108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

108年12月

大綱

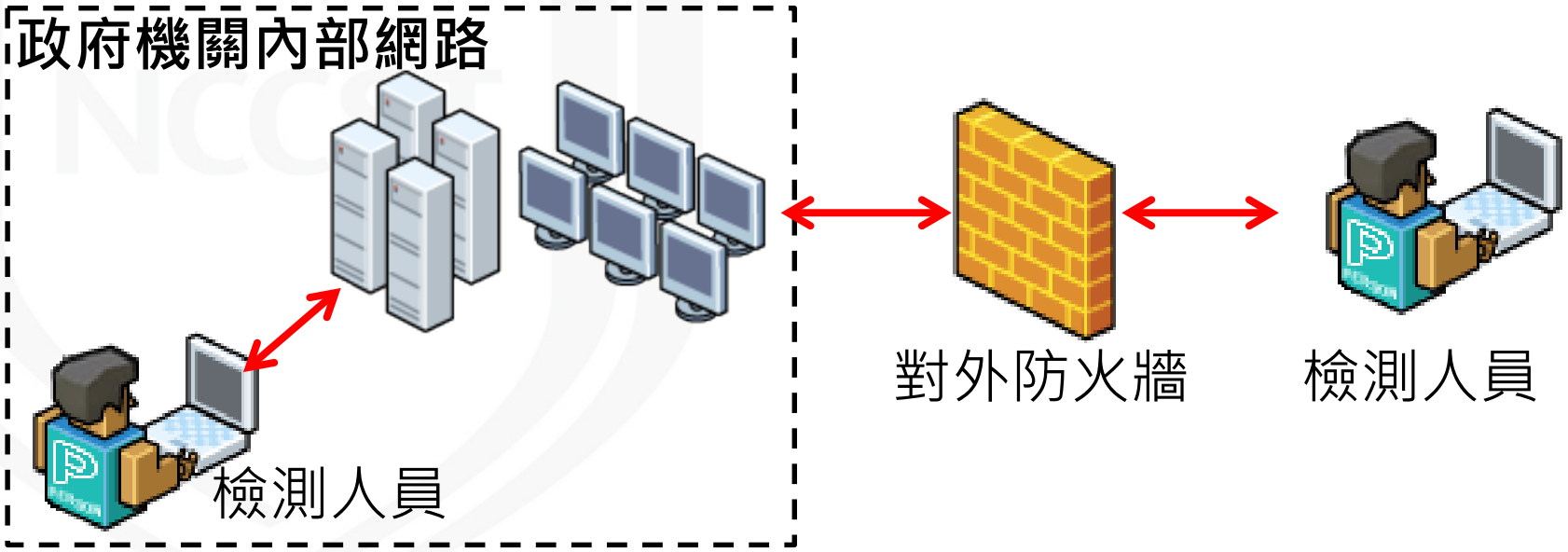
- 前言
- 網路攻防演練發現與建議
- 資安稽核技術檢測發現與建議
- 結論與建議

大綱

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

前言

- 技服中心歷年透過網路攻防演練與資安稽核檢測共兩個面向檢測政府機關資安防護能量
- 網路攻防演練藉由外部網路檢驗機關整體防禦機制是否完備，資安稽核檢測則透過內部網路驗證系統本身安全性強度



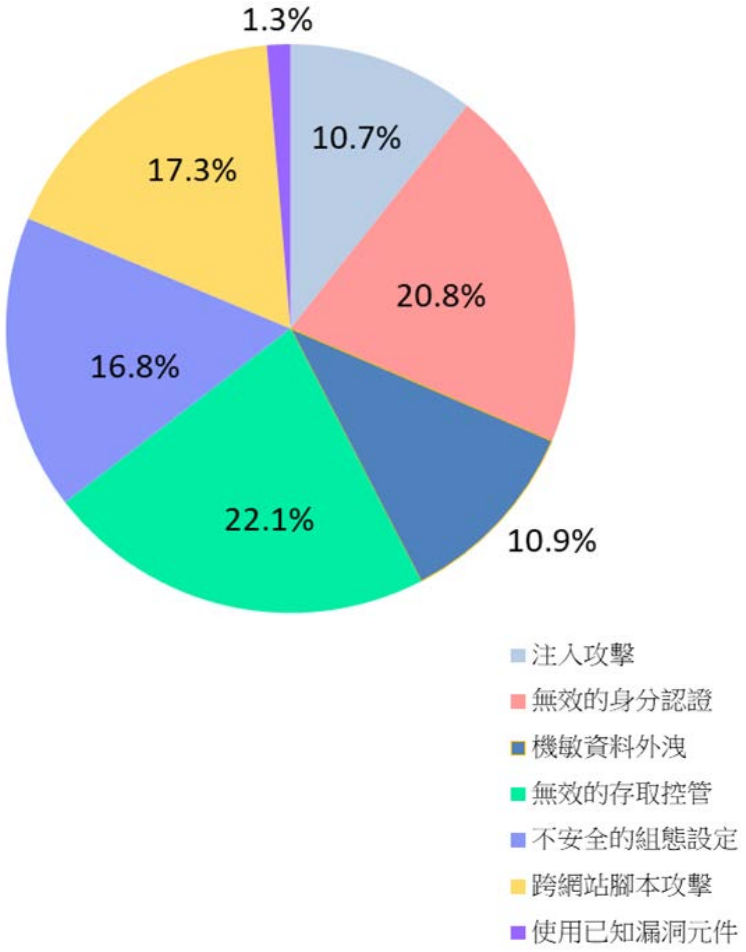
大綱

- 前言
- 網路攻防演練發現與建議
- 資安稽核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108年網路攻防演練攻擊紀錄，其中無效的存取控管與無效的身分認證筆數比例最高

排名	弱點類型	比例
1	無效的存取控管	22.1%
2	無效的身分認證	20.8%
3	跨網站腳本攻擊	17.3%
4	不安全的組態設定	16.8%
5	機敏資料外洩	10.9%
6	注入攻擊	10.7%
7	使用已知漏洞元件	1.3%
總計		100%



網路攻防演練綜合發現

- 歸納上述弱點類型，其根因可匯整為下列5項，建議參考以下9個案例介紹，清查機關潛在弱點

項次	發現事項	案例
1	未落實通行碼強度檢查機制	案例1,2
2	集中使用相同套件或委外廠商	案例3,4
3	不當的轉導設計	案例5,6
4	未即時更新網站使用之套件	案例7,8
5	不正確的安全觀念	案例9

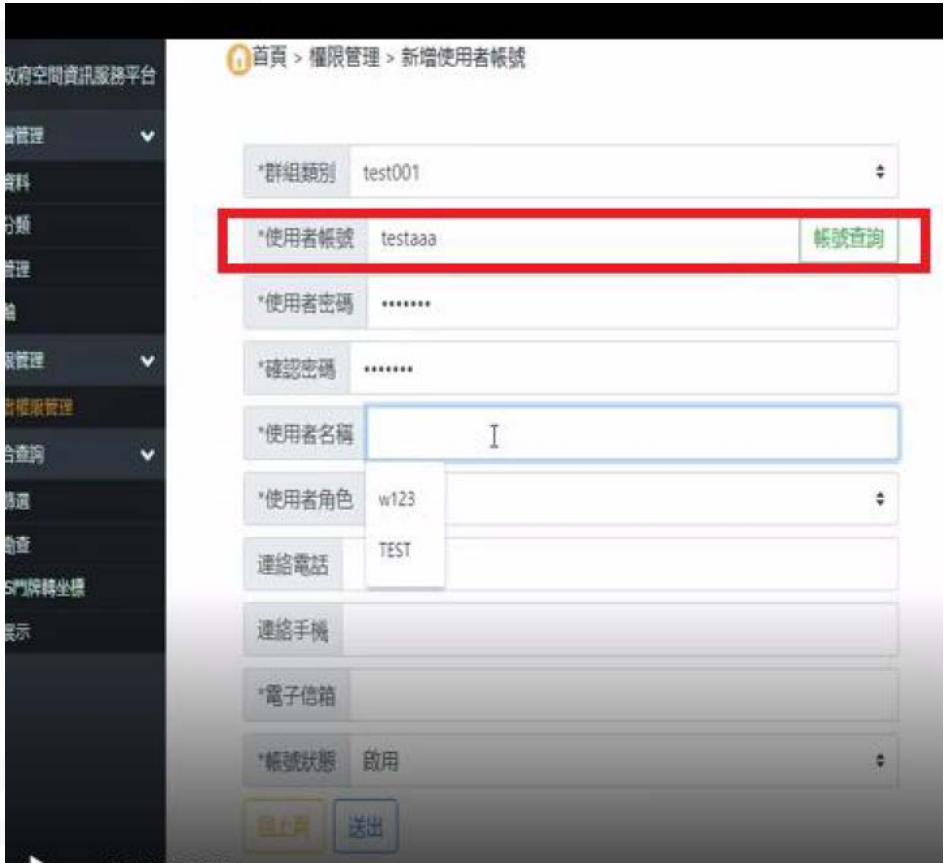
1.未落實通行碼強度檢查機制

未落實通行碼強度檢查機制樣態

- 108年網路攻防演練期間仍發現部分機關未強化通行碼設定原則
- 107年已介紹相同案例所造成的影響
- 利用帳號與通行碼相同手法入侵系統複雜度極低，但影響範圍輕則取得一般同仁權限，重則揭露內部往來信件或者取得系統權限

案例1 測試帳號遭利用 (1/3)

- 攻擊手瀏覽教學影片，發現一組測試用帳號，嘗試猜測與帳號相同之通行碼，可成功登入後台，但不具備帳號管理權限



案例1 測試帳號遭利用 (2/3)

- 攻擊手發現「詮釋資料維護」功能可上傳任意檔案，透過下載按鈕取得Webshell上傳後之網址

案例1 測試帳號遭利用 (3/3)

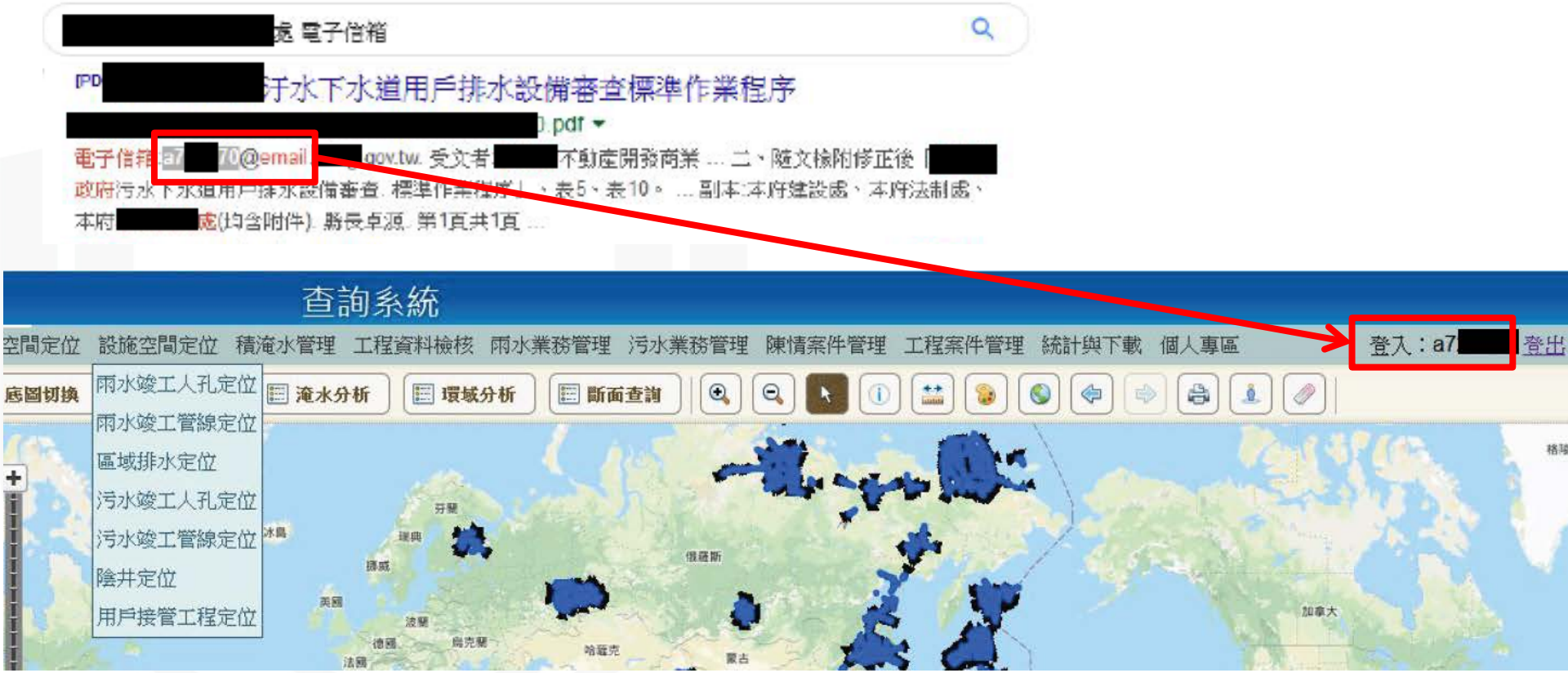
- 可成功於「C:\Windows\System32」目錄底下建立指定檔案

[redacted].gov.tw[redacted]

```
2014/10/29  上午 09:52         2,829,312 netshell.dll
2016/01/20  上午 12:55            39,936 NETSTAT.EXE
2014/10/29  上午 09:53           924,672 nettrace.dll
2013/06/18  下午 10:45            21,812 NetTrace.PLA.Diagnosti
2014/10/29  下午 12:04            44,368 netutils.dll
2018/04/06  上午 01:38            66,560 NetVscCoinstall.dll
2013/08/22  下午 08:27            44,544 netvscres.dll
2014/10/29  上午 09:45         1,678,336 networkexplorer.dll
2014/10/29  上午 09:59            56,320 networkitemfactory.dll
2013/08/22  下午 11:39
               networklist
2014/10/29  上午 08:58           106,496 NetworkStatus.dll
2014/10/29  上午 10:02           333,824 newdev.dll
2014/10/29  上午 10:22            76,288 newdev.exe
2019/05/07  下午 04:55                15 nicst108pt.txt
```

案例2 帳號與通行碼相同 (1/3)

- 攻擊手透過尋找承辦處室同仁信箱，發現可透過帳號與通行碼相同方式登入，取得一般同仁權限



案例2 帳號與通行碼相同 (2/3)

- 攻擊手發現「專用下水道屬性內容」功能可上傳任意檔案，透過預覽按鈕取得Webshell上傳後之網址

案例2 帳號與通行碼相同 (3/3)

- 可成功於「網站目錄」底下建立指定檔案

未落實通行碼強度檢查機制改善建議

- 建議刪除或停用預設帳號，再另行建立管理者帳號；若預設帳號無法更動則至少須修改預設通行碼
- 通行碼建議具備高複雜度，同時禁止使用者設定與帳號相同之通行碼

2.集中使用相同套件或委外廠商

集中使用相同套件或委外廠商樣態

- 多個系統皆使用相同套件
- 單一委外廠商承接多個縣市系統開發委外案，雖設有高複雜度通行碼，卻跨機關使用相同帳號與通行碼

案例3 參數設計不良 (1/3)

- 攻擊手發現其中一個特定參數可控制公告狀態

案例3 參數設計不良 (2/3)

- 透過修改此參數，可開啟編輯模式

案例3 參數設計不良 (3/3)

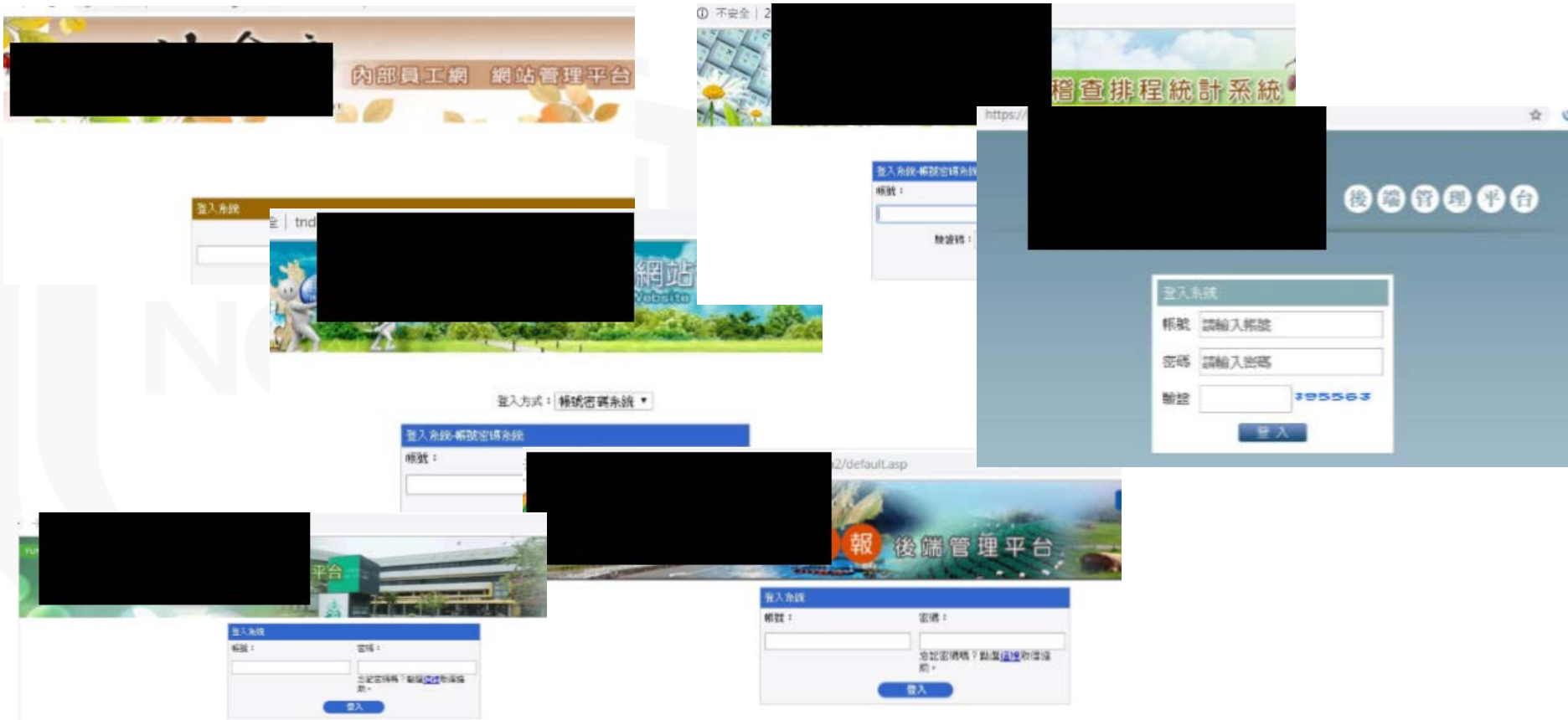
- 藉由編輯模式，可在未登入時任意修改公開內容
- 相同手法影響高達18個系統

案例4 後台管理不當 (1/2)

- 以其他手法進入後台後發現一組帳號，並與其他網站之教學手冊進行比對，推測可能為廠商通用之帳號通行碼

案例4 後台管理不當 (2/2)

- 搜尋該廠商開發之政府單位網站，成功利用同一組帳號通行碼登入6個網站，並取得管理者權限



集中使用相同套件或委外廠商改善建議

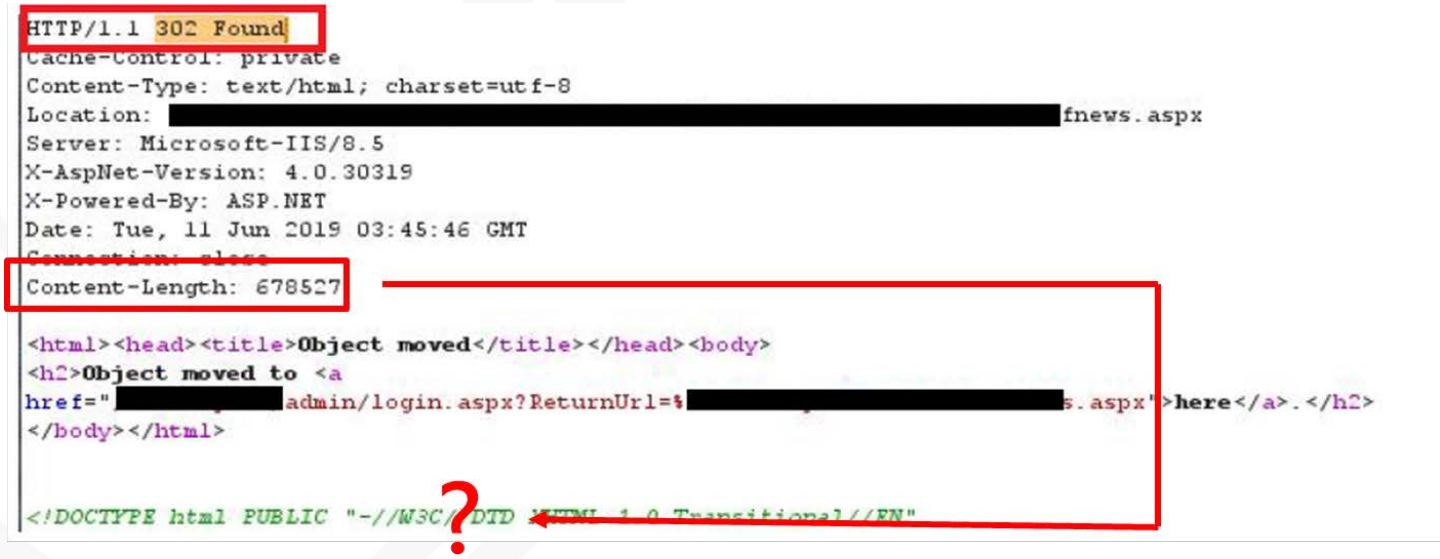
- 建議針對機關內部若有使用相同套件之系統，應納入定期追蹤，如發現該套件弱點應建立情資分享管道

- 針對委外廠商應要求其使用之通行碼須符合機關通行碼複雜度原則

3.不當的轉導設計

不當的轉導設計樣態

- 多數系統當權限檢查失敗時，皆會透過特定方式進行轉導
- 若轉導過程存在缺陷，攻擊者則可透過修改封包標頭等方式中斷轉導，進而存取未經授權之功能



案例5 轉導設計不當 (1/4)

- 攻擊手首先利用目錄列舉軟體進行列舉，發現存在特定路徑回應302轉導

```
---- Scanning URL: https://[redacted]/admin/ ----
+ https://[redacted].gov.tw/[redacted]/admin/analysis.aspx (CODE:302|SIZE:19739)
+ https://[redacted].gov.tw/[redacted]/admin/index.aspx (CODE:302|SIZE:2534)
+ https://[redacted].gov.tw/[redacted]/admin/Index.aspx (CODE:302|SIZE:2534)
+ https://[redacted].gov.tw/[redacted]/admin/info.aspx (CODE:302|SIZE:475983)
+ https://[redacted].gov.tw/[redacted]/admin/login.aspx (CODE:200|SIZE:5075)
+ https://[redacted].gov.tw/[redacted]/admin/Login.aspx (CODE:200|SIZE:5075)
+ https://[redacted].gov.tw/[redacted]/admin/logout.aspx (CODE:200|SIZE:2406)
+ https://[redacted].gov.tw/[redacted]/admin/member.aspx (CODE:302|SIZE:2969145)
+ https://[redacted].gov.tw/[redacted]/admin/news.aspx (CODE:302|SIZE:678527)
+ https://[redacted].gov.tw/[redacted]/admin/News.aspx (CODE:302|SIZE:678527)
+ https://[redacted].gov.tw/[redacted]/admin/post.aspx (CODE:302|SIZE:346375)
```

案例5 轉導設計不當 (2/4)

- 接著利用封包攔截工具將302轉導改為200 OK，使其自動轉導回首頁功能失效

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: [redacted]fnews.aspx
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 11 Jun 2019 03:45:46 GMT
Connection: close
Content-Length: 678527

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a
href="[redacted]admin/login.aspx?ReturnUrl=%[redacted]s.aspx">here</a>.</h2>
</body></html>


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

案例5 轉導設計不當 (3/4)

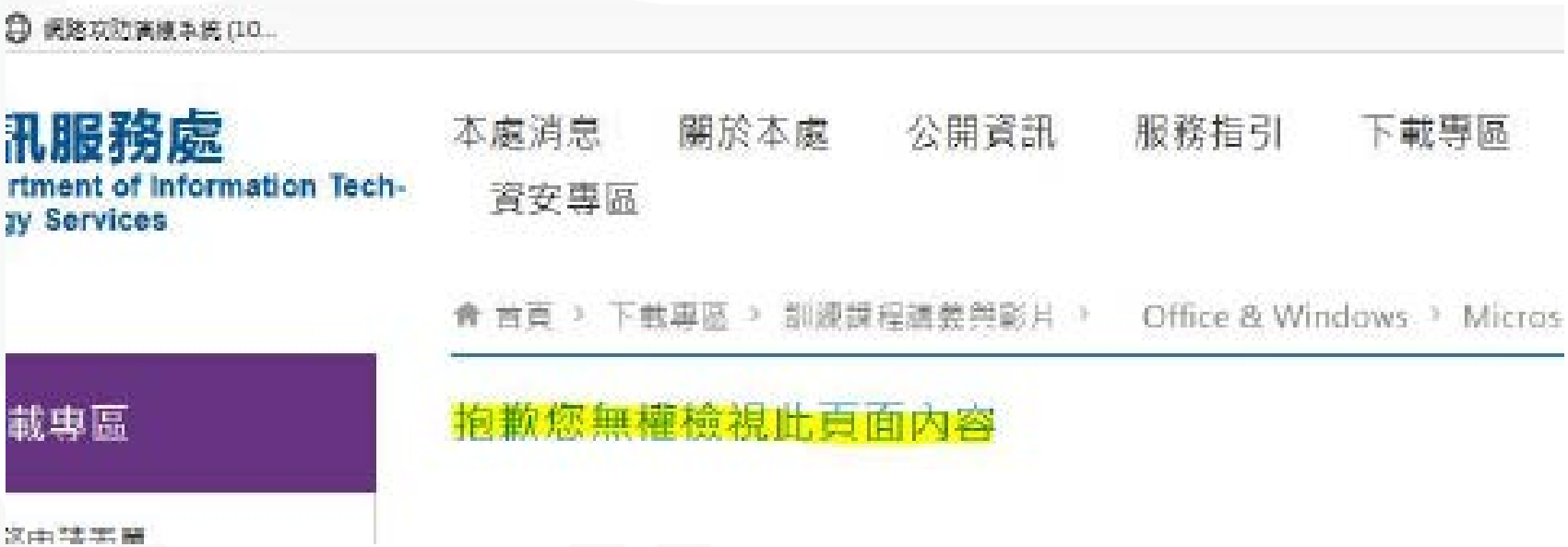
- 可成功進入後台管理介面，且無須帳號通行碼

案例5 轉導設計不當 (4/4)

- 編輯內容亦可直接顯示於前台頁面

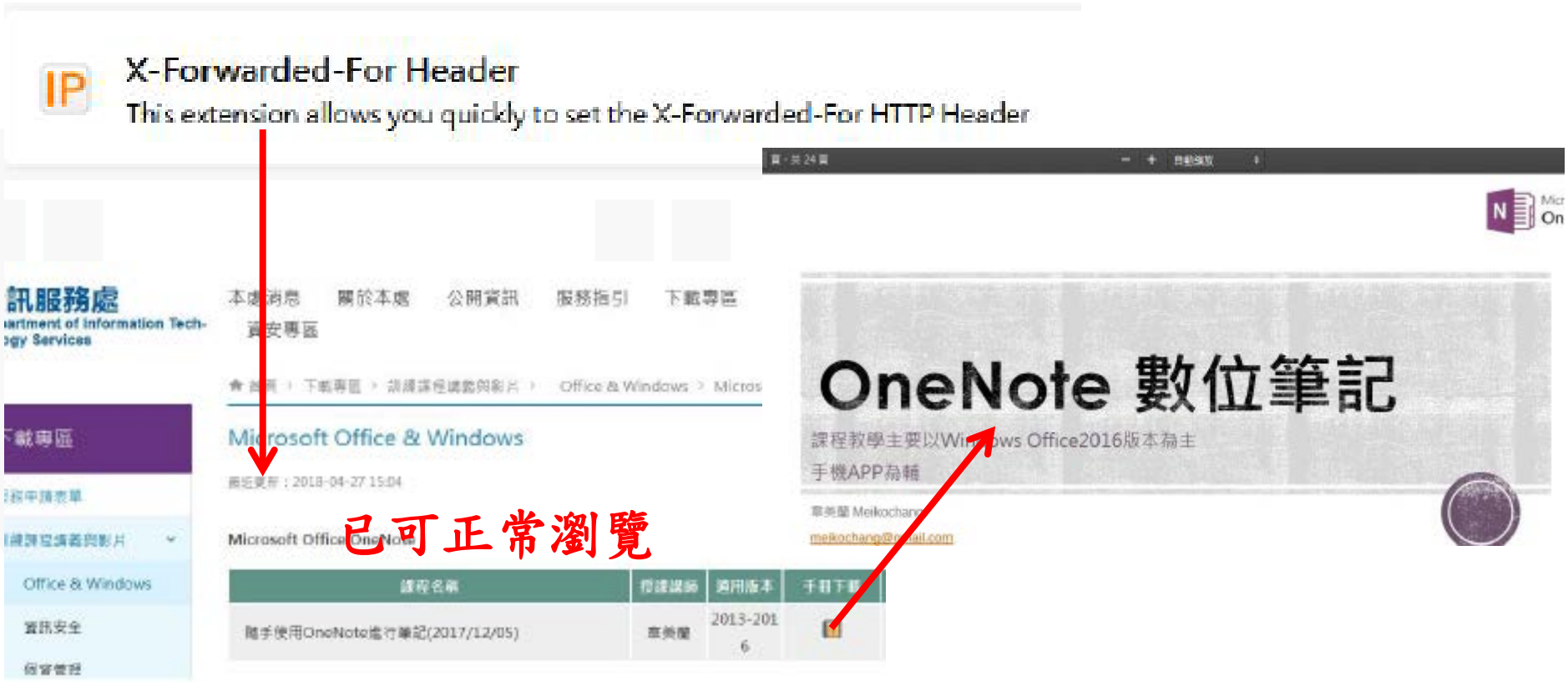
案例6 轉導設計不當 (1/2)

- 攻擊手直接瀏覽目標網頁，顯示「抱歉您無權檢視此頁面內容」訊息，但此頁面本身為公開頁面



案例6 轉導設計不當 (2/2)

- 利用X-Forwarded-For Header套件輸入與受測系統相同IP，即可瀏覽原先禁止存取之頁面



不當的轉導設計改善建議

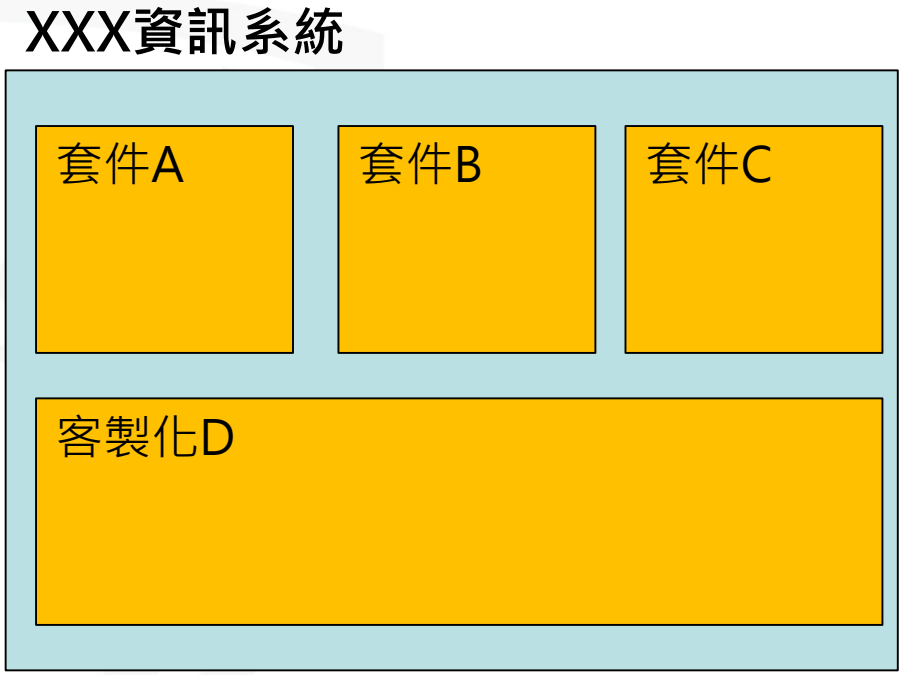
- 應對所有功能頁面進行權限控管，同時權限檢查須區分存取來源為使用者或管理者

- 所有檢查應於伺服器端進行，僅回傳必要之檢查結果，避免將未授權之功能頁面併入檢查結果中回傳，以防遭攻擊者竄改進而繞過檢查機制

4.未即時更新網站使用之套件

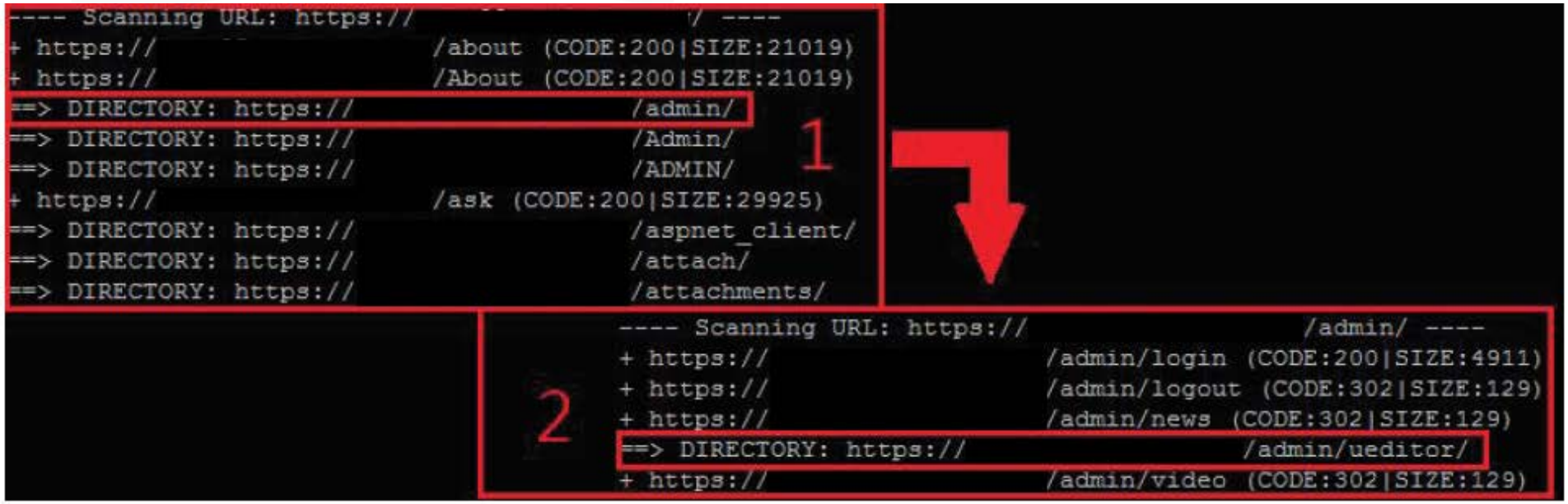
未即時更新網站使用之套件樣態

- 現今系統多包含第三方套件以加快開發速度，但當第三方套件出現弱點時，卻容易在盤點期間遭忽略



案例7 ueditor 套件弱點 (1/3)

- 攻擊手使用Dirb工具進行路徑掃描，發現路徑「/admin」，並發現路徑「/admin/ueditor」，推測使用ueditor套件



案例7 ueditor 套件弱點 (2/3)

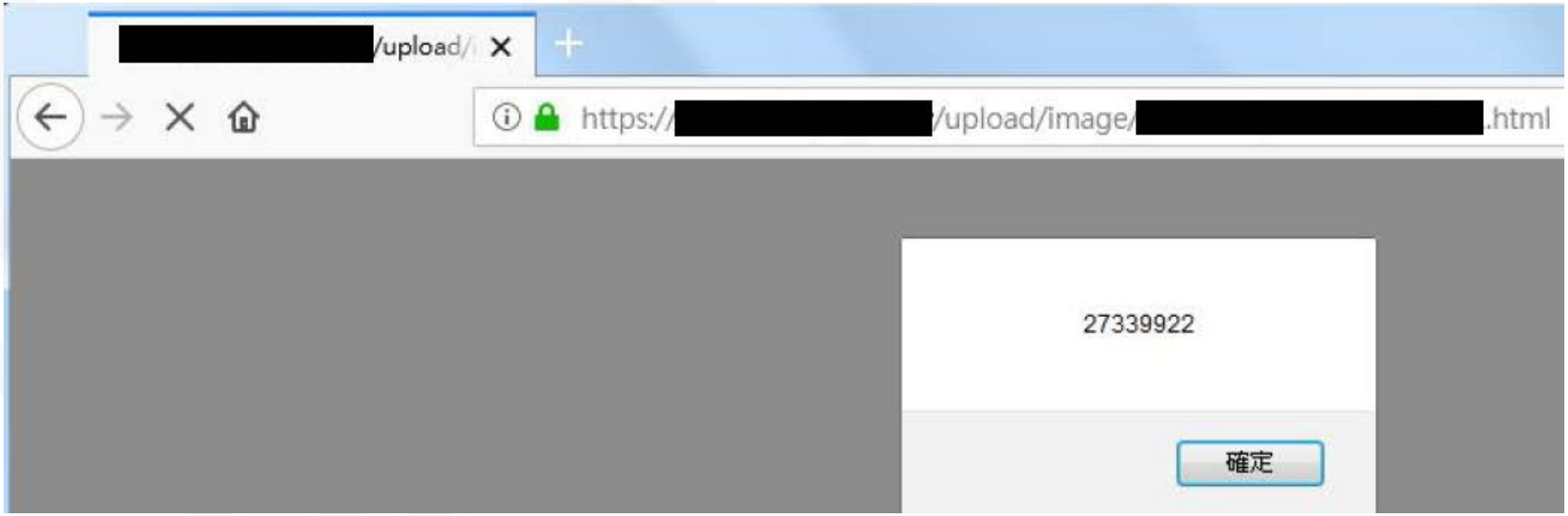
- 實際存取漏洞頁面，確認頁面存在且可正常回應

- 參考弱點PoC資料，自行編輯網頁原始碼，新增表單元素作為檔案上傳使用

案例7 ueditor 套件弱點 (3/3)

- 上傳後，回應顯示檔案連結之路徑

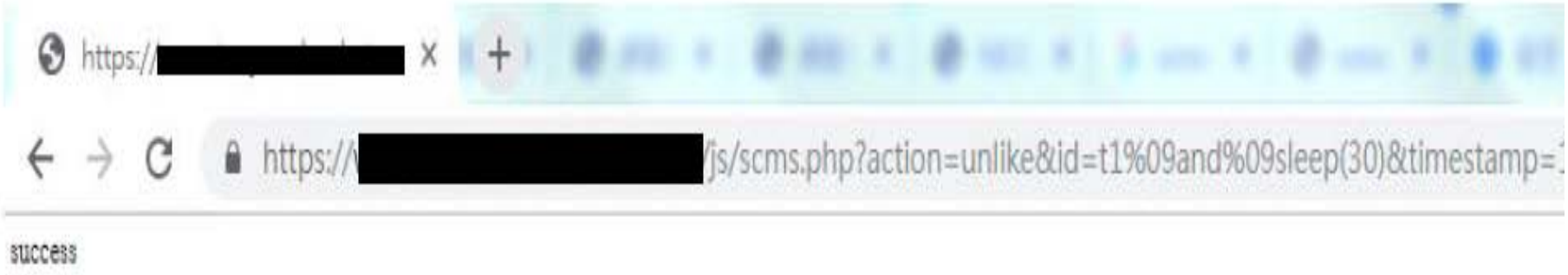
- 實際存取該頁面，確認可觸發所上傳之XSS語法



案例8 PHP 套件弱點 (1/3)

- 由網址猜測可能使用S-CMS PHP套件，搜尋相關資料後，發現可能存在CVE-2019-10708漏洞，可針對參數「id」進行注入攻擊

- 利用Time-Based注入語法確認弱點存在



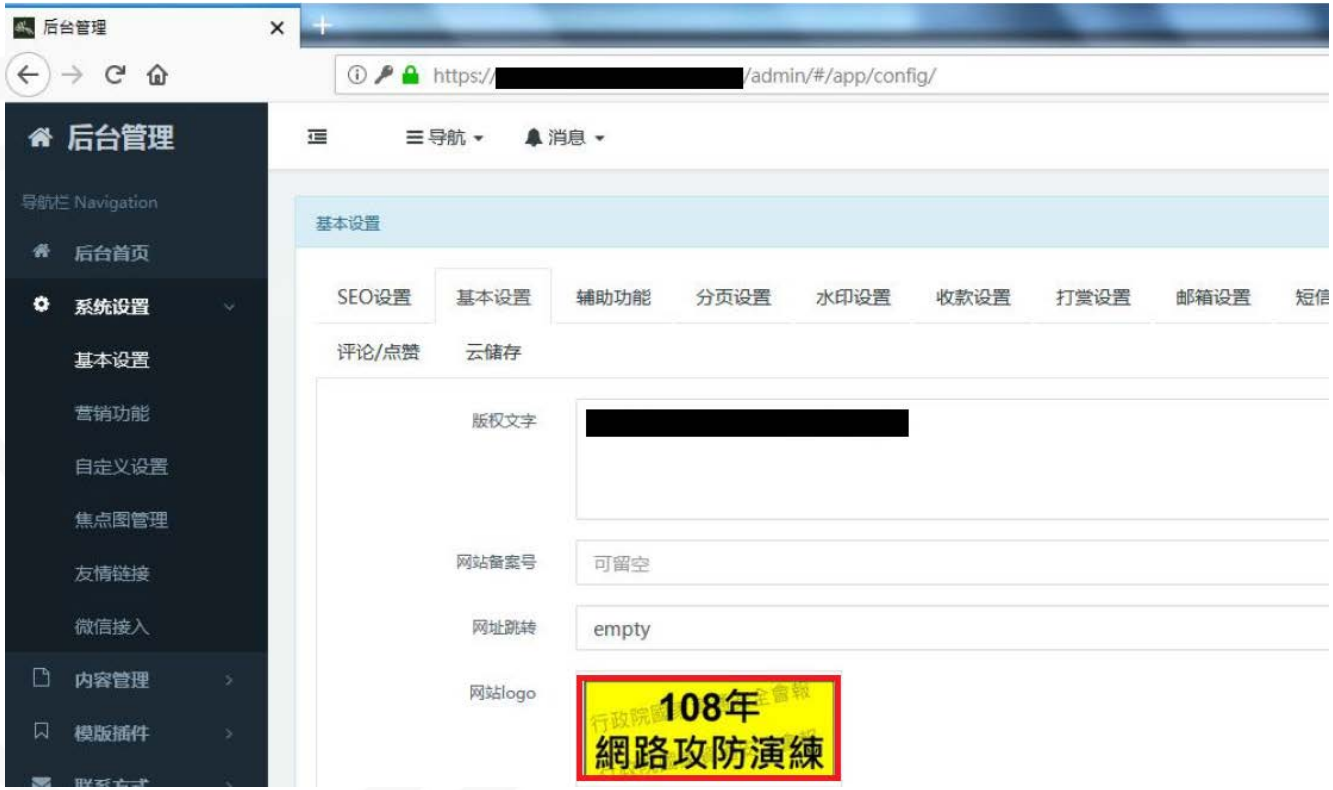
案例8 PHP 套件弱點 (2/3)

- 使用攻擊腳本執行注入攻擊，獲取管理員帳號與加密通行碼並透過破密軟體得知通行碼明文

```
@kali24:~$ python3 scms_sqli.py https://
>---- A_login length: 5
>---- A_login value: admin
@kali24:~$ python3 scms_sqli.py https://
>---- A_pwd length: 32
>---- A_pwd value: ce                                    54
```

案例8 PHP 套件弱點 (3/3)

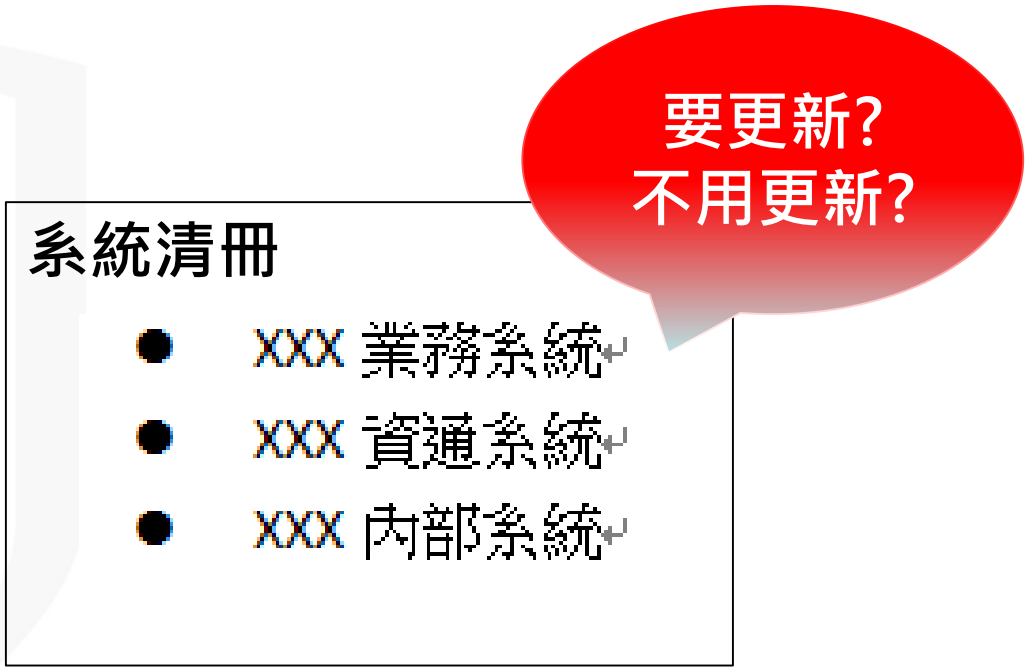
- 利用取得之明文帳號通行碼，攻擊手可成功登入網站管理後台，並修改前台公開資料



未即時更新網站使用之套件改善建議

- 建議若開發期間已知使用第三方套件時，將套件名稱與版本納入該系統之備註資訊
- 當套件出現漏洞時可儘早發覺

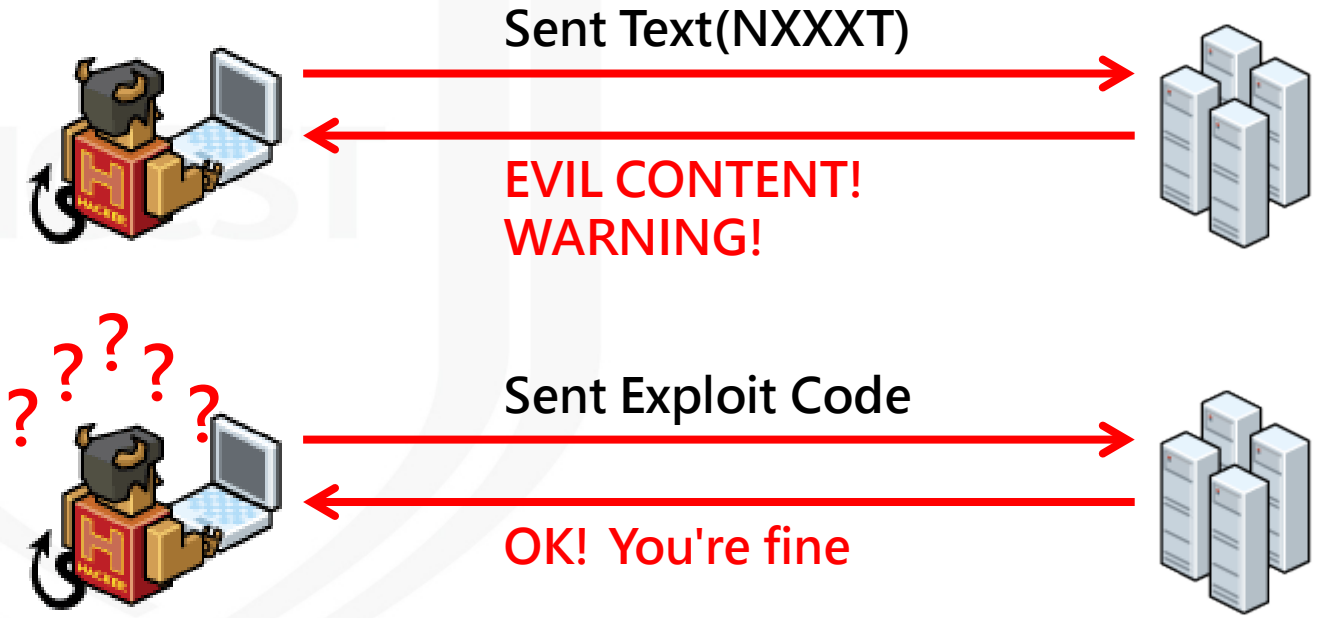
CVE-2019-0001
CVE-2019-0002
CVE-2019-0003
…
CVE-2019-7XXX
CVE-2019-8XXX
CVE-2019-9XXX



5.不正確的安全觀念

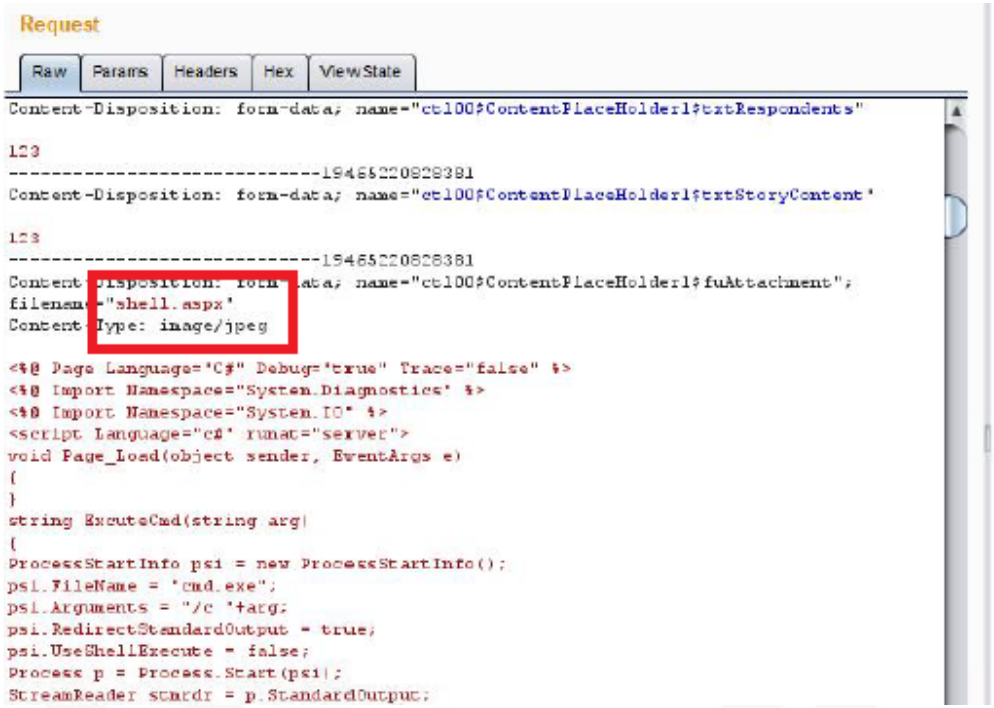
不正確的安全觀念樣態

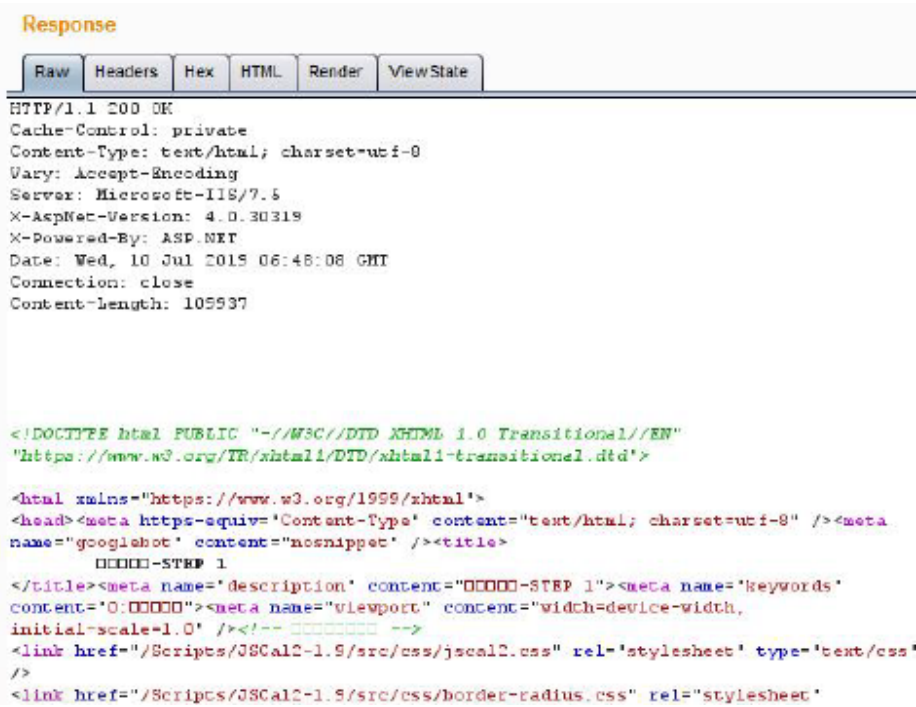
- 演練期間，為幫助機關區分真實資安事件與演練事件，故於字串內加入固定特徵字串作為識別
- 近期發現，機關開始針對特徵字串做過度防禦，即便單純輸入特徵字串亦被視為攻擊



案例9 規避演練之無效防護 (1/3)

- 攻擊手首先利用Burp Suite繞過前端檢查，同時檔名使用shell.aspx



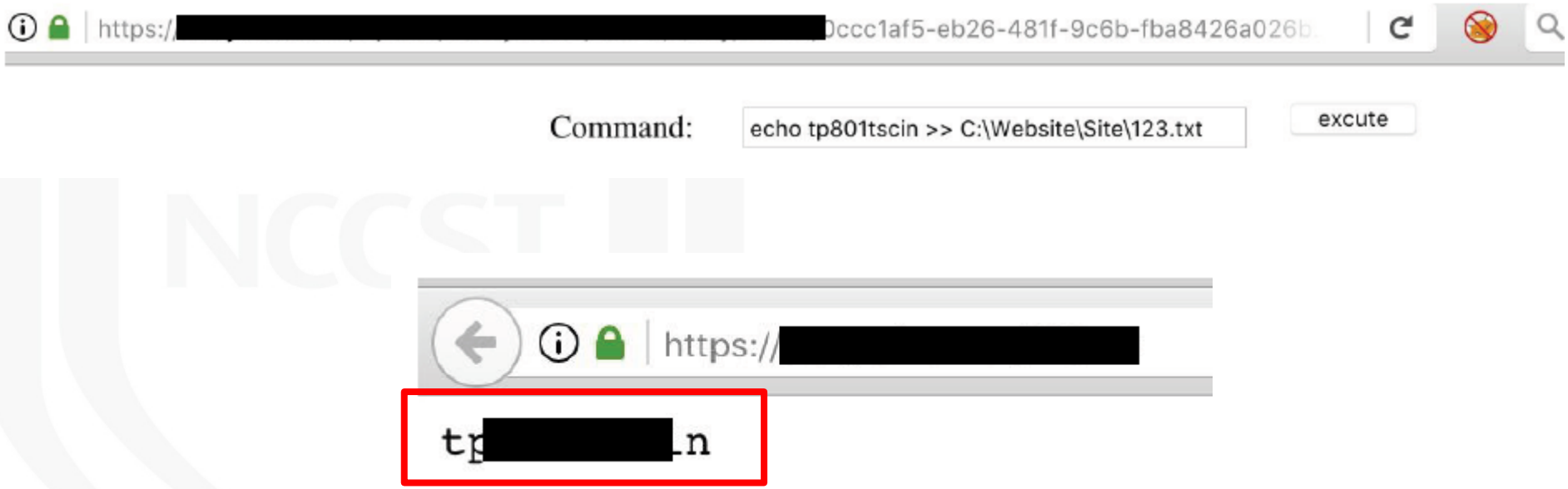


案例9 規避演練之無效防護 (2/3)

- 發現檔案可成功上傳，複製檔案路徑嘗試執行 WebShell

案例9 規避演練之無效防護 (3/3)

- 從圖片可得知，WebShell已成功執行，下一步則是執行指令。但原規定字串NXXXT已被阻擋，僅能透過文字型態轉換等方式輸入



不正確的安全觀念改善建議

- 建議應僅針對惡意語法進行阻擋，若在防護設備套用錯誤的防護規則，僅會讓系統暴露在外部真實威脅之下

大綱

- 前言
- 網路攻防演練發現與建議
- 資安稽核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20個高風險與307個中風險弱點
- 使用者電腦安全性更新共發現26台電腦未落實安全性更新
- 使用者電腦應用程式更新共發現11台電腦未落實應用程式更新

惡意中繼站連線阻擋檢測

- 共發現514筆IP中繼站名單未阻擋
- 共發現356筆DN中繼站名單未阻擋

核心資通系統安全檢測

- 滲透測試結果共發現59個高風險、3個中風險及27個低風險弱點項目
- 防護基準檢測結果共發現75個不符合項目

網路架構檢測

網路架構檢測結果共發現23個高風險、36個中風險及1個低風險弱點項目

AD主機安全防護檢測

AD伺服器主機安全性更新共發現3台伺服器未落實安全性更新

物聯網設備檢測

物聯網設備檢測結果共發現50個高風險、3個中風險及8個低風險弱點項目

組態設定安全檢測

- 使用者電腦發現10台電腦組態設定未符合
- 伺服器主機發現7台主機組態設定未符合
- 瀏覽器發現11台電腦組態設定未符合
- 網通設備發現3台設備組態設定未符合

共同發現事項(1/7)

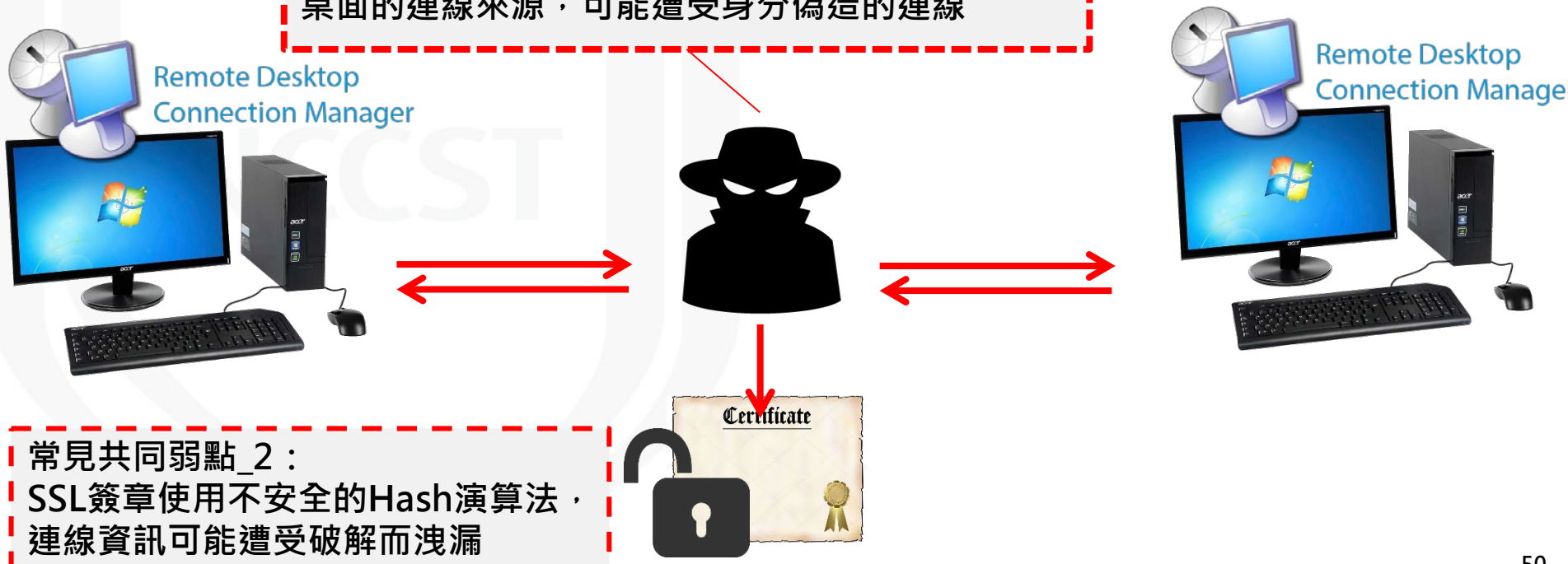
1.使用者電腦安全檢測

- 使用者電腦弱點掃描
- 使用者電腦安全防護檢測

改善建議：

- 使用具有更高安全性的加密簽章方式
- 重新設定遠端桌面連線之驗證及加密

常見共同弱點_1：
遠端桌面伺服器存在中間人攻擊弱點，未驗證遠端桌面的連線來源，可能遭受身分偽造的連線



常見共同弱點_2：
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

共同發現事項(2/7)

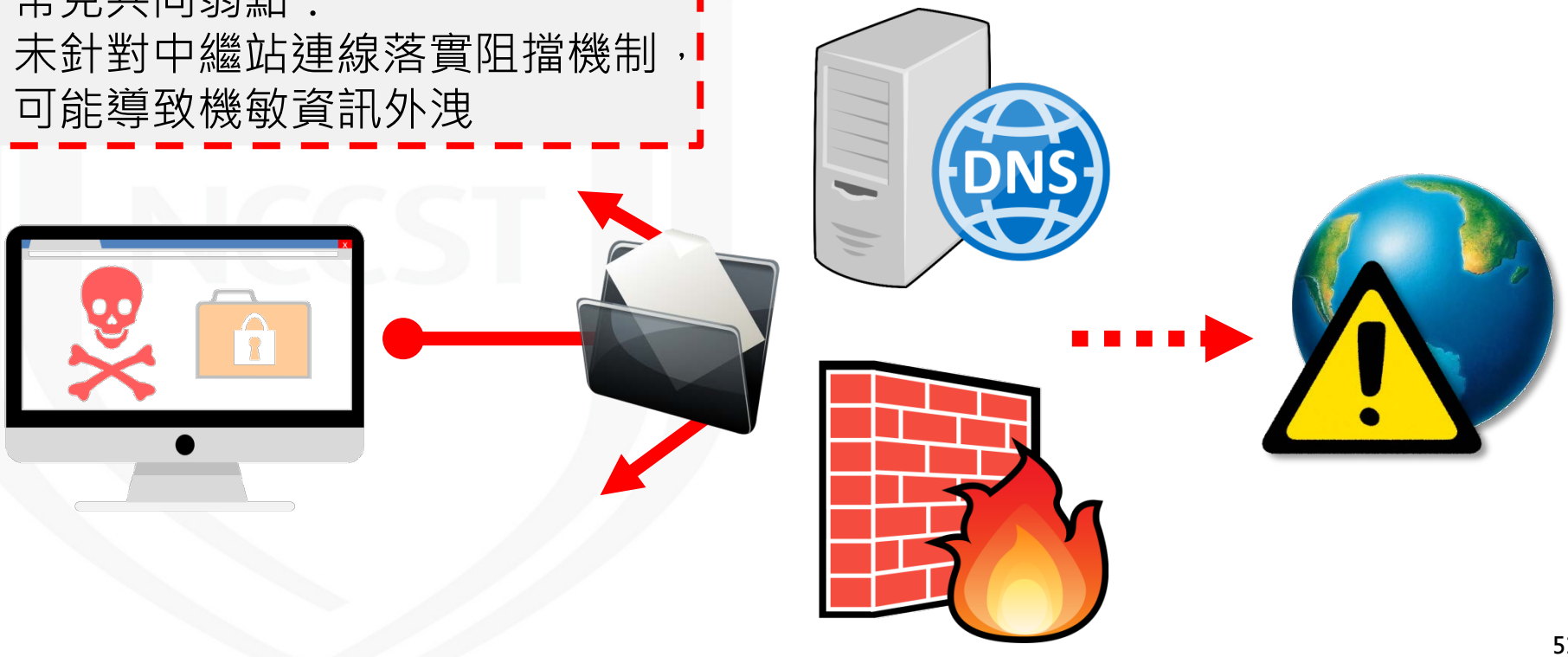
2.網路惡意活動檢視

- 機關使用者網段
- 資通系統管理者網段

改善建議：

- 應制定與落實中繼站更新週期
- 應定期進行惡意中繼站阻擋測試

常見共同弱點：
未針對中繼站連線落實阻擋機制，可能導致機敏資訊外洩



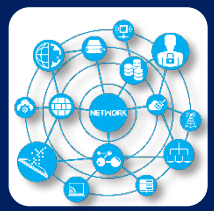
共同發現事項(3/7)

3.核心資通系統安全檢測

- 核心資通系統內網滲透測試
- 核心資通系統防護基準檢測

- 核心資通系統內網滲透測試，所發現共同事項：
  - 發現存在無效的存取控管與跨網站腳本攻擊
- 核心資通系統內網滲透測試，所提出改善建議：
  - 應對所有功能頁面進行適當權限控管
  - 過濾可能造成危害的符號及語法輸入
- 核心資通系統防護基準檢測，所發現共同事項：
  - 發現存在不符合的存取控管
- 核心資通系統防護基準檢測，所提出改善建議：
  - 身分驗證相關資訊不以明文傳輸
  - 使用者更換通行碼時，至少不可以與前3次使用過之通行碼相同
  - 使用者輸入資料合法性檢查應置放於應用系統伺服器端
  - 使用公開、國際機構驗證且未遭破解之演算法

共同發現事項(4/7)



4.網路架構檢測

- 網路與系統之管理控制措施
- 網路與系統之安全控制措施
- 網路與系統架構之備援機制
- 防火牆規則及存取控制

- 網路架構檢測，所發現共同事項：
  - 發現存在不安全的網路設備存取控制
  - 發現存在不安全的網路區域存取
  - 發現存在未限制非加密資料傳輸協定
- 網路架構檢測， 所提出改善建議：
  - 網路區域間的存取、限制內部對外連線
    - 建議重新檢視防火牆，並依需求設定防火牆規則
  - 限制非加密資料傳輸協定
    - 建議關閉未加密傳輸協定, 並使用加密傳輸協定傳遞資料
  - 網路設備存取控制
    - 建議限制僅管理人員的IP可存取管理介面

共同發現事項(5/7)

5.AD主機安全防護檢測

- 防毒軟體
- 安全性修補程式更新檢視
- 惡意程式檢測

改善建議：
建議定期檢視網域主機更新與自動化派送結果情況，以避免未更新所導致之資安風險

常見共同弱點：
AD伺服器主機，未落實安全性更新

共同發現事項(6/7)

6.物聯網設備檢測

- 網路攝影機檢測
- 門禁系統檢測
- 網路印表機檢測
- 無線AP/無線路由器檢測
- 環控系統檢測

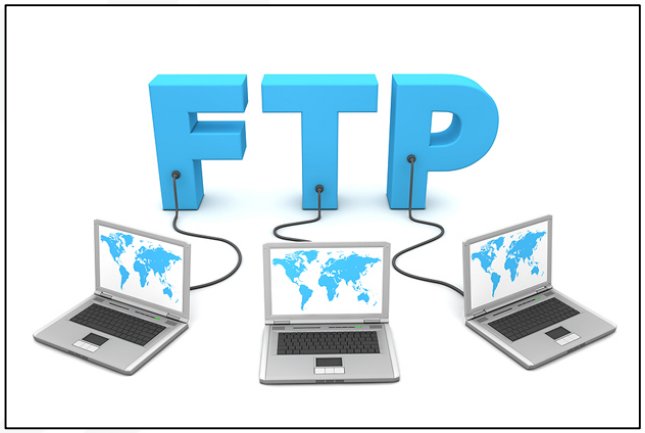
改善建議：

- 禁止使用設備預設帳號通行碼
- 網站管理介面應設定通行碼
- 關閉非必要性的網路服務
- 更新韌體至最新版本

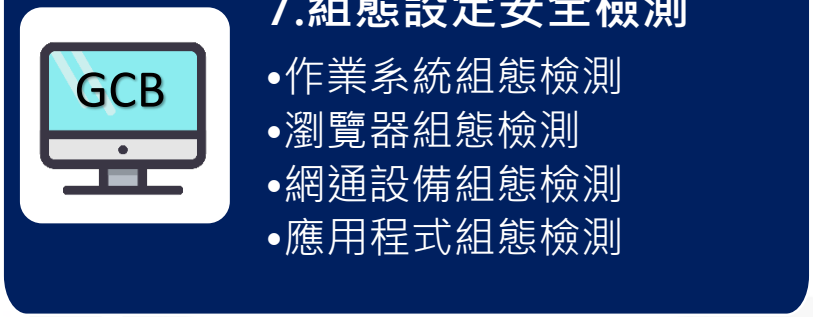
常見共同弱點_1：
缺乏適當的通行碼保護

常見共同弱點_2：
不安全的網路服務

常見共同弱點_3：
使用不安全的系統或元件



共同發現事項(7/7)



- 組態設定安全檢測，所發現共同事項：
  - 受測的使用者電腦存在不符合組態項目
  - 受測的瀏覽器存在不符合組態項目
  - 受測的網域主機存在不符合組態項目
  - 受測的網通設備存在不符合組態項目
- 組態設定安全檢測，所提出改善建議：
  - 建議定期抽檢組態設定內容，以確保組態設定防護之完整性
  - 建議定期檢視例外管理項目與實際環境之一致性

大綱

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

結論與建議

- 強化通行碼檢查機制
  - 建議核心系統、連網設備等皆應設定高複雜度通行碼，且避免預設通行碼或帳號與通行碼相同等情形
- 加強存取控管機制
  - 連網設備、VLAN及核心系統功能頁面皆應進行適當存取控管機制，避免攻擊者越權存取
- 訂定檢視機制
  - 使用者端除定期執行更新外，更應確認更新是否落實
    核心系統若可將引用套件版本納入追蹤，亦有助於追蹤套件安全性。防護設備應進行規則測試，確認阻擋規則生效
- 落實系統安全防護
  - 應正確檢查使用者輸入是否具備惡意語法，同時傳輸協定應使用具有高強度之加密演算法

報告完畢
敬請指教