.資料庫未限縮存取來源

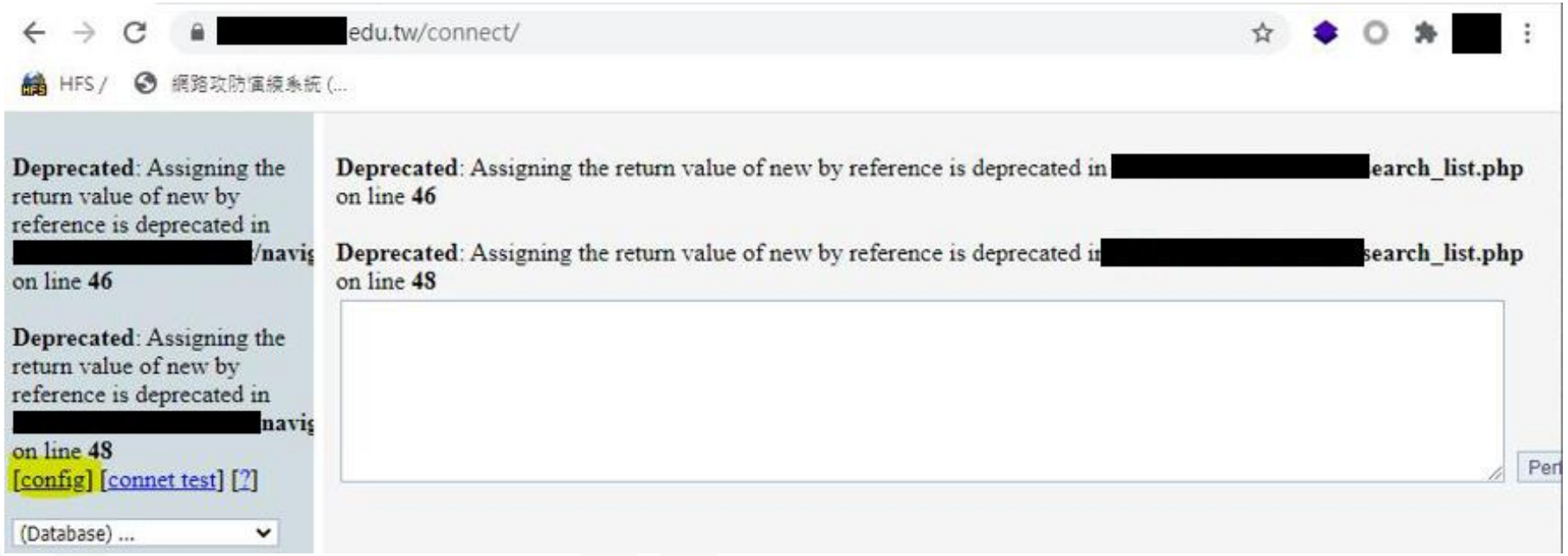
資料庫未限縮存取來源樣態

- 取得明文資料庫連線設定，且允許外網來源直接存取資料庫



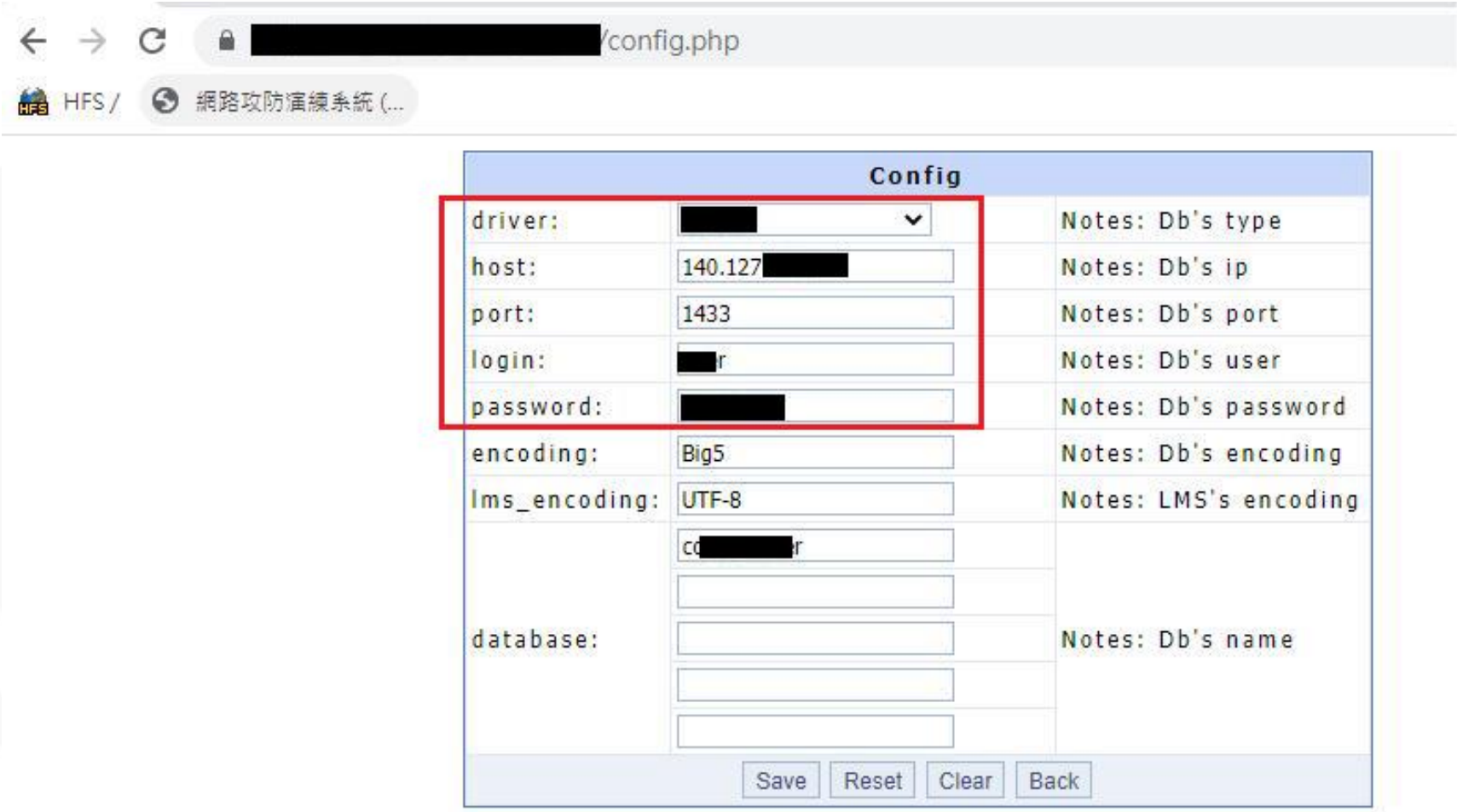
案例1 暴露連線設定(1/3)

- 攻擊手嘗試對路徑進行列舉，發現除顯示錯誤外，左下角另有config連結



案例1 暴露連線設定(2/3)

- 發現該連結存有資料庫連線設定與明文密碼



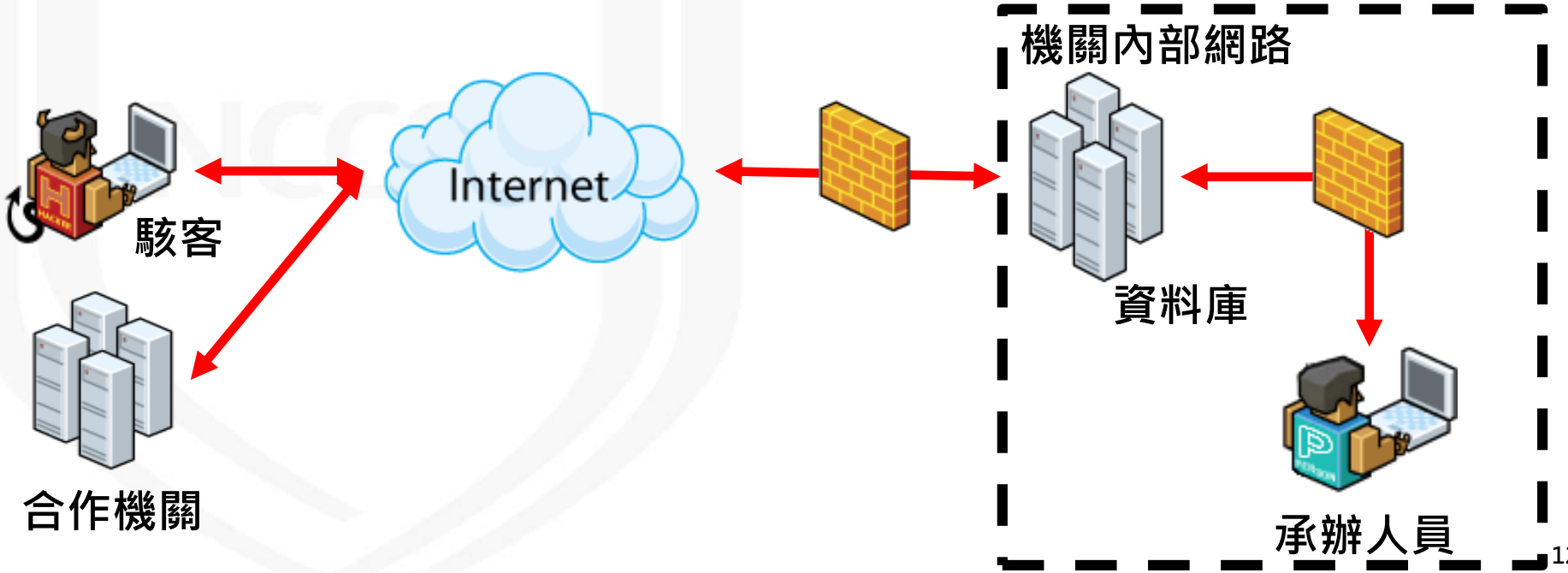
案例1 暴露連線設定(3/3)

- 成功遠端連線至該資料庫

```
[14:09:26] [INFO] connection to Sybase server '140.127          ' established
[14:09:26] [INFO] testing
[14:09:26] [INFO] confirming
[14:09:26] [INFO] resumed: [['1']]...
[14:09:26] [INFO] the back-end DBMS is
back-end DBMS: Sybase
[14:09:26] [INFO] fetching database names
[14:09:26] [INFO] fetching number of distinct values for column 'n  e'
[14:09:27] [INFO] using column 'name' as a pivot for retrieving row data
available databases [38]:
[*]          ll
[*]          hrd
[*]          ca
[*]          y
[*]          yc
[*]          gpa
[*]          je
[*]          akka
[*]          c
[*]          lc
[*]          sngccu
[*]          lc
[*]          nservice
[*]          h
[*]          l
[*]          m
```

資料庫未限縮存取來源改善建議

- 資料庫應控管於內部網段，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SA等高權限帳號進行登入及執行AP程式，其餘帳號亦須限縮存取範圍



2.上線前未落實安全設定檢查

上線前未落實安全設定檢查樣態

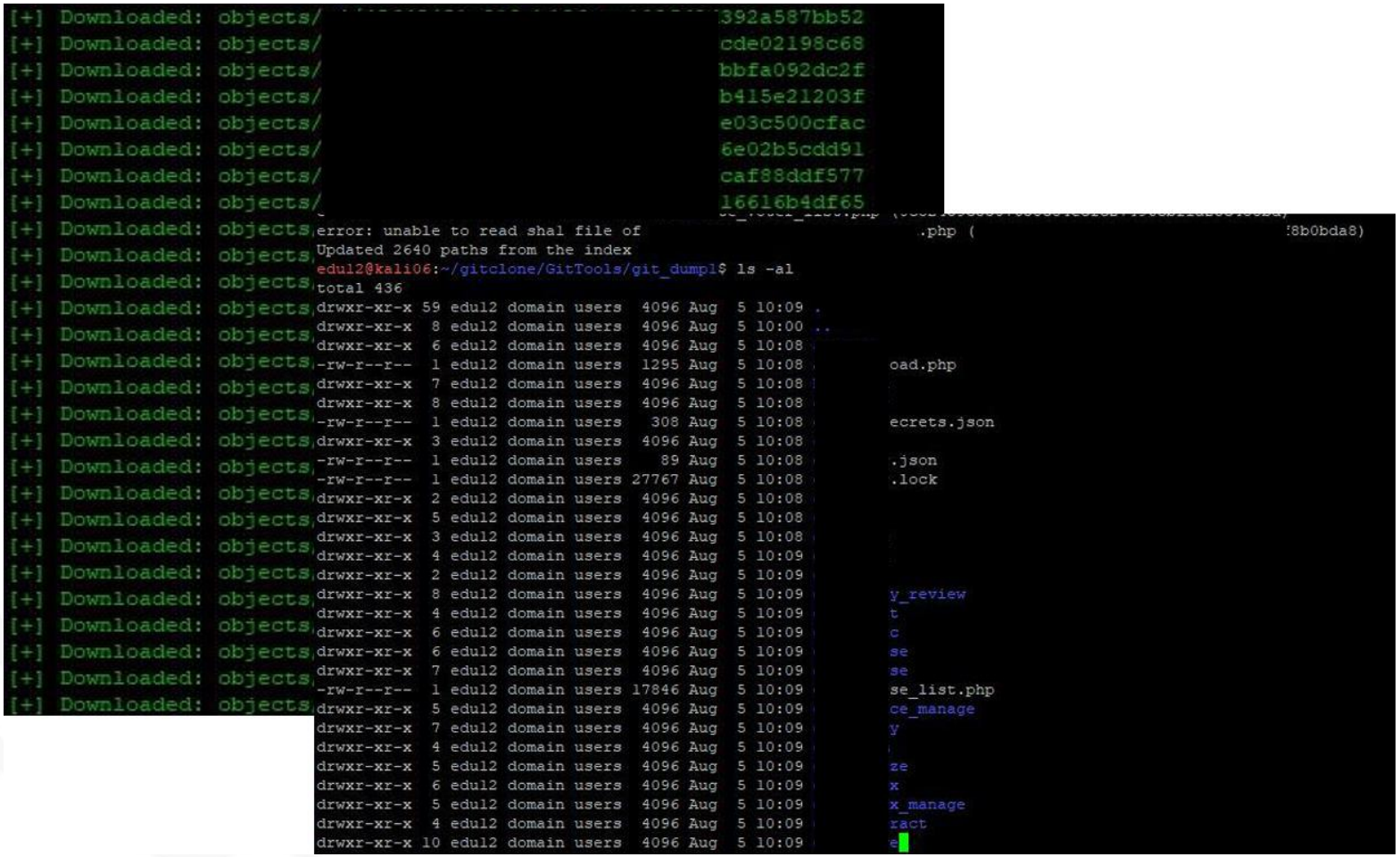
- 正式系統保有Git版控資訊，卻未有存取控制，因而可下載網站原始碼，取得資料庫設定或API金鑰
- 未清查設備既有預設帳號與通行碼，導致仍可成功登入低權限帳號，進而暴露防火牆規則
- 使用第三方套件卻未控管後台權限，駭客無需帳密即可上傳檔案至網站公開頁面

案例2-1 未限縮Git目錄存取(1/3)

- 攻擊手進行路徑猜測與列舉，確認.git相關路徑存在且可存取

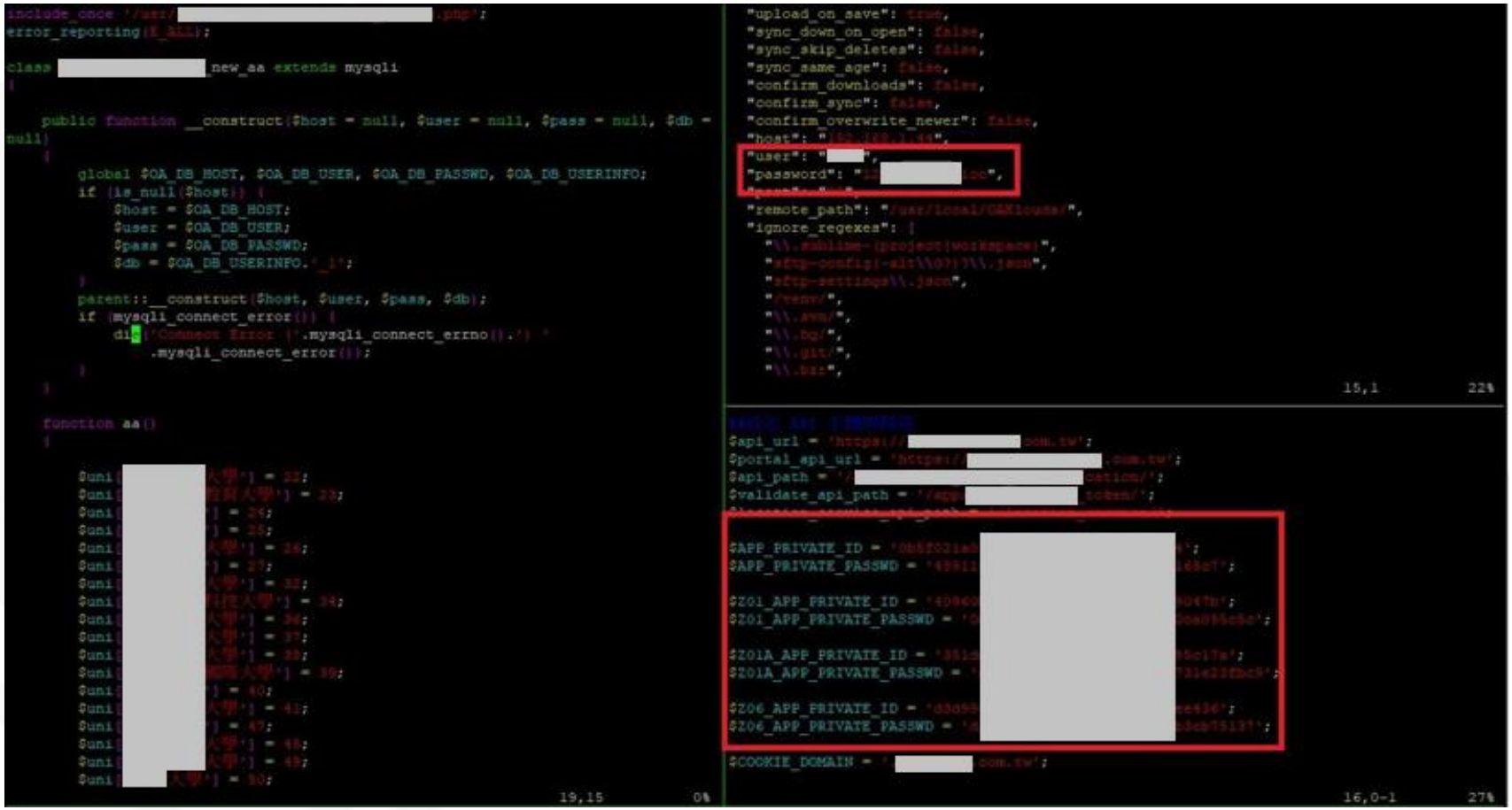
案例2-1 未限縮Git目錄存取(2/3)

- 接著透過GitHack或gitdumper等工具，進行網站原始碼打包下載與還原



案例2-1 未限縮Git目錄存取(3/3)

- 透過檢視網站程式碼，取得DB連線設定檔與API控制金鑰等資訊，網站程式碼亦可用於源碼分析

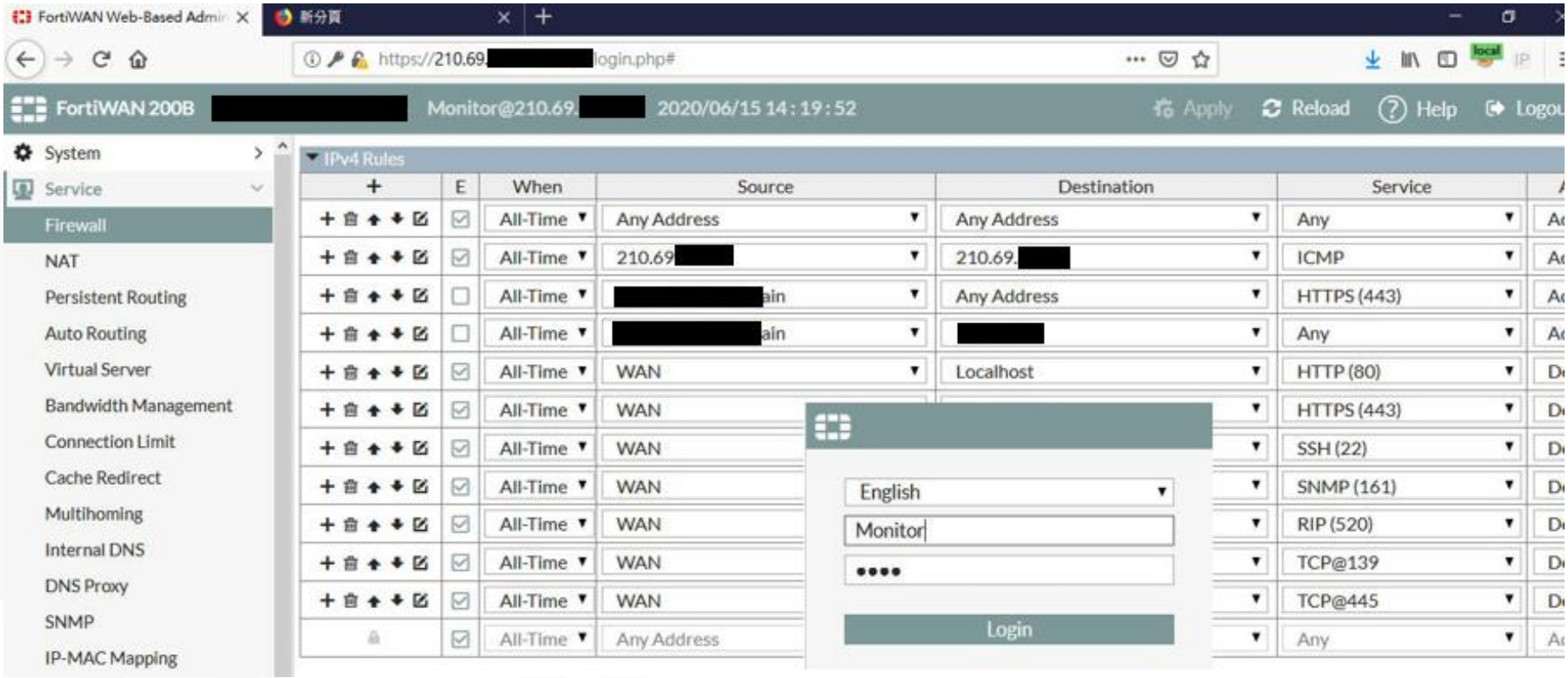


案例2-2 未修改預設通行碼(1/2)

- 攻擊手發現某防火牆可被連線，透過Google搜尋預設密碼，得知Administrator/1234與Monitor/5678兩組預設密碼

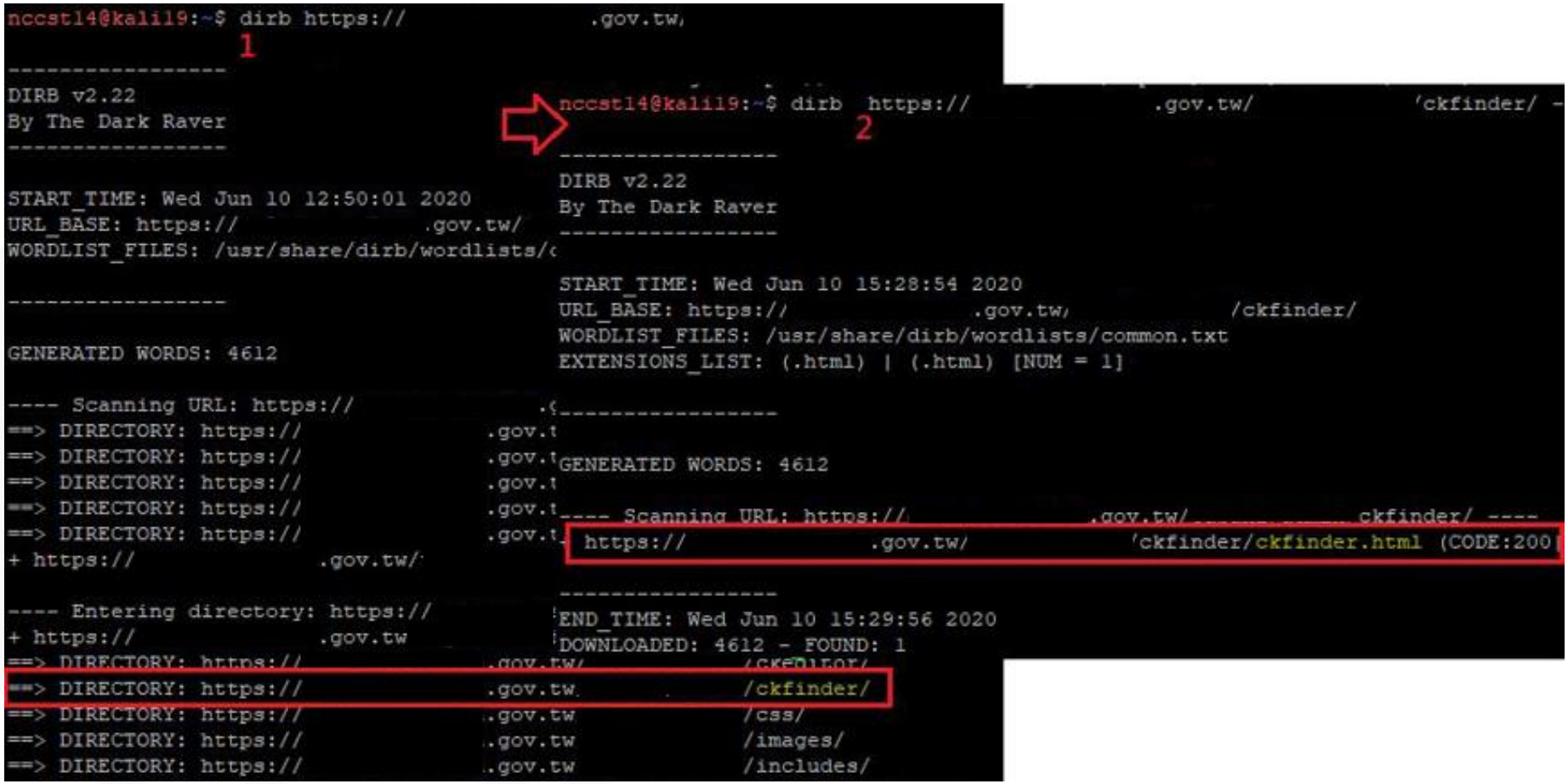
案例2-2 未修改預設通行碼(2/2)

- 嘗試使用預設帳號密碼(Monitor/5678)進行登入，發現可成功登入設備並取得防火牆規則設定



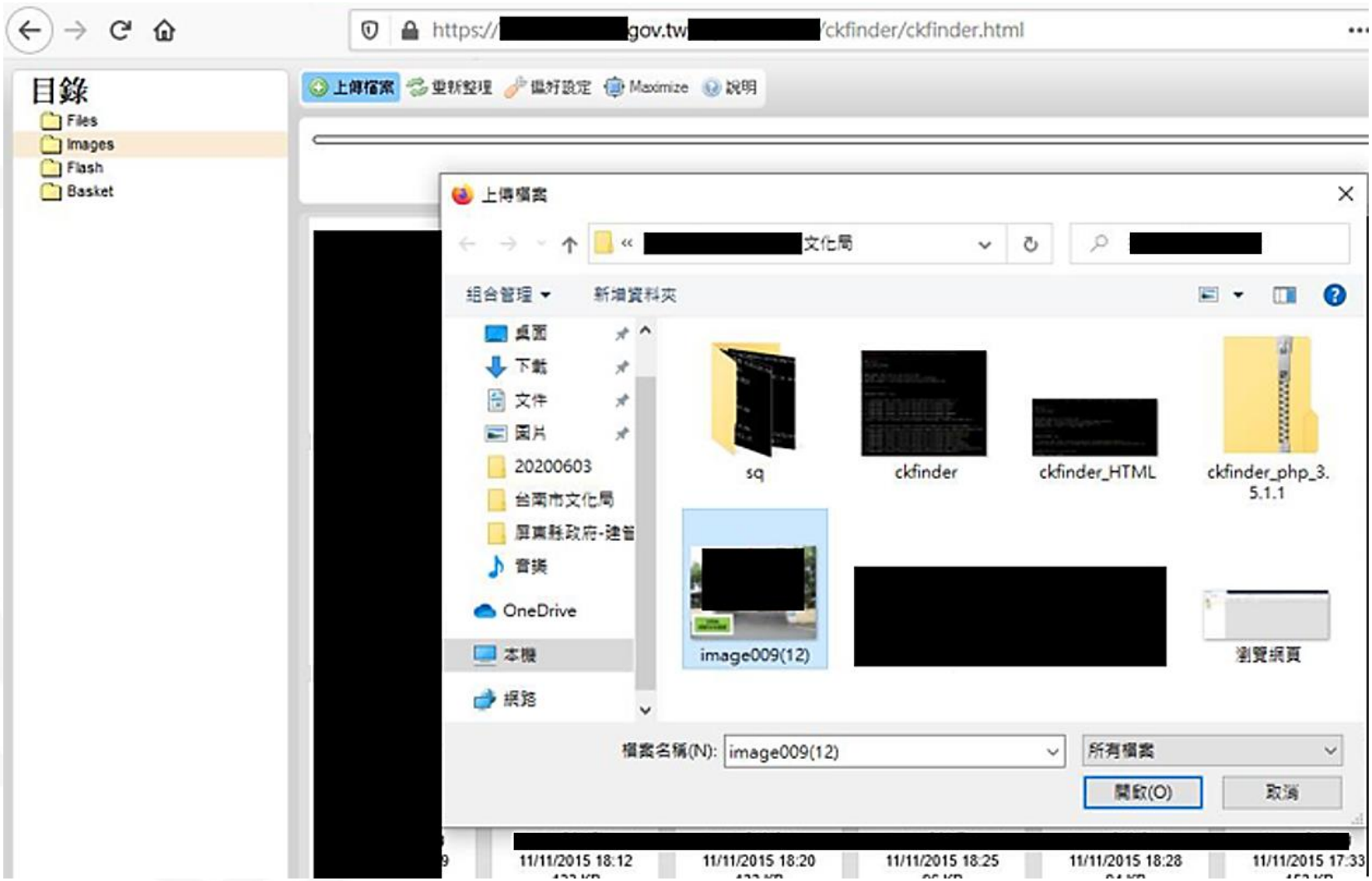
案例2-3 未限縮後台存取權限(1/3)

- 攻擊手利用掃描目錄發現存在ckfinder.html檔案



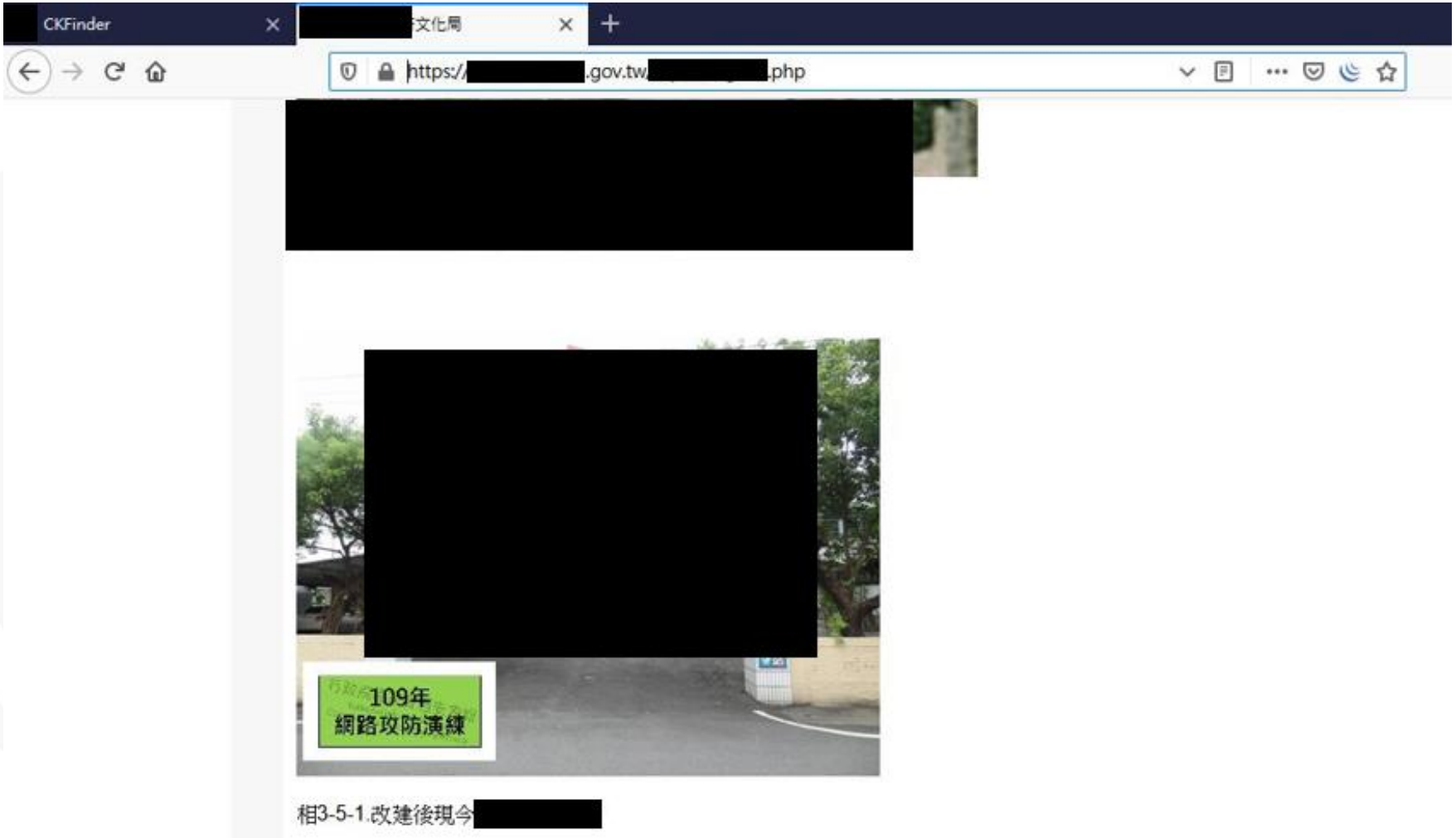
案例2-3 未限縮後台存取權限(2/3)

- 上傳經過修改的圖片



案例2-3 未限縮後台存取權限(3/3)

- 成功修改公開資料



上線前未落實安全設定檢查改善建議

- 建議訂定上線前檢查程序，將開發期間可能因測試而啟用之機制逐一確認關閉或修正
  - 變更預設帳號/測試帳號/管理者帳號等通行碼
  - 停用除錯模式與目錄瀏覽模式
  - 確認版控資訊與第三方套件完成安全設定
  - 系統操作手冊確實遮蔽帳號與網頁路徑等資訊
  - 弱點掃描/源碼檢測/滲透測試之弱點完成修補與複測

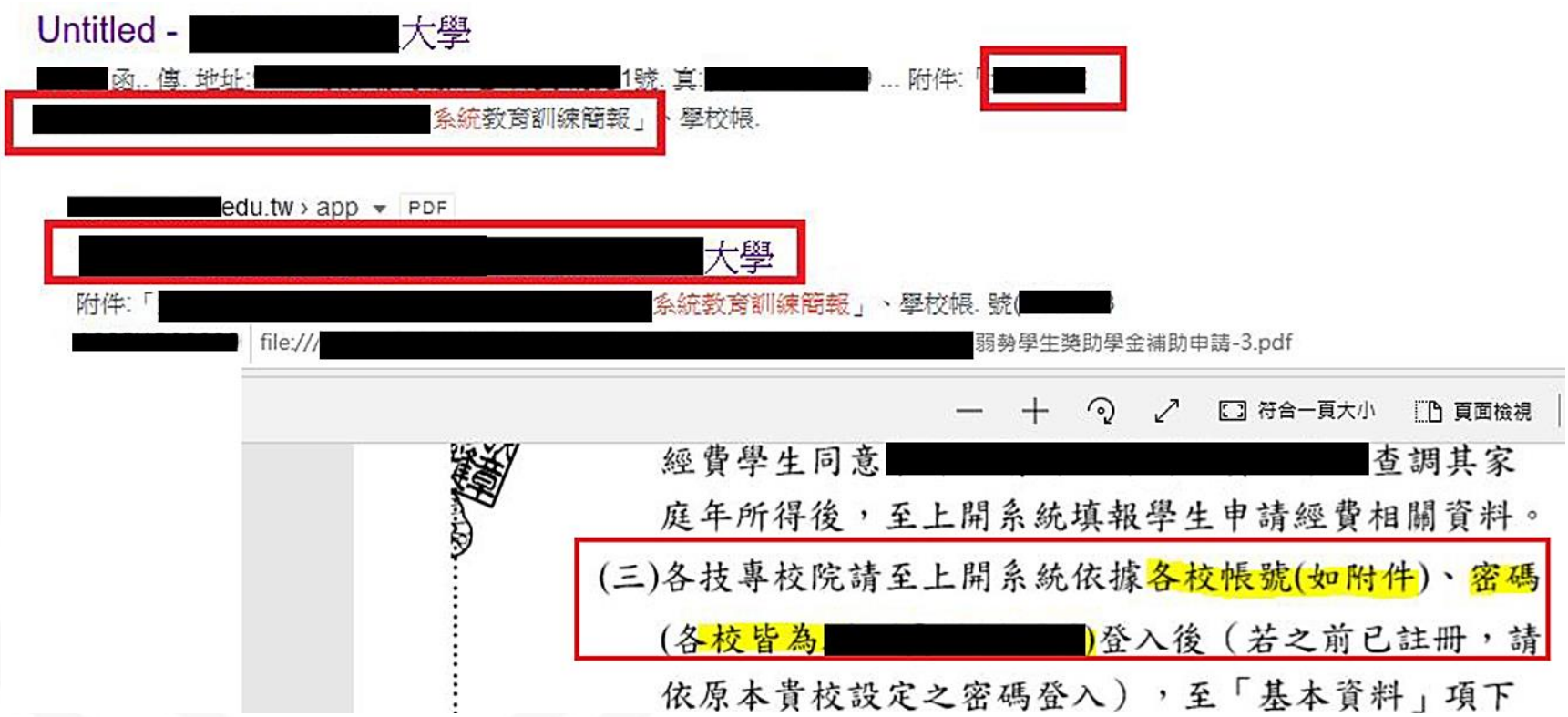
3.公開預設帳號與通行碼原則

公開預設帳號與通行碼原則樣態

- 公文記載帳號清單與共用預設密碼，且受文單位逕行公開於單位網站
- 「首次使用預設密碼登入須變更密碼」機制淪為系統公告性質，程式並未強制要求變更，導致使用者沿用預設密碼

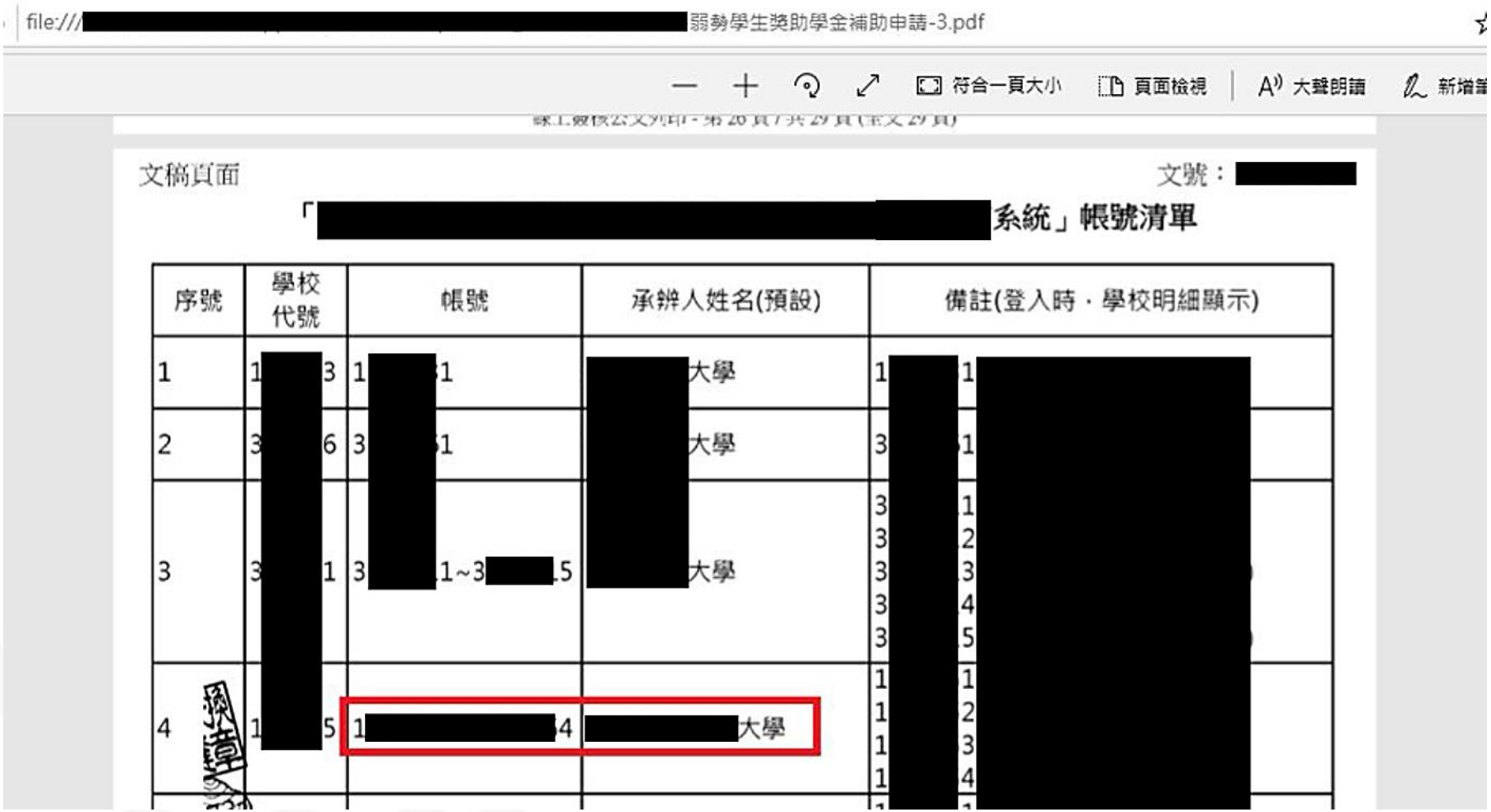
案例3 公文洩漏預設規則(1/4)

- 攻擊手透過Google得知，某系統曾有教育訓練簡報，並取得該份簡報檔及公文內容(含預設密碼)



案例3 公文洩漏預設規則(2/4)

- 檔案附件亦有各校帳號清單



案例3 公文洩漏預設規則(3/4)

- 透過該資料，攻擊手成功登入某所大學(該帳號曾使用過，但系統並未強制要求修改預設密碼)

案例3 公文洩漏預設規則(4/4)

- 因此攻擊手除可登入該大學帳號，亦取得承辦人登打之學生個資

https://[redacted]ApplyData

[redacted]申請[redacted]

學校名稱：[redacted]大學

承 辦 人：[redacted]大學　　聯絡電話：[redacted]

編號	學制	部別	年級	姓名	身分證字號
1	[redacted]學士班	[redacted]部	4	施[redacted]	D22[redacted]
2	[redacted]學士班	[redacted]部	4	蔡[redacted]	D22[redacted]
3	[redacted]學士班	[redacted]部	4	畢[redacted]	D22[redacted]
4	[redacted]學士班	[redacted]部	4	薛[redacted]	D22[redacted]
5	[redacted]學士班	[redacted]部	4	陳[redacted]	N22[redacted]
6	[redacted]學士班	[redacted]部	4	曾[redacted]	P22[redacted]
7	[redacted]學士班	[redacted]部	4	許[redacted]	R22[redacted]

公開預設帳號與通行碼原則改善建議

- 避免以任何形式公開帳號與通行碼原則
- 若應教育訓練需求，需事先提供簡報，則應準備兩個版本簡報，登入資訊等細節僅於現場講解，並提醒保密義務
- 變更預設通行碼應從系統面設計為強制性機制，且不可設定為預設通行碼，以防遭他人事先盜用

4.未落實權限檢查

未落實權限檢查樣態

- 網站透過前端JavaScript語法進行轉導，卻於回應封包夾帶過多資訊，攻擊者可修改JavaScript繞過身分驗證。管理介面亦暴露明文密碼，攻擊者可匿蹤控制系統，或嘗試登入其他系統

- 網站未正確檢查Cookie，攻擊者可透過偽造Cookie，直接取得網站管理者權限，無需取得帳號與通行碼

案例4-1 JavaScript轉導語法繞過(1/4)

- 攻擊手瀏覽網頁發現下一層目錄為SYS，並利用目錄列舉工具得知存在/AP/SYS/acct.aspx路徑

view-source:https://[redacted].gov.tw/[redacted].aspx

```
82              if ($("#Hid_Tag").val() != '') {
83                  ClickTag($("#Hid_Tag").val());
84              }
85              else
86                  $("#BtnTag1").addClass('act');
87          });
88
89          function GoFirstLogin(oid) {
90              if (CheckDevice())
91                  location.href = "SYS/[redacted].aspx?oid=" + oid;
92              else
```

```
---- Scanning URL: https://[redacted].gov.tw/ ----
+ https://[redacted].gov.tw/[redacted]/acct.aspx (CODE:200|SIZE:48135)
+ https://[redacted].gov.tw/[redacted]/calendar.aspx (CODE:200|SIZE:20721)
+ https://[redacted].gov.tw/[redacted]/category.aspx (CODE:302|SIZE:140)
+ https://[redacted].gov.tw/[redacted]/changepassword.aspx (CODE:200|SIZE:5985)
```

案例4-1 JavaScript轉導語法繞過(2/4)

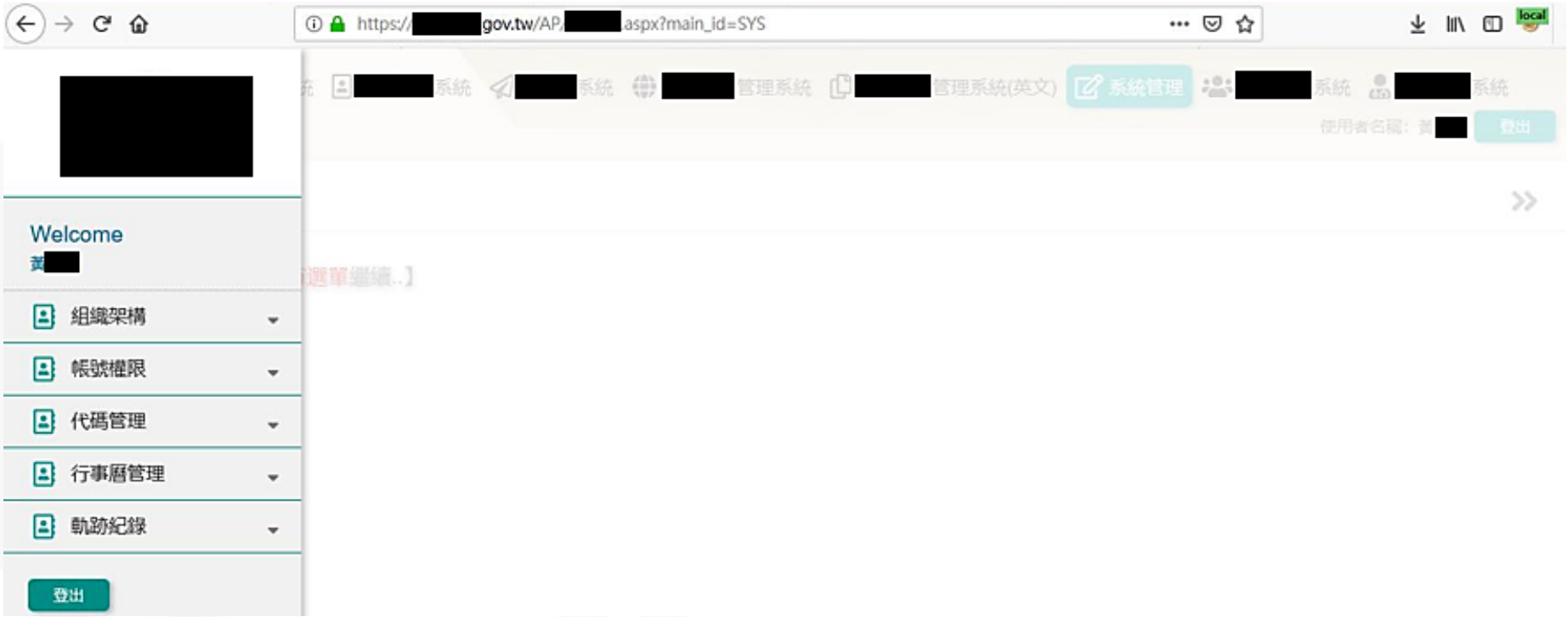
- 實際存取發現係透過JavaScript語法限制未登入使用者存取後臺，遂嘗試利用Burp Suite繞過限制

案例4-1 JavaScript轉導語法繞過(3/4)

- 成功進入使用者管理介面，發現密碼欄位依靠password屬性保護，透過瀏覽器之「開發人員工具」即可得知明文密碼

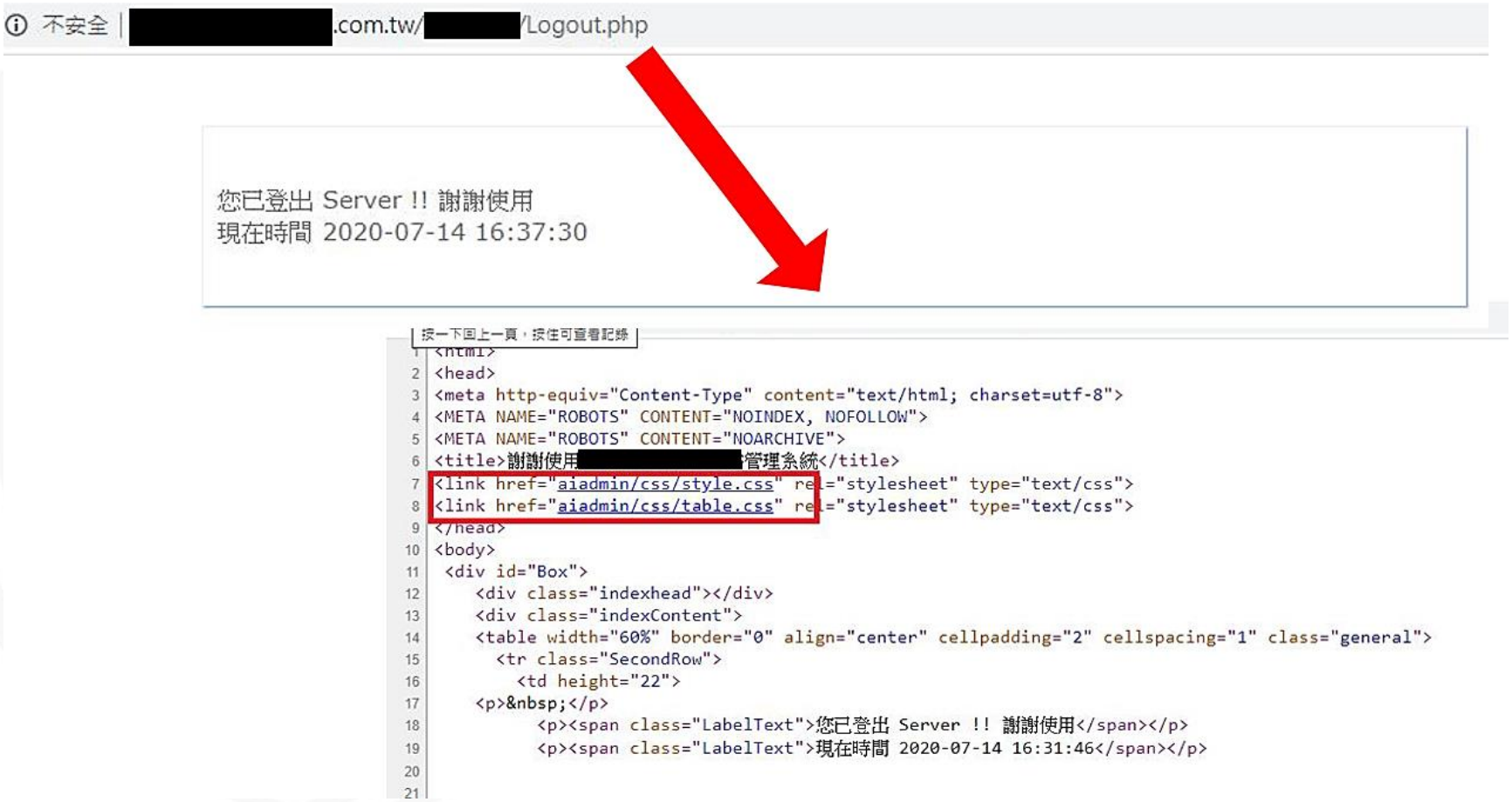
案例4-1 JavaScript轉導語法繞過(4/4)

- 利用取得之密碼資訊，成功登入系統，並取得系統管理者權限



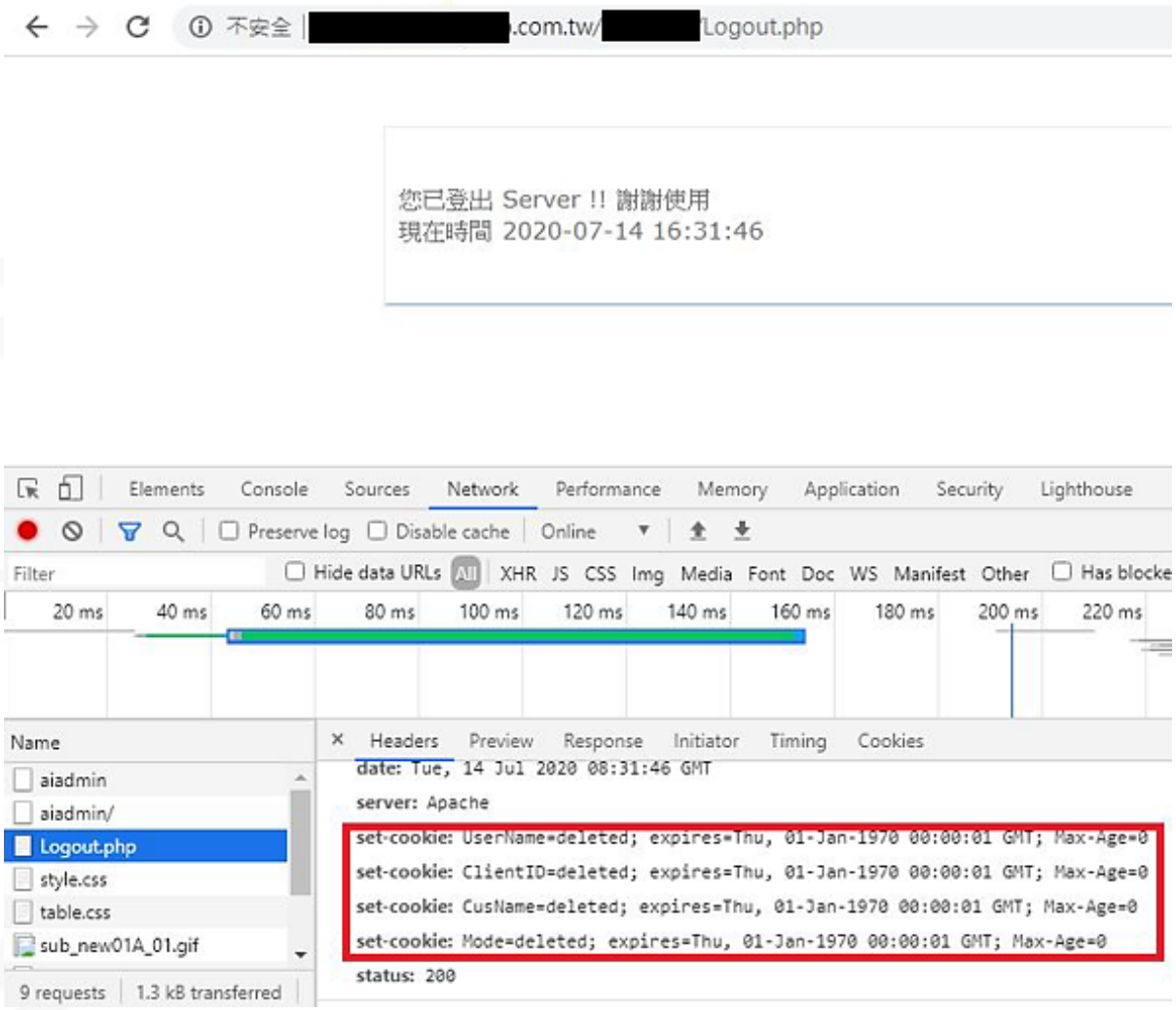
案例4-2 Cookie資訊偽造(1/4)

- 攻擊手進行路徑猜測，得知登出頁面路徑，並從html原始碼發現路徑aiadmin



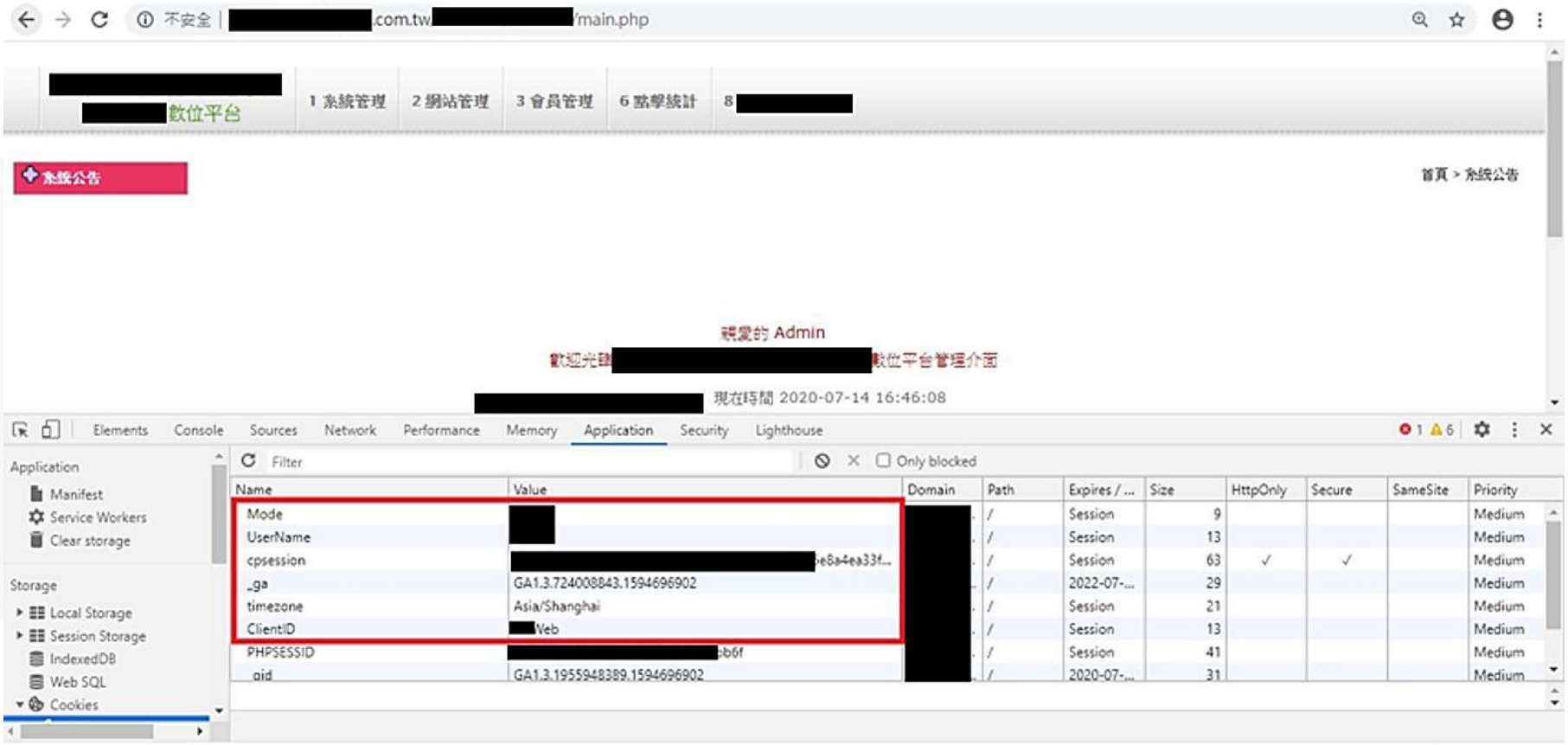
案例4-2 Cookie資訊偽造(2/4)

- 存取aiadmin頁面會導回logout頁面，藉由觀察往來封包，發現該頁面刪除特定cookie內容



案例4-2 Cookie資訊偽造(3/4)

- 將刪除的cookie新增至瀏覽器，並填入猜測之cookie值，重新檢視頁面後發現可成功登入



案例4-2 Cookie資訊偽造(4/4)

- 透過管理者上傳檔案功能，可成功執行Webshell

未落實權限檢查改善建議

- 建議逐一頁面落實權限檢查機制，且依系統角色差異，明確區分訪客(未登入)、一般使用者及管理者等權限差異

- 資料庫不應儲存使用者明文通行碼，以免系統遭入侵時連帶暴露使用者常用通行碼。若有變更通行碼需求，可透過亂數產生後直接通知使用者

大綱

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

資料庫資安檢測目的

- 為強化政府機關重要資料保護，針對核心資料庫執行技術檢測，並設計以資料庫為核心，結合主機安全、資通系統安全及網路安全等面向之技術檢測框架

資料庫安全檢測

確認資料庫本身防護措施，與介接應用系統連線管理之安全性

主機安全檢測

確認資料庫主機之帳號管理、權限設定、存取管控及弱點防護情形

資通系統安全檢測

針對與資料庫介接之資通系統，確認滲透測試執行結果與弱點修補情形

網路安全檢測

確認資料庫之網路安全防護機制，與內外部應用系統介接情形及VPN管理方式

資料庫資安檢測項目

資料庫安全檢測

透過訪談及設定檢視，檢測資料庫之特權帳號管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全機制，以確認資料庫安全管理與防護狀況

主機安全檢測

透過訪談及實際檢視，檢測主機帳號管理、權限設定及存取管控情形，以及透過弱點掃描方式，確認主機相關弱點防護情形

資通系統安全檢測

透過檢視滲透測試報告及複測，檢測介接資通系統之權限存取、應用程式與系統弱點及系統通訊保護等項目之防護情形

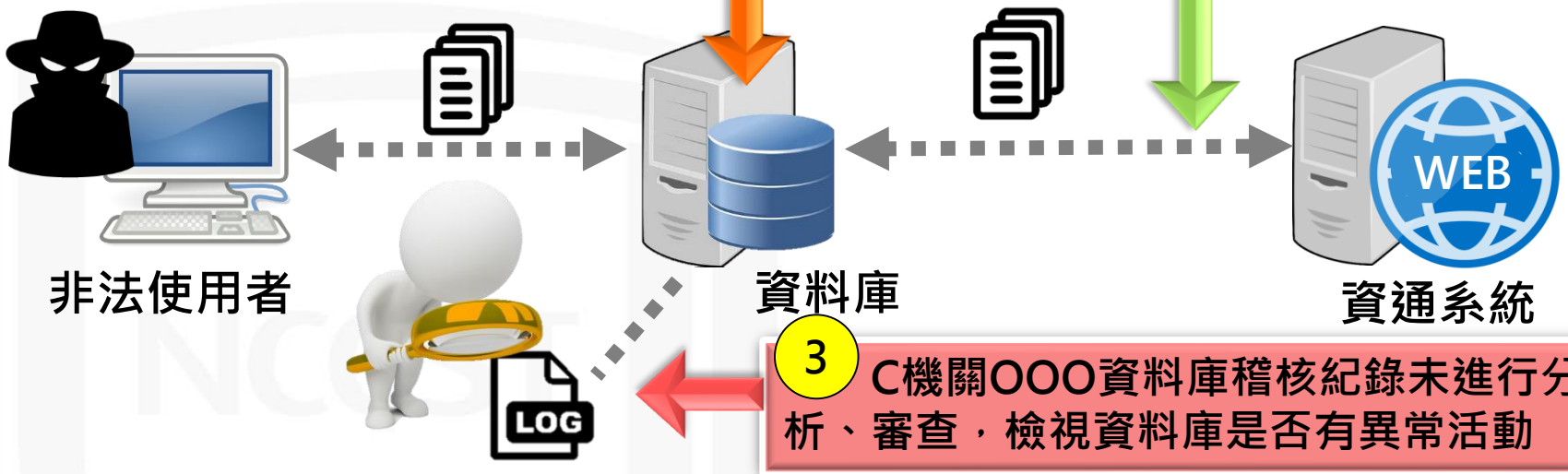
網路安全檢測

透過訪談及實際檢視，檢測應用系統與資料庫介接情形、VPN連線管理、防火牆規則、遠端連線管理及存取控制等項目之防護情形

共同發現事項(1/4)

1 經檢測發現A機關OOO資料庫資料為明文資料，未採取適當資料加密、遮罩或混淆機制，機敏資料恐有遭受侵害之風險

2 B機關OOO分析與管理資料庫未設置安全的加密傳輸管道，機敏資料恐被攔截而曝光



3 C機關OOO資料庫稽核紀錄未進行分析、審查，檢視資料庫是否有異常活動

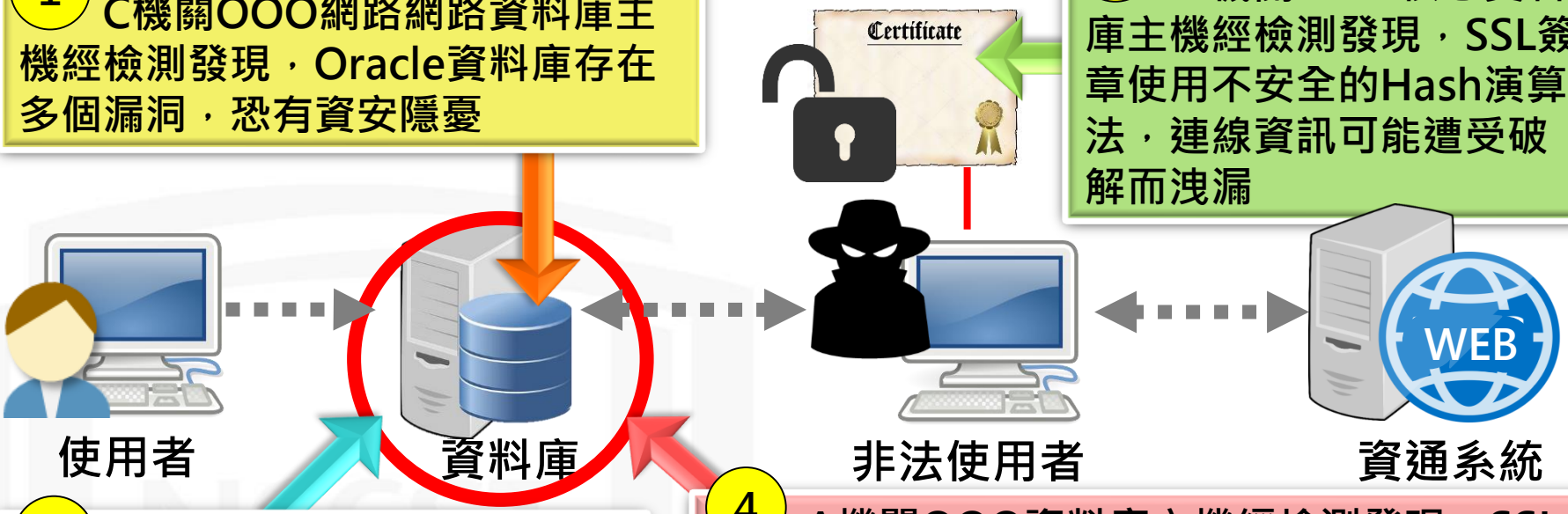
資料庫安全檢測改善建議：

1. 建議針對資料庫中機敏資料採取加密或欄位內容遮罩、混淆等保護機制，強化資料安全性
2. 建議資料庫應設置安全的加密傳輸方式
3. 建議定期分析資料庫稽核紀錄，發現潛在異常行為，及早因應

共同發現事項(2/4)

1 C機關OOO網路網路資料庫主機經檢測發現，Oracle資料庫存在多個漏洞，恐有資安隱憂

2 D機關OOO核心資料庫主機經檢測發現，SSL簽章使用不安全的Hash演算法，連線資訊可能遭受破解而洩漏



3 E機關OOO資料庫主機帳號未啟用帳號與密碼原則設定

4 A機關OOO資料庫主機經檢測發現，SSL使用中強度的加密，防護強度不足有被破解偷窺的風險

主機安全檢測改善建議：

1. 資料庫軟應定期進行軟體更新或評估可行之風險控管措施，進行風險管理
2. 使用具有更高安全性的加密簽章方式
3. 針對資料庫主機應強制啟用帳號與密碼原則設定，強化帳號密碼安全性
4. 停止中強度的SSL加密演算法，採行更安全的加密演算法

共同發現事項(3/4)

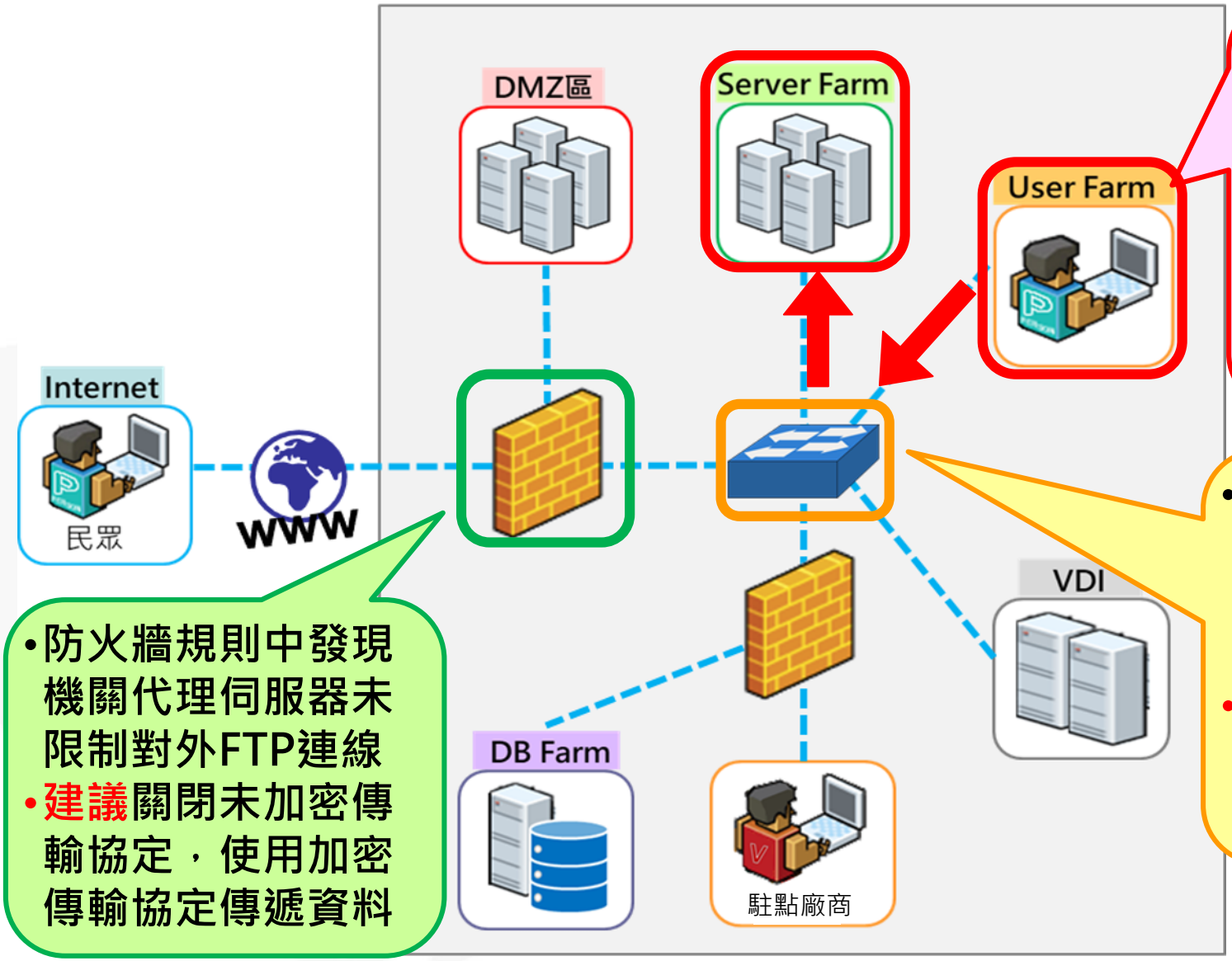
1 E機關XXX資通系統存在跨網站腳本攻擊弱點未修補，可能竊取使用者Cookie 中之機敏資料或將使用者自動引導至釣魚網站

2 D機關XXX資通系統存在無效的存取控管弱點未修補，恐讓使用者取得其他權限方可使用的功能頁面或下載的檔案等

資通系統安全檢測改善建議：

1. 過濾可能造成危害的符號及語法輸入，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
2. 建議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

共同發現事項(4/4)



- 內網使用者網段與伺服器網段間未有存取控制
- 建議依需求配置網路區域間存取控制

- 核心交換器管理介面，未限制存取之網路位址
- 建議限制僅管理人員IP可存取管理介面

- 防火牆規則中發現機關代理伺服器未限制對外FTP連線
- 建議關閉未加密傳輸協定，使用加密傳輸協定傳遞資料

大綱

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

結論與建議

- 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，同時啟用高強度之協定或演算法
- 加強存取控制措施
  - 連網設備、資通系統及資料庫等可透過限縮來源IP或對外服務埠進行網路控管，並搭配帳號權限強化權限區隔
- 建立內部驗證機制
  - 資通系統上線前應有基本檢查清單，提醒負責同仁應確認事項；針對弱點修復應檢附驗證結果，確認弱點已無法重現
- 落實資安防護政策
  - 應從系統面強制實施防護政策；同時建立稽核制度，定期追蹤未符合資安規範之事件

報告完畢
敬請指教