# 111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

111年11月

# 大綱

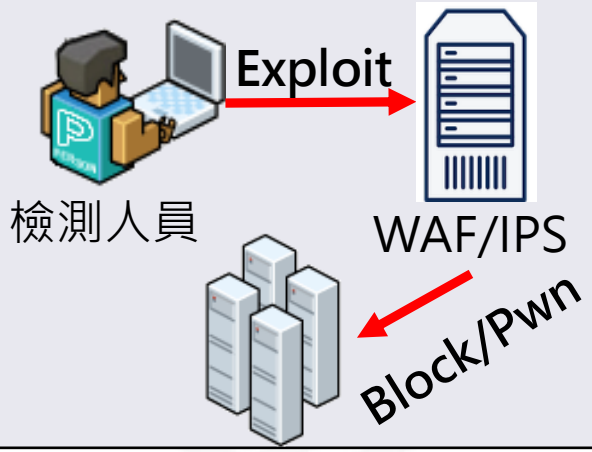
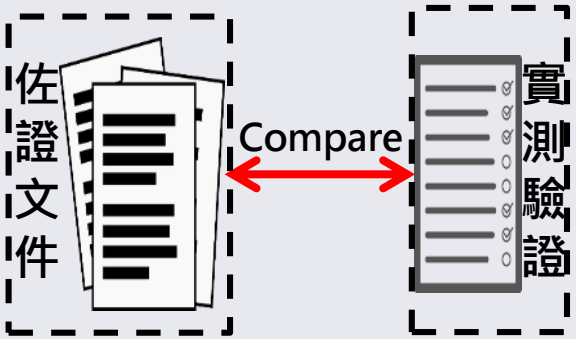
- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

# 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 | 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，111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

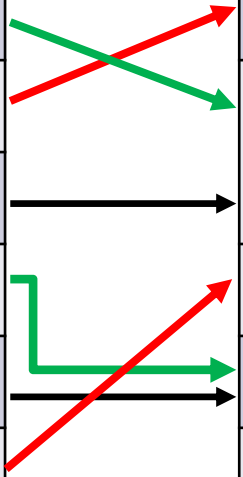
- 本年度經由網路攻防演練，整理主要弱點類型、常見攻擊手法與可能危害如下

| 項次 | 弱點類型 | 常見攻擊手法 | 可能造成危害 |
|---|---|---|---|
| 1 | 無效的存取控管 | • Google Hacking取得未公開網址<br>• 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<br>• 取得系統儲存之機敏資訊(如：個人資料) |
| 2 | 認證及驗證機制失效 | • 弱通行碼破解<br>• 透過系統手冊取得帳號通行碼資訊 | |
| 3 | 不安全的組態設定 | • 使用預設之帳號密碼登入<br>• 繞過檔案上傳格式限制<br>• 透過安全設定不足取得攻擊資訊 | • 取得系統管理權限<br>• 被植入後門程式 |
| 4 | 危險或過舊之元件 | 透過已知弱點進行攻擊 | 遭駭客利用從遠端進行攻擊，取得系統管理權限 |
| 5 | 注入攻擊 | • 跨網站腳本攻擊<br>• SQL Injection攻擊 | • 竊取使用者資訊<br>• 資料庫資訊外洩 |

# 網路攻防演練結果比較

- 依據弱點類型，比較110年類型之變化如下，其中無效的存取控管、認證及驗證機制失效及不安全的組態設定比例最高

| 排名 | 110年 |
|---|---|
| 1 | 無效的身分認證(49%) |
| 2 | 無效的存取控管(21%) |
| 3 | 不安全的組態設定(19%) |
| 4 | 跨網站腳本攻擊(8%) |
| 5 | 注入攻擊(2%) |
| 6 | 使用已知漏洞元件(1%) |
| 7 | 機敏資料外洩(~1%) |



| 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%) |

# 網路攻防演練綜合發現

- 歸納上述弱點類型，挑選7項常見弱點樣態並分析其原因，建議參考下列7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 | 無效的存取控管 | **參數猜測*** | 案例1 |
| 2 | | 限制存取功能失效 | 案例2 |
| 3 | 認證及驗證機制失效 | **未落實通行碼強度檢查機制*** | 案例3 |
| 4 | 不安全的組態設定 | 網頁功能頁面未限制存取 | 案例4 |
| 5 | 危險或過舊之元件 | 使用存在漏洞之套件 | 案例5 |
| 6 | 注入攻擊 | **跨網站腳本攻擊*** | 案例6 |
| 7 | | **注入漏洞*** | 案例7 |

*註：與110年攻防演練發現事項相同

# 1.參數猜測

# 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，攻擊者可竄改參數值，因系統未檢查使用者身分，成功竊取機密資訊

# 案例1 功能參數猜測(1/2)

- 攻擊手瀏覽網頁，並以正常程序進行活動報名

# 案例1 功能參數猜測(2/2)

- 完成報名時發現「報名完成」頁面網址參數疑似為數字流水編號
- 嘗試修改參數，成功取得其他報名者資料

# 參數猜測改善建議

- 系統開發者
  - 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
  - 網頁所使用之網址路徑與參數，建議進行編碼或不易猜測之規律，減少透過簡單掃描與猜測獲知重要功能之路徑

# 2.限制存取功能失效

# 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

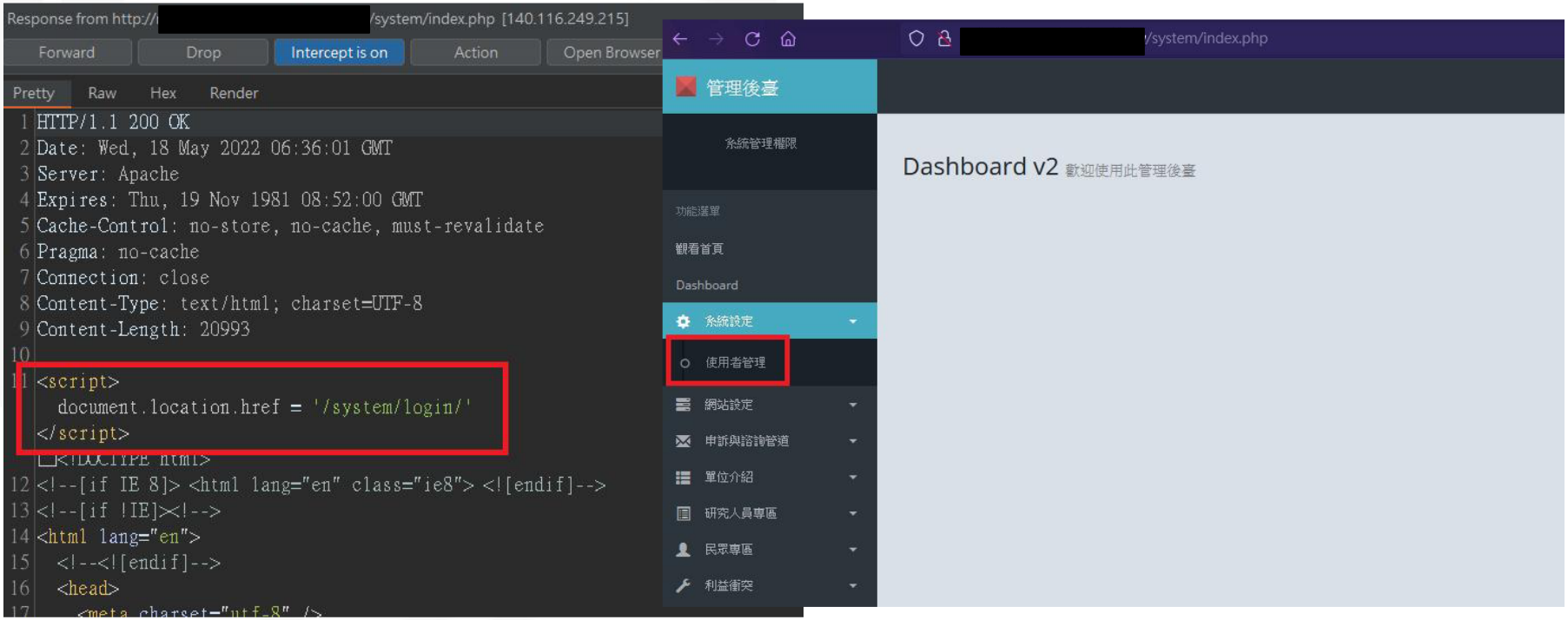
# 案例2 限制存取功能失效(1/3)

- 攻擊手利用掃描目錄，發現網頁後台頁面，並可成功由外部進行存取

```
dirb http://                                    /system -r

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

START_TIME: Wed May 18 14:34:25 2022
URL_BASE: http://                               /system/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

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

GENERATED WORDS: 4585

---- Scanning URL: ht                                .tw/system/ ----
==> DIRECTORY: http:/                               system/system/
==> DIRECTORY: http:/                               system/login/
==> DIRECTORY: http:/                               system/about/
==> DIRECTORY: http:/                               system/contact/
==> DIRECTORY: http:/                               system/css/
==> DIRECTORY: http:/                               system/dashboard/
==> DIRECTORY: http:/                               system/english/
+ http://nckuhhrpc.me                              log (CODE:200|SIZE:83664)
==> DIRECTORY: http:/                               system/images/
+ http:/                                           /system/index (CODE:200|SIZE:20993)
+ http:/                                           /system/index.php (CODE:200|SIZE:20993)
==> DIRECTORY: http:/                               system/js/
==> DIRECTORY: http:/                               system/member/
==> DIRECTORY: http:/                               system/news/
+ http:/                                           ts (CODE:200|SIZE:13)
==> DIRECTORY: http:/                               system/people/
==> DIRECTORY: http:/                               system/plugins/
```

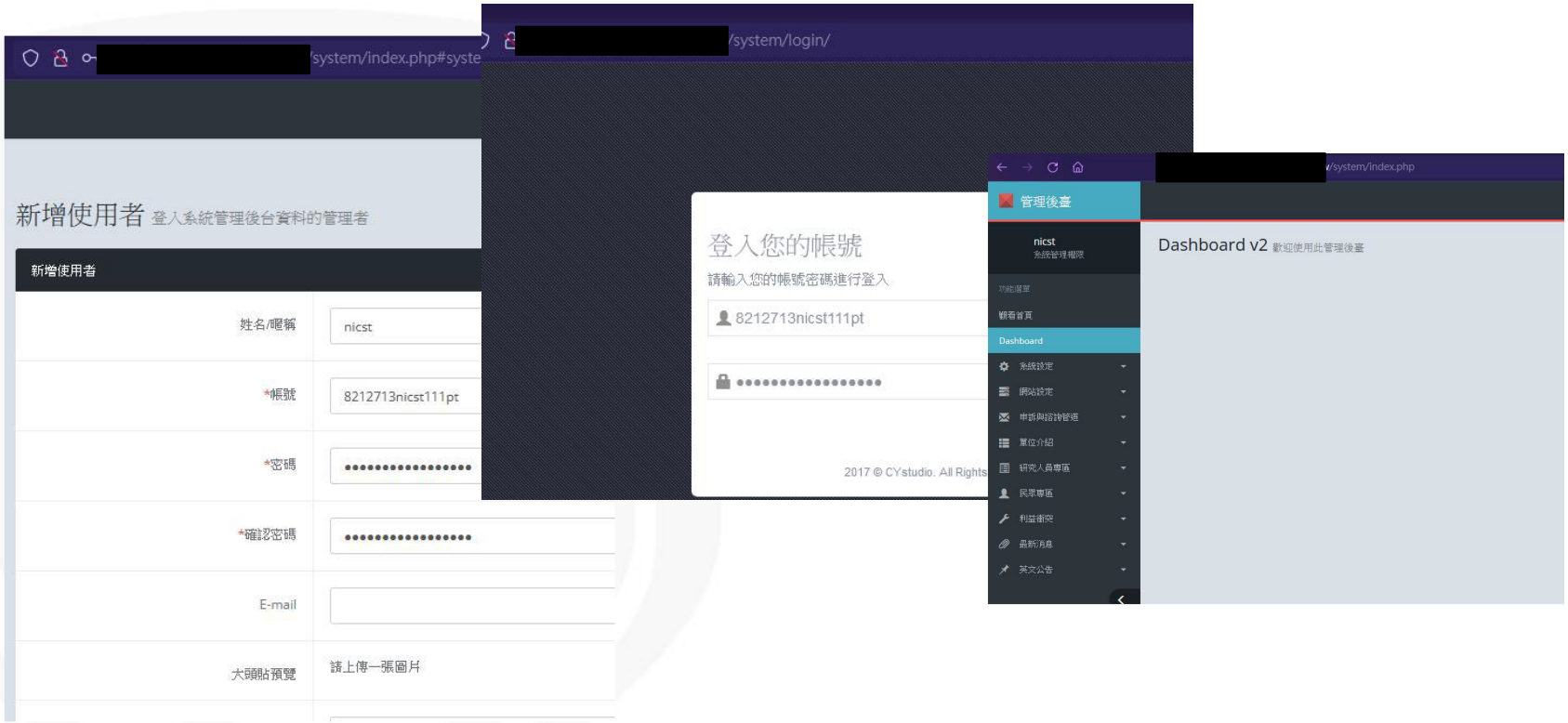
# 案例2 限制存取功能失效(2/3)

- 使用Burp Suite工具攔截封包，發現網頁透過JavaScript程式碼轉導致登入頁面
- 嘗試刪除伺服器端回傳之JavaScript程式碼，成功存取後臺功能頁面



# 案例2 限制存取功能失效(3/3)

- 透過刪除伺服器端回傳之JavaScript程式碼，成功於網頁伺服器上新增使用者



# 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

# 3.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
- 使用之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3 帳號與通行碼相同(1/3)

- 攻擊手瀏覽網頁會員登入頁面，發現會員帳號可使用E-Mail或統一編號登入

# 案例3 帳號與通行碼相同(2/3)

- 攻擊手於網頁內查詢廠商名稱，再以Google搜尋查得廠商統編資訊
- 利用統編資訊進行帳號密碼猜測

# 案例3 帳號與通行碼相同(3/3)

- 成功登入後發現多筆個資

# 未落實通行碼強度檢查機制改善建議

- 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
- 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

# 4.網頁功能頁面未限制存取

# 網頁功能頁面未限制存取樣態

- 以網頁套件進行後台管理上傳圖片功能，功能路徑容易遭攻擊者進行路徑猜測
- 針對網頁套件圖片上傳頁面未限制存取來源，導致任一使用者皆可透過此頁面上傳圖片

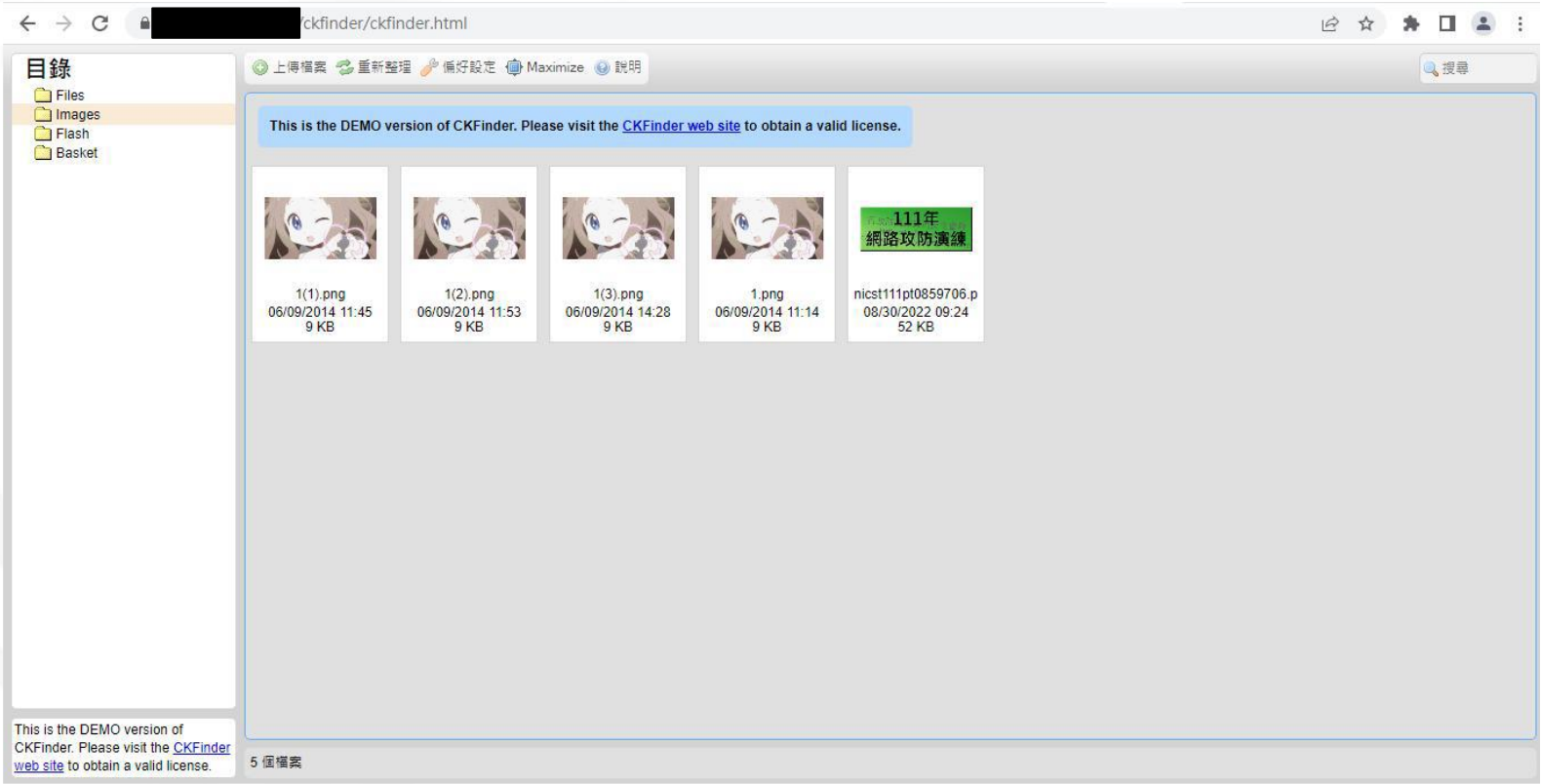
# 案例4 不當使用ckfinder元件(1/3)

- 攻擊手進行路徑掃描，發現含有「ckfinder/」路徑

```
GENERATED WORDS: 4612

---- Scanning URL: ht                                    .tw/ ----
==> DIRECTORY: https:                                    /about/
==> DIRECTORY: https:                                    /About/
==> DIRECTORY: https:                                    /activities/
==> DIRECTORY: https:                                    /aspnet_client/
+ https://pbike.pthg.                                    2|SIZE:175)
==> DIRECTORY: https:                                    /ckeditor/
==> DIRECTORY: https:                                    /ckfinder/
```

# 案例4 不當使用ckfinder元件(2/3)

- 進行路徑猜測「../ckfinder/ckfinder.html」並瀏覽網頁，發現ckfinder檔案上傳頁面，並上傳攻防演練圖片



# 案例4 不當使用ckfinder元件(3/3)

- 成功上傳圖片

# 網頁功能頁面未限制存取改善建議

- 系統開發者
  - 針對網頁套件之預設路徑進行更改，避免攻擊者可輕易猜測路徑進行存取
- 系統管理者
  - 應限制功能頁面之存取來源，若為外部使用者不需使用之功能，應禁止由外部存取該頁面
  - 應避免直接由外網存取系統管理介面，應統一透過內網或透過VPN連線後，進行系統管理介面操作

# 5.使用存在漏洞之套件

# 使用存在漏洞之套件樣態

- 使用網頁套件進行網頁文字編輯或圖片上傳管理，攻擊者可識別套件之版本資訊，進而搜尋並利用該版本存在之已知弱點

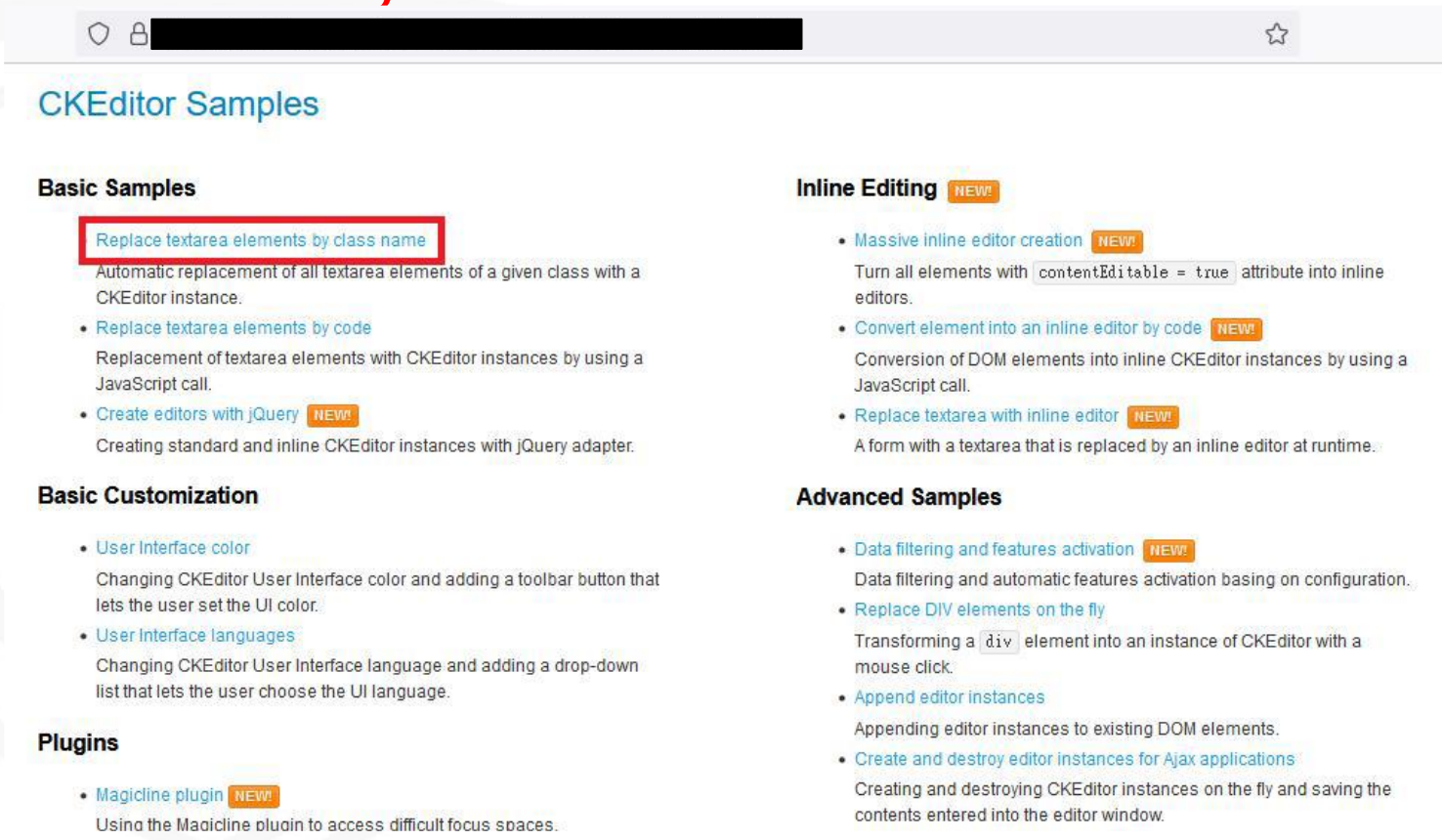
# 案例5 使用存在漏洞之套件(1/4)

- 攻擊手進行路徑掃描，發現含有「ckeditor」路徑

```
---- Entering directo                                    ext/script/ ----
==> DIRECTORY: https:/                                   /ckeditor/
+ https://                                               fig.js (CODE:200|SIZE:2236)
+ https://                                               ples/index.html (CODE:200|SIZE:5845)
+ https://                                               E:200|SIZE:188)
==> DIRECTORY: https:/                                   /fancybox/
==> DIRECTORY: https:/                                   /images/
```

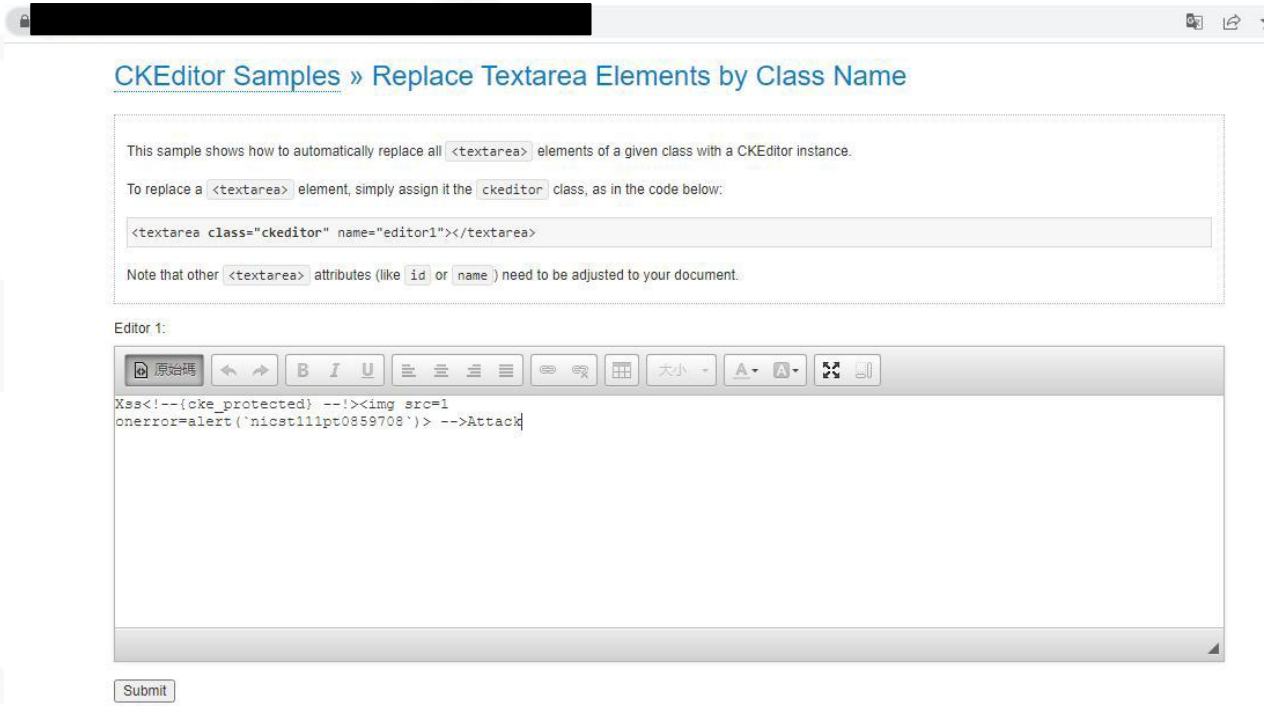
# 案例5 使用存在漏洞之套件(2/4)

- 瀏覽「../ckeditor/samples/index.html」路徑，發現ckeditor頁面，點選「Replace textarea elements by class name」



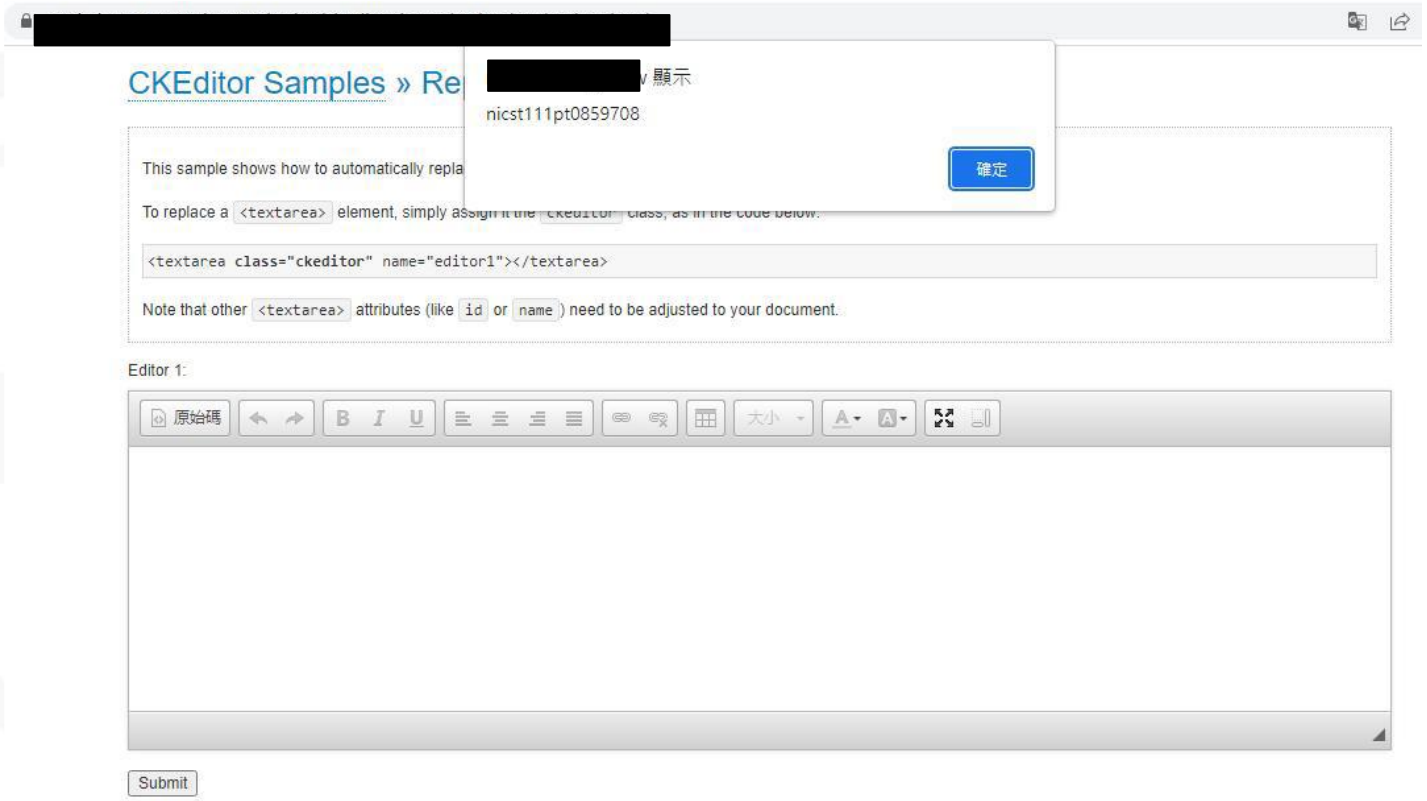
# 案例5 使用存在漏洞之套件(3/4)

- 輸入攻擊語法
  - 攻擊語法：Xss<!--{cke_protected} --!><img src=1 onerror=alert(`nicst111pt0859708`)> -->Attack



# 案例5 使用存在漏洞之套件(4/4)

- 點選「原始碼」按鈕，成功顯示彈跳式視窗



# 使用存在漏洞之套件改善建議

- 系統管理者
  - 針對套件之相關預設頁面應禁止外部存取，或將預設相關頁面移除
  - 定期盤點網頁與伺服器使用之相關套件與程式版本，並進行版本更新與測試，若因版本影響可用性，應針對相關弱點實施緩解措施

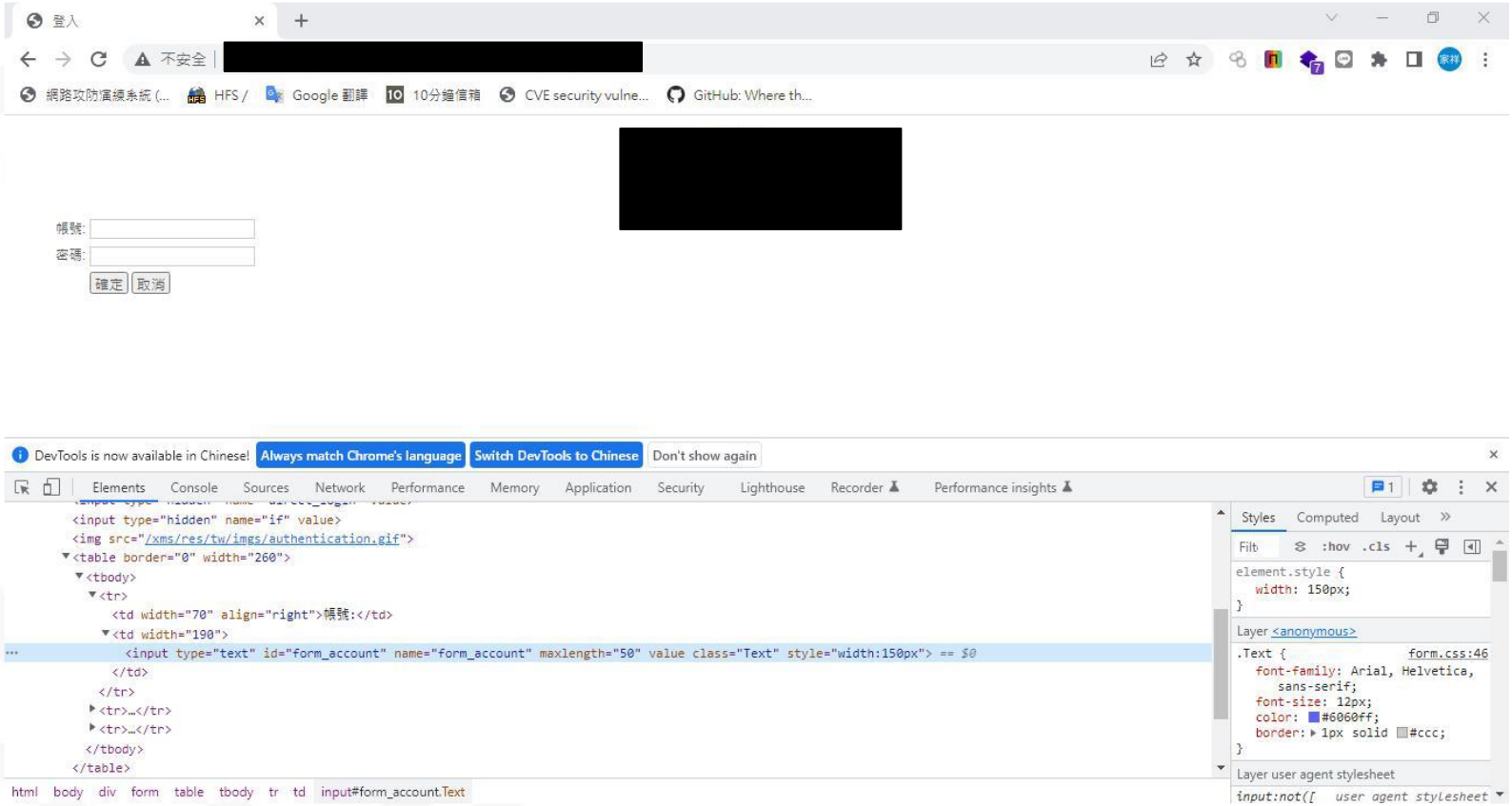
# 6.跨網站腳本攻擊

# 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6 跨網站腳本攻擊(1/2)

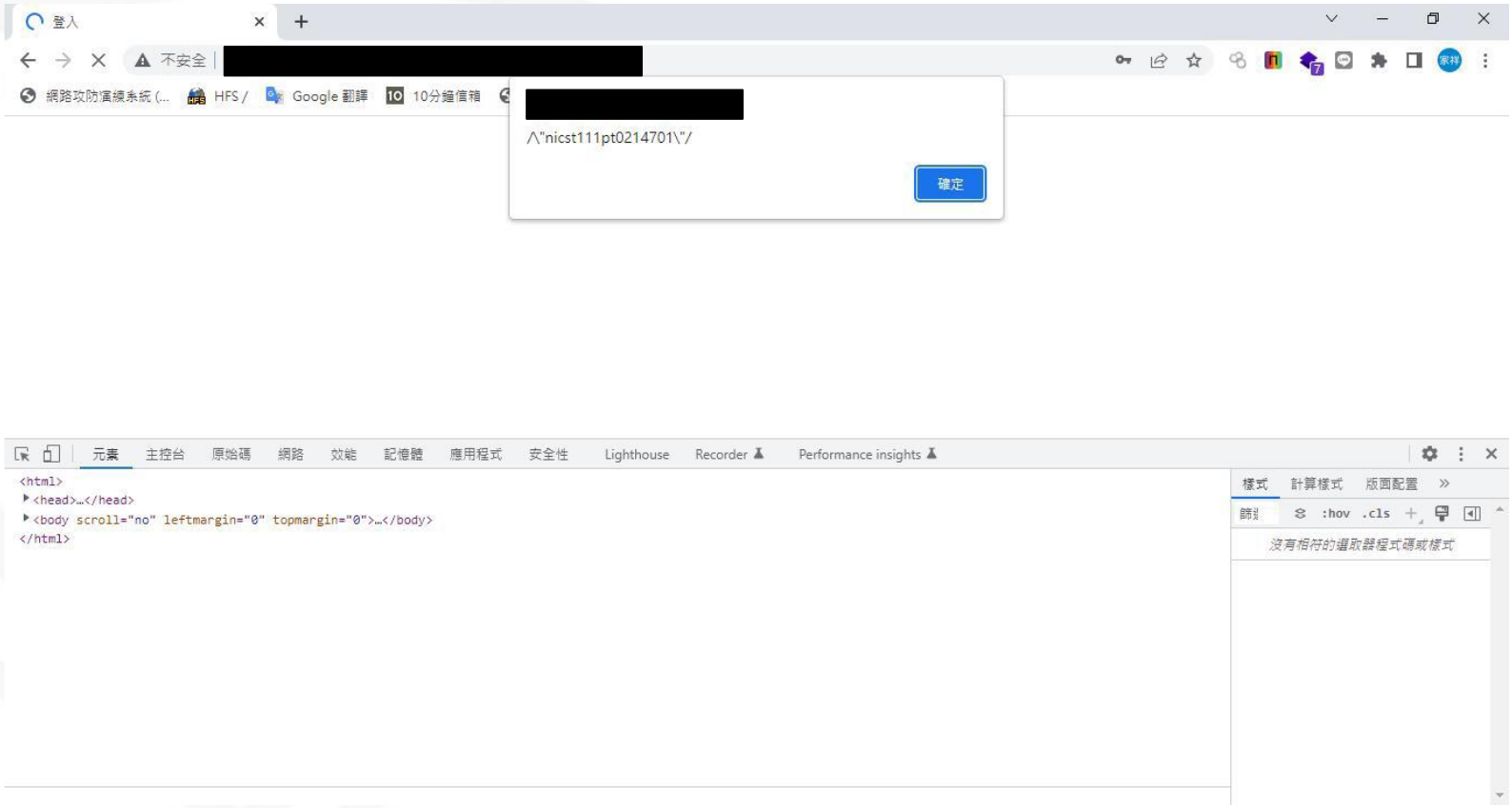
- 攻擊手瀏覽登入頁面，使用開發者工具嘗試更改輸入欄位長度限制



# 案例6 跨網站腳本攻擊(2/2)

- 攻擊手輸入攻擊語法，成功顯示彈跳視窗
  - 攻擊語法：

```
<script>alert(/"nicst111pt0214701"/)</script>
```



# 跨網站腳本攻擊防護建議

- 系統開發者
  - 以白名單限制輸入內容
    - 限定輸入內容[a~z][A~Z][0~9]
    - 限定輸入長度
  - 將字串內容進行編碼
    - 範例：< 轉成 <、" 轉成 "
  - 系統可輸入之位置，不信任任何來源輸入內容，並進行相關控管
  - 引用JavaScript需詳細檢查資料，避免操作DOM過程被帶入惡意指令

# 7.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7 注入漏洞(1/2)

- 攻擊手於網頁登入欄位輸入攻擊語法，嘗試繞過登入驗證


# 案例7 注入漏洞(2/2)

- 成功登入，並可直接修改網頁公開資訊

# 注入漏洞改善建議

- 系統開發者
  - 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66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、11台電腦未落實安全性更新及4台電腦應用程式未更新

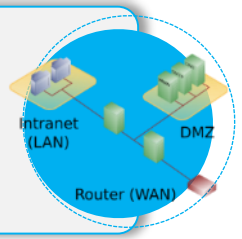
## 核心資通系統安全檢測


- 核心資通系統內網滲透測結果共發現20個高風險、1個低風險弱點，其中61.9%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10個不符合項目

## 物聯網設備檢測

- 物聯網設備檢測結果共發現34個不符合項目，其中47%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」，29.4%為「管理介面身分鑑別使用預設帳號密碼」

## 網路架構檢測




- 網路架構檢測共發現5個高風險、14個中風險、1個低風險及5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

## 組態設定安全檢測


- 共發現1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
- 共發現1台網通設備組態設定未符合
- 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14個不符合項目，其中42.8%為「資料庫傳輸未具有安全機制」

## 網路惡意活動檢視

- 共發現41筆IP中繼站名單未阻擋
- 共發現5筆DN中繼站名單未阻擋

# 連兩年發現之重要檢測結果

| 檢測項目 | 110年與111年共通發現事項 |
| --- | --- |
| 使用者電腦安全檢測 | • 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<br>• 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<br>• 機關所使用服務存在SSL簽章使用不安全之Hash演算法弱點 |
| 物聯網設備檢測 | • 設備的管理介面、Telnet及SNMP服務使用預設帳號密碼<br>• 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 |
| 資料庫安全檢測 | • 資料庫資料為明文資料<br>• 資料庫未設置安全加密傳輸管道 |
| 網路架構檢測 | • 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<br>• 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 |
| 組態設定安全檢測 | • 結果未完全符合機關例外管理清單規定值 |
| 網路惡意活動檢視 | • 機關未確認惡意中繼站名單部署完整性與正確性 |

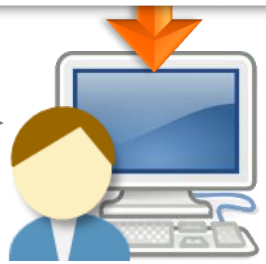
# 使用者電腦安全檢測共同發現事項

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 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、Adobe Reader、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**

發現事項同110年

1. 使用者採用更高強度加密演算法
2. 使用者採用更高安全性加密簽章方式
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)

# 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. 設備管理介面未設定密碼錯誤嘗試次數，容易遭受暴力破解攻擊

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

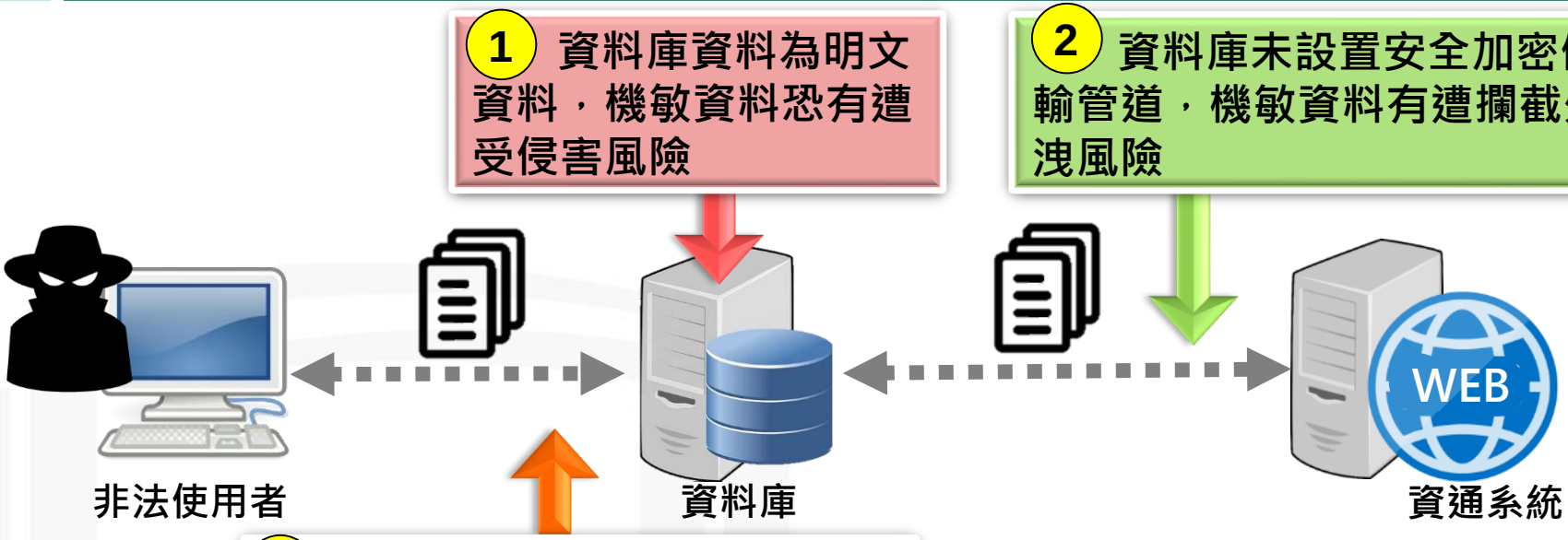
物聯網設備

發現事項1與2同110年

## 改善建議

1. 設備管理者應禁止管理介面使用預設帳號密碼，並關閉非必要服務
2. 設備管理者定期針對物聯網設備韌體與後端服器主機作業系統進行更新
3. 設備管理者應設定與啟用密碼錯誤嘗試次數，避免遭受暴力破解攻擊

# 資料庫安全檢測共同發現事項

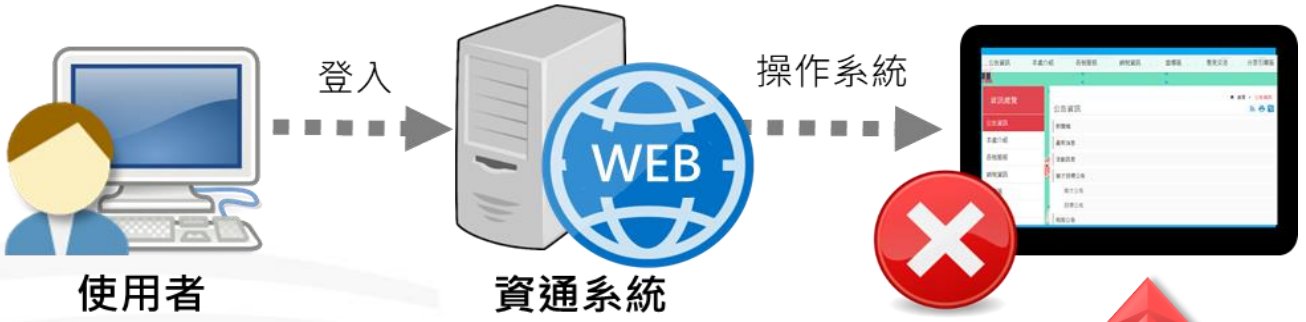



發現事項1與2同110年

**改善建議**

1. DB管理者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. DB管理者針對資料庫設置安全加密傳輸方式，以確保資料傳輸安全性
3. DB管理者重新檢視防火牆規則，僅允許通過申請之使用者可連線至資料庫主機，降低未授權存取之風險

# 核心資通系統安全檢測共同發現事項





資通系統主機

**2** 機關部署之環境未採用最小權限原則，使用者可跨權限存取非授權之資料

**1** 系統存在注入攻擊弱點，使用者可利用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

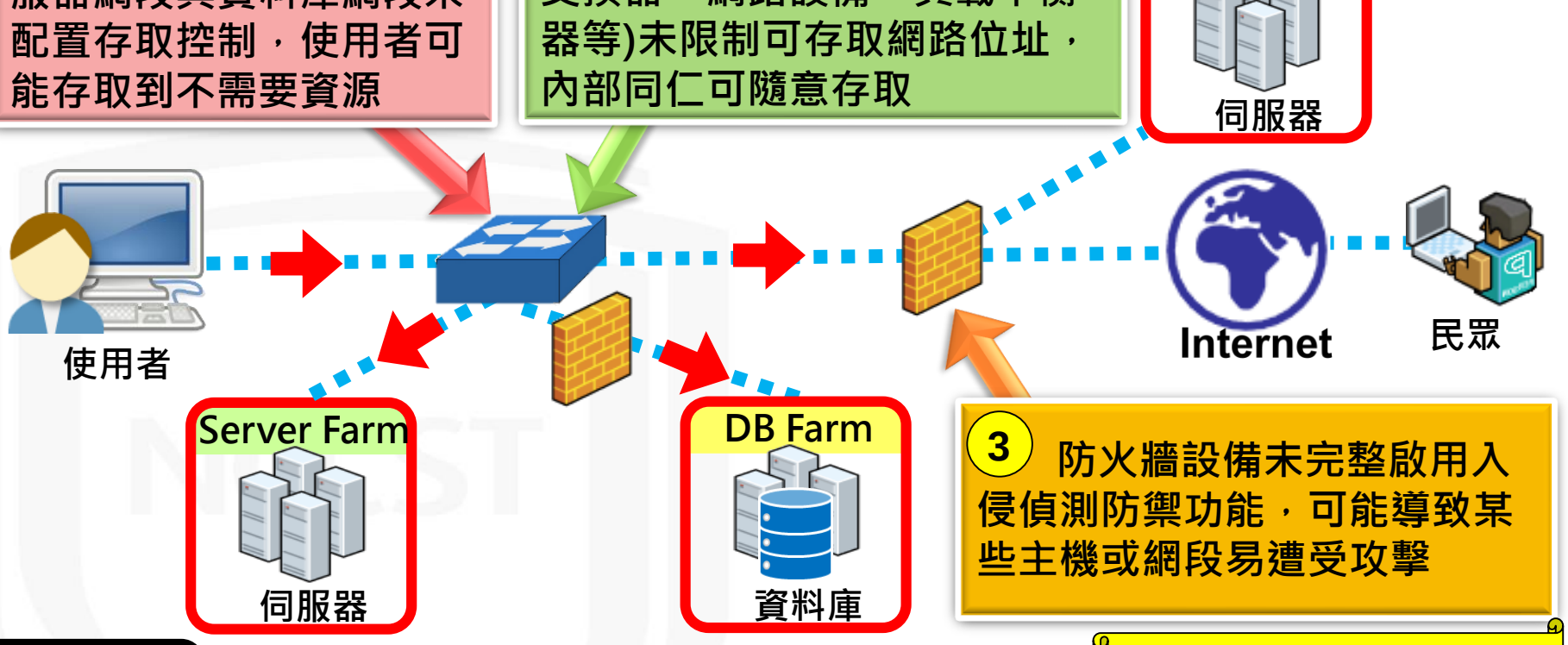
## 改善建議

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
2. 系統維運者依最小權限原則定期審查使用者權限

# 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、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



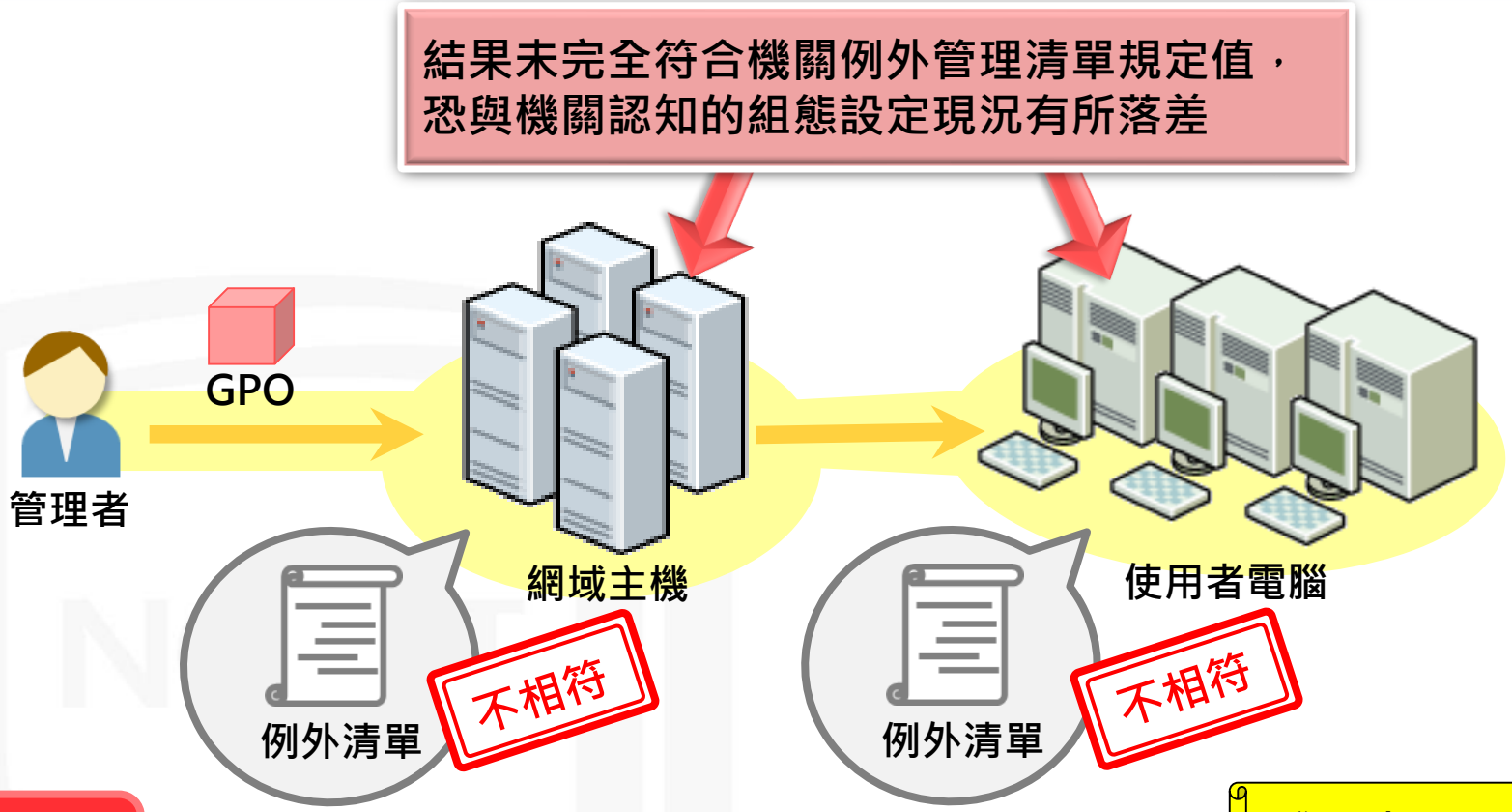

3 防火牆設備未完整啟用入侵偵測防禦功能，可能導致某些主機或網段易遭受攻擊

發現事項1與2同110年

**改善建議**

1. 針對網路區域間之存取，建議網管人員重新檢視防火牆，並設定存取控制規則
2. 針對網路設備存取控制，建議設備管理者限制僅管理人員之IP可存取管理介面
3. 網管人員重新檢視防火牆並全面啟用入侵偵測防禦功能，以提升防護完整性

# 組態設定安全檢測共同發現事項



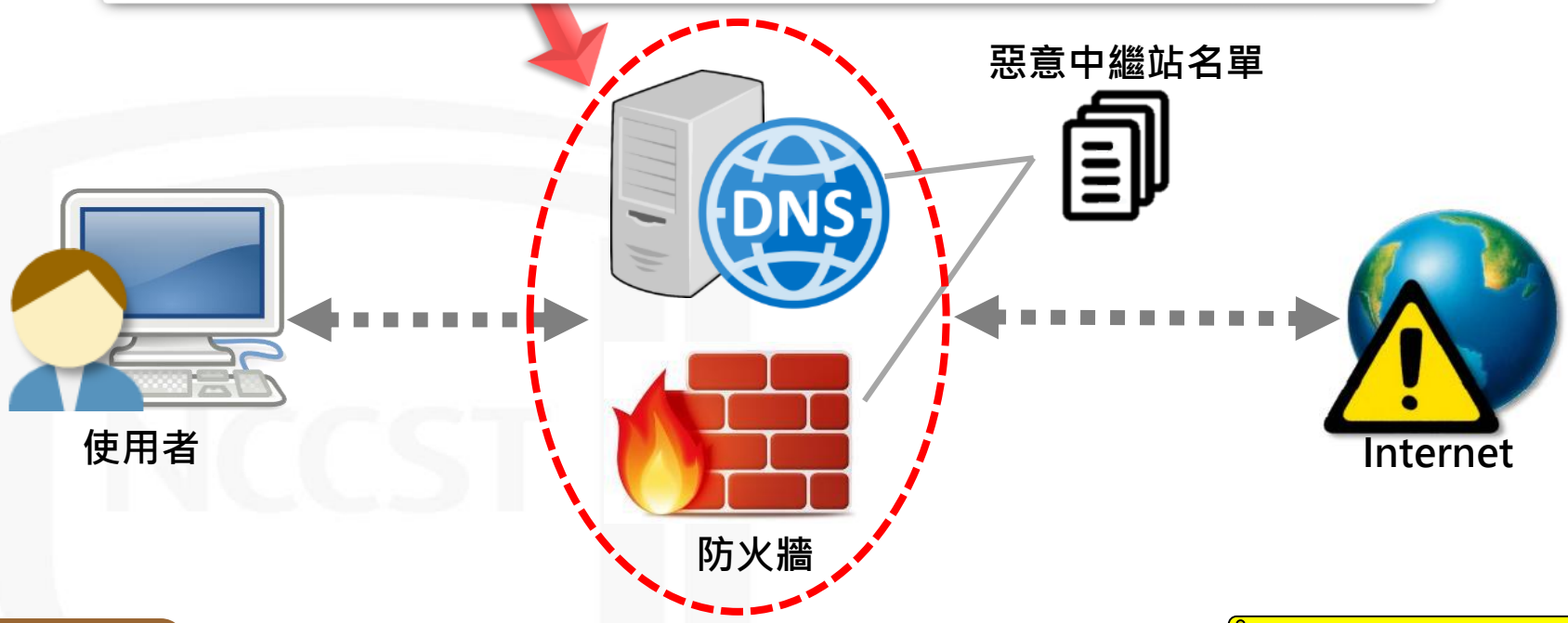

發現事項同110年

**改善建議**

1. GCB導入人員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. 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

# 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




發現事項同110年

**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

- 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
- 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