

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

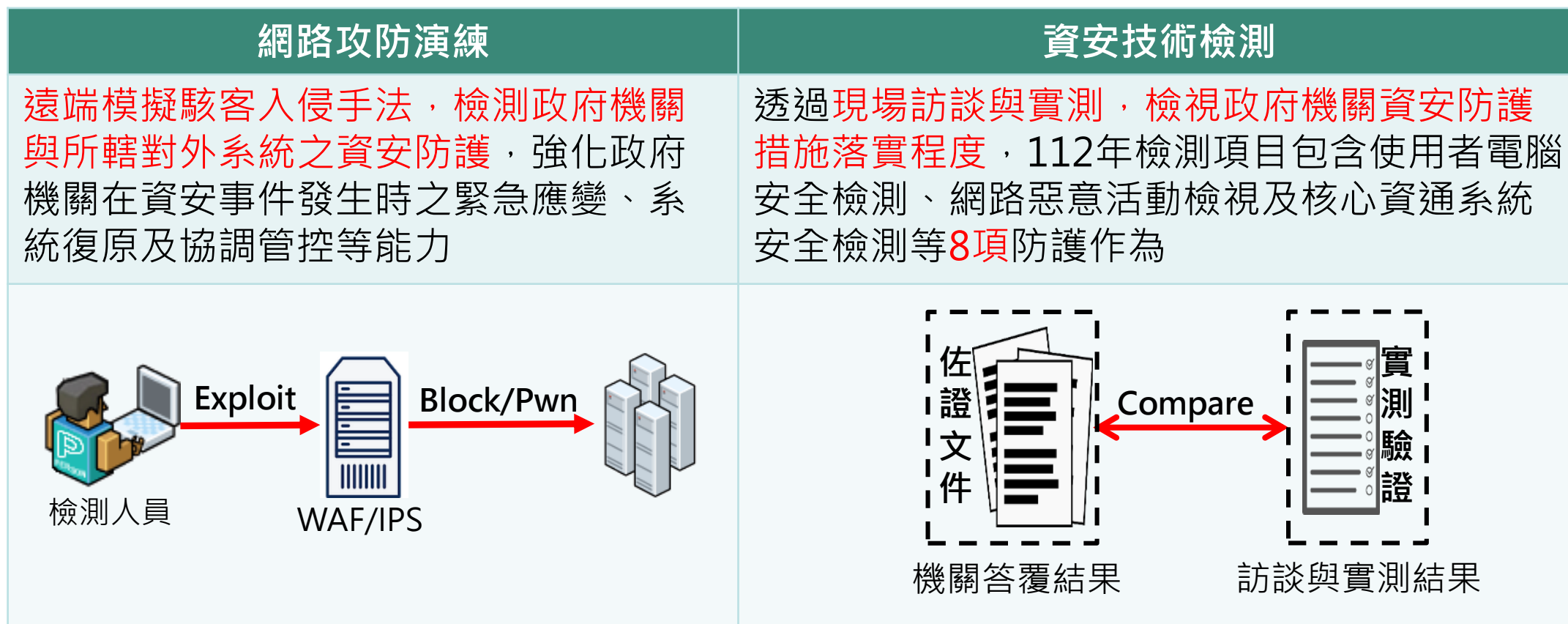
【普通】



- 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
- 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



- 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	認證及驗證機制失效	<ul style="list-style-type: none">• 弱通行碼破解• 透過系統手冊取得帳號通行碼資訊	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 跨網站腳本攻擊• SQL Injection攻擊	<ul style="list-style-type: none">• 竊取使用者資訊• 資料庫資訊外洩
3	無效的存取控管	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

- 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	排名	112年
1	無效的存取控管(26%)	1	認證及驗證機制失效(35.6%)
2	認證及驗證機制失效(25%)	2	注入攻擊(25.8%)
	不安全的組態設定(25%)	3	無效的存取控管(19.3%)
4	危險或過舊之元件(14%)	4	不安全的組態設定(7.7%)
5	注入攻擊(9%)	5	加密機制失效(6.9%) <i>NEW</i>
		6	危險或過舊之元件(2.1%)
6	不安全設計(1%)		不安全設計(2.1%)

網路攻防演練綜合發現

- 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

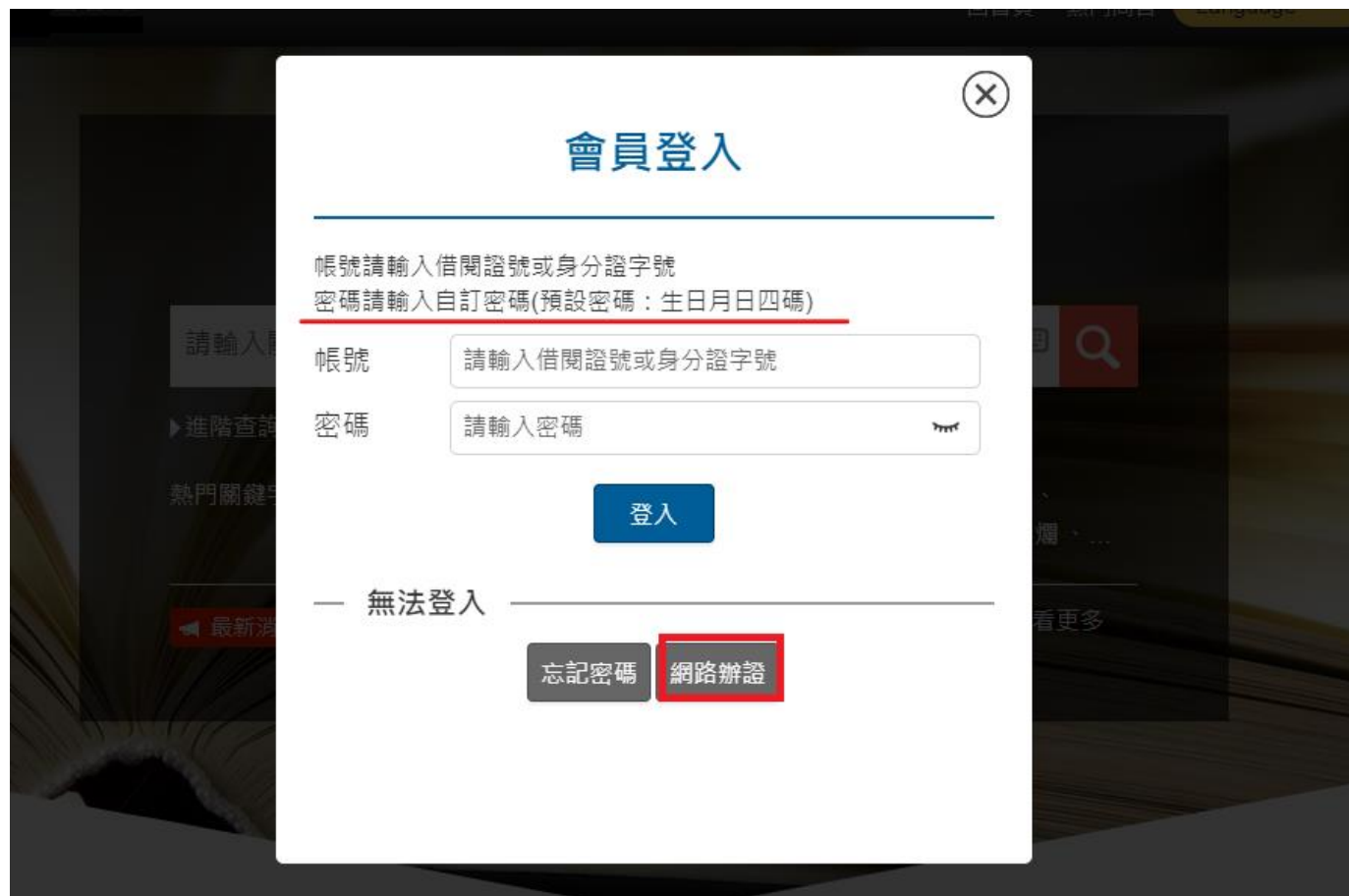
1.未落實通行碼強度檢查機制 (認證及驗證機制失效)

未落實通行碼強度檢查機制樣態

- 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



The screenshot shows a modal window titled "會員登入" (Member Login). It contains the following text and elements:

- Header: 會員登入 (Member Login)
- Instructions: 帳號請輸入借閱證號或身分證字號 (Account: please enter library card number or ID number); 密碼請輸入自訂密碼(預設密碼: 生日月日四碼) (Password: please enter your custom password (default password: birthday month and day four digits)).
- Form fields: 帳號 (Account) with placeholder "請輸入借閱證號或身分證字號"; 密碼 (Password) with placeholder "請輸入密碼" and a visibility toggle.
- Buttons: 登入 (Login), 忘記密碼 (Forgot Password), and 網路辦證 (Online Registration).
- Footer: 無法登入 (Cannot login).

The password hint "(預設密碼: 生日月日四碼)" is underlined in red in the original image, and the "網路辦證" button is highlighted with a red box.

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

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer

1 x 2 x 3 x **5 x** +

Positions Payloads Resource Pool Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 12

Payload type: Numbers Request count: 372

? Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 01

To: 12

Step: 1

How many:

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder

1 x 2 x 3 x **5 x** +

Positions Payloads Resource Pool Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 31

Payload type: Numbers Request count: 372

? Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 01

To: 31

Step: 1

How many:



● 成功登入後發現讀者個資

<ul style="list-style-type: none">變更密碼待繳費用/罰則紀錄借閱證線上掛失 <hr/> <p>我的閱讀紀錄</p> <hr/> <p>我的書櫃</p> <hr/> <p>歷史紀錄</p>	讀者姓名	張■■■	讀者證號	11■■■■15
	密碼	0411	辦證館別	■■■■
	讀者性別	男(Male)	生日	19■■■1
	身分證字號	P1■■■■2	讀者類型	一般讀者
	有效期限	2038/09/13		
	借閱證類型	正常使用		
	聯絡方式			
	戶籍地址	雲林縣 ■■■■ 重■■■■號	通訊地址	雲林縣 ■■■■ 重■■■■號
	市內電話	05■■■■6	行動電話號碼	09■■■■91
	電子信箱		常用電子信箱	

案例1-2 利用通行碼提示暴力破解(1/2)



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

- 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

Openfind™
MAIL2000

帳號：
m[redacted]e

密碼：
...

錯誤 -- 輸入帳號或密碼錯誤，請重新輸入

密碼提示：電話m096[redacted]

認證資訊檢查失敗，請重新輸入帳號及密碼，繼續您未完成的工作。

登入

Copyright © Openfind Information Technology INC. All rights reserved.

Openfind™
MAIL2000

帳號：
m[redacted]e

密碼：
m09[redacted]

錯誤 -- 輸入帳號或密碼錯誤，請重新輸入

密碼提示：電話m09[redacted]

認證資訊檢查失敗，請重新輸入帳號及密碼，繼續您未完成的工作。

登入

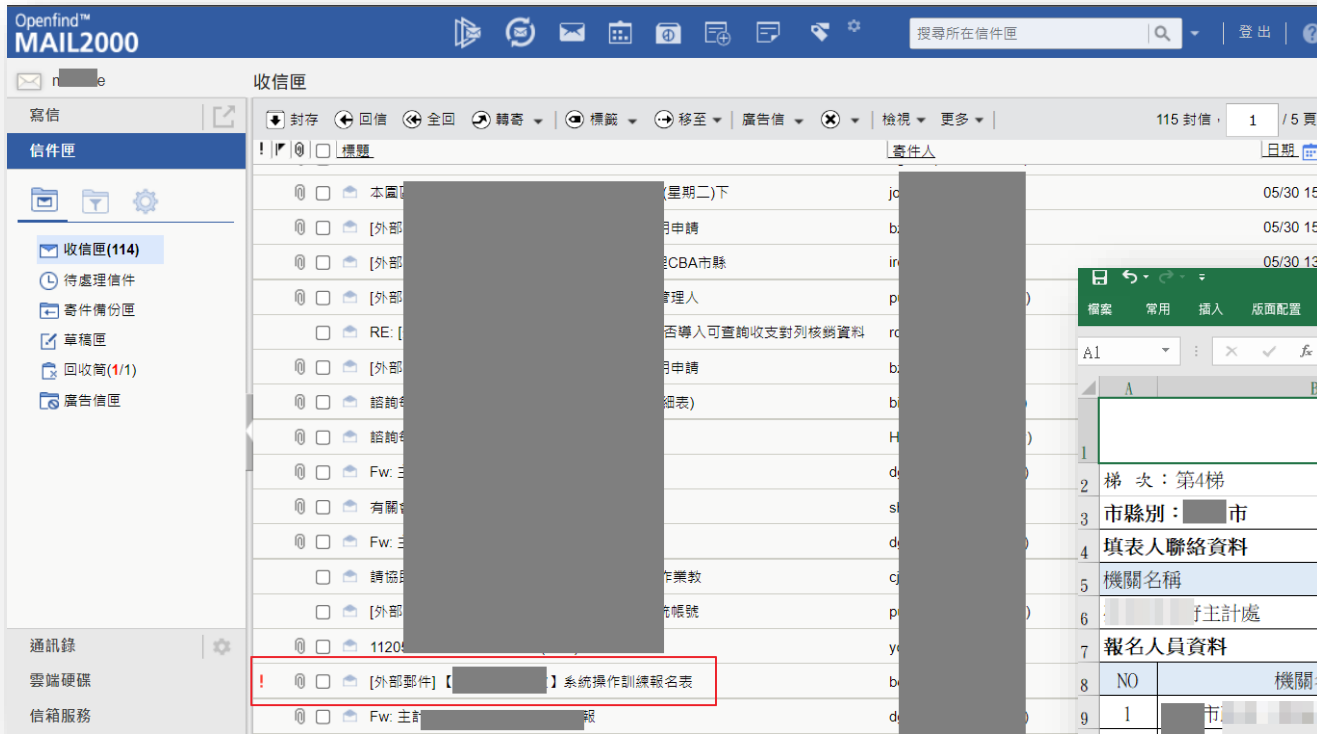
Copyright © Openfind Information Technology INC. All rights reserved.

案例1-2 利用通行碼提示暴力破解(2/2)



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

- 登入成功，並可檢視信件內容



Excel spreadsheet titled "直轄市及縣(市)公務機關會計月報電子化傳輸試辦作業 第1至5梯系統操作訓練報名表".

報名人員資料

NO	機關名稱	職稱	姓名	身分證字號	聯絡電話	電子郵件	
1	市	會計員	柯	M2	2289111分機17008	s1	.gov.tw
2	市	科員	歐	B2	2289111分機11083	ou	.gov.tw
3	市	辦事員	林	B2	2289111分機11085	lc	.gov.tw
4	市	佐理員	呂	L1	9	ba	.gov.tw
5	市	科員	張	E1	0	yi	.gov.tw
6	市	業務助理	陳	Q2	2289111分機39456	lc	.gov.tw
7	市	約用人員	謝		2289111分機50007	hb	.gov.tw
8	市	工友	徐		2289111分機50009	ca	.com.tw
9	市	會計主任	蘇	B2	2289111分機13503	nt	.gov.tw

- 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)

- 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)

- 利用Google Hacking發現「無標題文件」網頁



The screenshot shows a website's '資訊網' (Information Network) page. The page features a navigation bar with links like '回首頁', '網站導覽', '意見信箱', and 'Q&A'. Below the navigation bar is a table with the following columns: '申請學校', '申請計畫名稱', '111年度計畫申請審查意見', '110年度計畫結案審查意見', '綜合意見', and '學校回應'. The table contains several rows of data, with the first row highlighted in blue. The table content is as follows:

申請學校	申請計畫名稱	111年度計畫申請審查意見 (審查委員對本年度各項工作項目意見)	110年度計畫結案審查意見	綜合意見 (此欄意見為審查委員回答各項評分意見)	學校回應
[redacted]	多元培力，職涯卓越	(一)社團增進—多元培育，適性揚才--1.社團與職涯經驗分享： (一)社團增進—多元培育，適性揚才--2.職能體驗系列活動： (二)生涯加值—洞悉職場，健全職涯--1.職場風向球： (二)生涯加值—洞悉職場，健全職涯--2.職場軟實力： (二)生涯加值—洞悉職	(一)社團增進—多元培育，適性揚才--2.社團實務論壇： (二)生涯加值—洞悉職場，健全職涯--1.業師開講： (二)生涯加值—洞悉職場，健全職涯--2.職涯規劃： (二)生涯加值—洞悉職場，健全職涯--3.求職實戰力： (一)社團增進—多元培	委員評分項1.特色主題三年中長期發展計畫之發展性與延續性 委員評分項2.特色主題計畫之具體執行內容及其可達成效益程度 委員評分項3.教育部獎補助私立技專校院整體發展經費用於學生事務與輔導相關設備執行成效表(表20)	【回應2022年審查意見】 【回應2021年結案審查意見】 【學校回應綜合意見】

案例2-1 注入漏洞(2/3)

- 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

```
Database: ██████████
Table: users_account
[775 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| id      | telephone | fax      | user_level | email                               | name      | passwd      | school | job_level |
+-----+-----+-----+-----+-----+-----+-----+-----+
[15:55:13] [WARNING] console output will be trimmed to last 256 rows due to large table size
| user1  2 | ██████████ | 8█████████ | 6 | ██████████@mail.█████████/tw | 饒█████████ | 1█████████0 | 1005 | 專員 |
| 2 | ██████████ | 5656-2048 | 3 | ██████████ | ██████████ | ██████████ | 1005 | 專員 |
| user1  3 | ██████████ | N█████████ | 3 | ██████████038@mail.█████████/tw | ██████████處 | 9█████████1 | 1005 | 專員 |
| N█████████ | ██████████ | ██████████ | 3 | ██████████ | ██████████ | ██████████ | 1006 | 學長 |
| user1  1 | ██████████ | 0█████████ | 3053 | ██████████15@█████████.tw | 李█████████ | 1█████████1 | 1006 | 學長 |
| 0 | ██████████ | 8610511*1 | 4 | ██████████ | ██████████ | ██████████ | 1006 | 學聘組員 |
| user1  2 | ██████████ | 0█████████ | 3053 | ██████████4@█████████.tw | 許█████████ | 1█████████0 | 1006 | 學聘組員 |
| 0 | ██████████ | 8610511#1 | 3 | ██████████ | ██████████ | ██████████ | 1007 | 學 |
| user1  1 | ██████████ | 0█████████ | 029 | ██████████n@█████████.tw | 游█████████ | 1█████████7 | 1007 | 學 |
| 0 | ██████████ | 4517250轉 | 4 | ██████████ | ██████████ | ██████████ | 1007 | 組 |
| user1  2 | ██████████ | N█████████ | 3 | ██████████niau@█████████.tw | 蕭█████████ | f█████████81241 | 1007 | 組 |
| 0 | ██████████ | 24517250轉 | 3 | ██████████ | ██████████ | ██████████ | 1008 | 學書 |
| user1  1 | ██████████ | 0█████████ | 0020 | ██████████nen@█████████.tw | 陳█████████ | 1█████████6 | 1008 | 學書 |
| 0 | ██████████ | 6328001轉 | 4 | ██████████ | ██████████ | ██████████ | 1008 | 學員 |
| user1  2 | ██████████ | 0█████████ | 0020 | ██████████n@█████████.tw | 林█████████ | 1█████████9 | 1008 | 學員 |
| 0 | ██████████ | 6328001-1 | 3 | ██████████ | ██████████ | ██████████ | 1009 | 組長 |
| user1  1 | ██████████ | 0█████████ | 118 | ██████████ang@mail.█████████.tw | 王█████████ | 14█████████ | 1009 | 組長 |
| 03 | ██████████ | 18800#200 | 4 | ██████████ | ██████████ | ██████████ | 1009 | 專 |
| user1  2 | ██████████ | 0█████████ | 118 | ██████████2003@mail.█████████.tw | 高█████████ | 1█████████5 | 1009 | 專 |
| 0 | ██████████ | 118800#20 | 3 | ██████████ | ██████████ | ██████████ | 1010 | 學 |
| user1  1 | ██████████ | 0█████████ | 233 | ██████████chih@█████████.tw | 劉█████████ | 1█████████1 | 1010 | 學 |
| 0 | ██████████ | 638800 | 4 | ██████████ | ██████████ | ██████████ | 1010 | 研 |
| user1  2 | ██████████ | 0█████████ | 8233 | ███████████████████7@█████████.tw | 王█████████ | s█████████ | 1010 | 研 |
| 0 | ██████████ | 4638800轉 | 3 | ██████████ | ██████████ | ██████████ | 1010 | 研 |
```

案例2-1 注入漏洞(3/3)

- 利用取得之帳號密碼成功登入，並取得系統管理者權限

院 資訊網

您是第 1302934 位訪客 協助國內私立大專校院推動學生事務與輔導活動，落實學校學生事務與輔導工作，提昇學校學生

帳號登入

帳號: u: [redacted] 2
密碼: [redacted]
驗證碼: msn2

點擊圖片可以更換驗證碼

登入

活動快遞

案，申報時間為112年1月1日至112年2月7日。請依謝。
2 教育部將補助私立技專校院整體發展經費核配及

最新消息 | Latest News

相關辦法 | Laws and Regulations

教育部補助助及委辦經費核撥結報作業要點
教育部補助私立大專校院學生事務與輔導創新工作專業人力要點108
教育部補助(捐)助及委辦計畫經費編列基準表
教育部獎勵補助私立技專校院整體發展經費核配及申請要點
教育部獎勵補助私立大學校院校務發展計畫要點
教育部及所屬機關(構)辦理各類會議講習訓練與研討(習)會管理要點

學生事務與輔導工作補助款

本年度
前一年度
補助款修訂

審查意見查詢
依複審意見修訂本年度計畫
依審查意見修訂前一年度計畫結果
(前一年度執行成效、統計表)
列印本年度補助款修訂報部文件
本年度計畫預算變更

補助款相關訊息

補助經費申請(流程圖)

年度	狀態	申請經費	申請日期
112	核定完畢	(以公文為準)	2023-01-12 09:47:29

【112年度學生事務與輔導工作補助款各階段時程通知】
*請注意藍色字的部分，表示正在進行的階段

各階段名稱	開始時間	結束時間
本年度計畫申請	2023-1-1	2023-2-7
本年度計畫申請審查	2023-2-15	2023-3-6
本年度計畫修訂	2023-3-24	2023-4-30
本年度預算變更	2023-5-1	2023-12-20
前一年度計畫結案	2023-1-1	2023-2-7
前一年度計畫結案審查	2023-2-15	2023-3-6

個人資料維護
修改個人資料
學輔經費使用說明研討會(特色主題計畫成果分享PPT)
學輔經費使用說明研討會-分組及綜合座談紀錄問答
「私立大專校院學生事務與輔導經費使用說明會-問與答」專區

學校資料維護
查詢(下載空白表格)
請選擇 年
(112年需填寫資料填寫情況)

回首頁 網站導覽 意見信箱 Q&A

資訊網

人員 學校財團法人 大學 護 登入

案例2-2 注入漏洞(1/2)

- 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

```
← → ↻ ⚠ 不安全 | ██████████.tw/robots.txt

User-agent: *
Disallow: /CDEC/
Disallow: /Clerk92/
Disallow: /EKG/
Disallow: /Gene_OPD/
Disallow: /Hema/
Disallow: /HemaBM/
Disallow: /HIE/
```



案例2-2 注入漏洞(2/2)

- 成功登入網站後，可取得特種個資

資料夾 病史 發展遲緩 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

[修改](#)

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

- 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)

- 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

The image shows a web browser window displaying a login page. The page title is "系統客" (System Guest). The login form includes fields for "帳號:" (username) and "密碼:" (password), along with buttons for "登入" (login), "忘記密碼" (forgot password), "最新消息" (latest news), and "加入會員" (join member). The "加入會員" button is currently hidden. The browser's developer tools are open, showing the HTML source code. A red box highlights the following line in the source code:

```
 == $0
```

A red arrow points from this line in the source code to the "加入會員" button in the login form, indicating that removing the "display: none" style attribute would make the button visible.

案例3-1 限制存取功能失效(2/4)

- 利用隱藏之功能建立帳號並成功登入

基本資料

前有 *符號必填，密碼預設與帳號相同，登錄後可修改密碼及基本資料

* 帳號	niccpt08513	* 姓名	王小明
* 單位	593301 高級中學	* 級別	不分
* 處室	不分		
訂閱電子報	否		
* 聯絡電話	0222222222		
* EMAIL	nccstet@gmail.com		

姓名: 王小明
身分: 學校人員
登出 修改密碼
修改個人資料

最新消息
疑難諮詢
系統建議

最新消息

所有類別 重要性 下頁 第 1 / 8 頁

日期	類別	標題	重要性	附
1120612	公告	nic112pt08510	一般	
1120612	公告	nic112pt08517	一般	
1120530	公告	(已完成修正)校務系統暫時無法登入	急件	
1120517	公告	5/17 中午十二點~一點將進行校務系統改版	一般	
1120511	公告	第六學期成績單無法產出pdf 已修正	急件	

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
187 </script>
188 <script type="text/javascript" src="/qanda/plugins/ech.multiselect/jquery.multiselect.filter.js">
</script>
189
190
191 <link rel="stylesheet" type="text/css" href="css/menulayout.css" />
192 <link rel="stylesheet" type="text/css" href="css/portlet.css" />
193 <link rel="stylesheet" type="text/css" href="css/MetroJs.css" />
194 <link rel="stylesheet" type="text/css" href="css/style.css" />
195 <link rel="stylesheet" href="/qanda/css/themes/start/jquery-ui.min.css" type="text/css" media="all" />
196
197 <script type="text/javascript">
198 $(function(){
199   var mo = $.evalJSON(' [{"n":"news","o":"Q0108S"}, {"n":"qa","o":"Q0204S"}, {"n":"plus","o":"Q0208S"} ] ');
200   if(mo.length){
201     $.each(mo, function(i,o){
202       $('').appendTo("#funcBar").css("cursor","pointer").click(function(){
203         $("#content").html('').load(o.o+'_load.action',{
204           session_key: 'ac244a01-db5a-4c3d-8439-b546f3e68162'
205         });
206       });
207     });
208   }
209 }
```

案例3-1 限制存取功能失效(4/4)

- 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

① 客服網服務網

管理員/客服人員 基本資料

前有 *符號必填，密碼預設與帳號相同，登錄後可修改密碼及基本資料

* 管理者	是
* 帳號	nics112pt08513
* 單位	613301 高級中
* 處室	不分
* 聯絡電話	0222222222
* EMAIL	nccstet@gmail.com

② 歡迎登入

帳號： nics112pt085

密碼：

X5F7 X5F7

登入 忘記密碼

▶ 最新消息

③ 使用者資訊

姓名： 王小明
身分： 廠商人員

登出 修改密碼
修改個人資料

▶ 最新消息
▶ 疑難諮詢
▶ 系統建議
▶ 加入管理員
▶ 作業管理

最新消息 所有類別 重要性

日期	類別	
1120612	公告	nics112pt08510
1120612	公告	nics112pt08517
1120530	公告	(已完成修正)校務系統暫時無法登入
1120517	公告	5/17 中午十二點~一點將進行校務系
1120511	公告	第六學期成績單無法產出pdf 已修正

案例3-2 限制存取功能失效(1/3)

- 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

開始使用

還沒有帳號?

若您尚未申請「[redacted] 共通服務平台」帳號，請先點選下方的申請帳號按鈕進入，完成帳號申請後即可直接登入使用。

申請帳號

登入系統

USER NAME 帳號：
leeqqleeqq123

PASSWORD 密碼：
●●●●●●

登入

登入說明：
如果您已有帳號，請直接輸入帳號及密碼登入系統。
若您忘記密碼，請點此 [忘記密碼](#)。
帳號因連續輸入3次錯誤密碼遭停用，請洽系統管理員。

人員： 帳號 查詢 [全選] [取消]

組 織	項次	姓名	帳號	代理設定
市政府				
長室	1	[redacted] admin	0	min [
書長室	2	機關系統管理者	1	min [
府民政局	3	系統管理者	0	min [
府財政局	4	系統管理者	0	min [
府教育局	5	系統管理者	0	min [
府工務局	6	系統管理者	1	min [
府社會局	7	系統管理者	1	min [
府警察局	8	系統管理者	1	min [
府衛生局	9	系統管理者	1	min [
府環境保	10	系統管理者	1	min [
政府地政局	11	系統管理者	1	min [
政府經濟發	12	系統管理者	1	min [
政府新聞局	13	系統管理者	1	min [
政府主計處	14	系統管理者	1	min [
政府人事處				
政府研究發				

案例3-2 限制存取功能失效(2/3)

- 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**

基本資料設定

《請確認欄位資料，按[確定儲存]完成註冊程序》

使用者基本資料

內部機關代碼	18AV	機關名稱	新	出版科
帳號	le...eqq123	姓名	林	
密碼	<input type="password"/>	單位	<input type="text"/>	<input type="button" value="修改"/>
憑證	<input type="text"/>	影像章	<input type="text"/>	<input type="button" value="設定"/>

樹閣下拉式選項設定

主要發文機關資訊

主要發文機關	政府	<input type="button" value="更新"/>	
郵遞區號	1	*地址	路2號
發文字	<input type="text"/>		
稿署名	<input type="text"/>		
署名	<input type="text"/>		

次要發文機關資訊

次要發文機關1	<input type="text"/>	<input type="button" value="刪除"/>	
郵遞區號	<input type="text"/>	*地址	<input type="text"/>
發文字	<input type="text"/>		
稿署名	<input type="text"/>		
署名	<input type="text"/>		

聯絡方式

*承辦人姓名	林	承辦人單位	新	版科二股
職稱	學生	*電話	123	
傳真	<input type="text"/>	電子信箱	le...ean123@gmail.com	

Intercept HTTP history WebSockets history Options

Request to https://...tw:443 [223.200.100.43]

Forward Drop Intercept is on Action Open

Pretty Raw Hex

```
1 POST /kw//maintain/asp/query_user.aspx HTTP/1.1
2 Host: ...gov.tw
3 Cookie: _ga_JRJVWC9DZC=GS1.1.1690855255.1.0.1690855256.0.0.0; _ga_QJNNLFPCLY=GS1.1.1693810976.2.1.1693811068.0.0.0; _ga_VZG8NN_ga_JCXCXWDC1J=GS1.3.1693274846.1.0.1693274846.0.0.0; ASP.NET_SessionIDCEADRASB=ENKEDGGCFMFBKPMIEOLDMFH; _gid=GA1.3.348861ID=c1fe62686129ee4f:T=1693811011:RT=1693811011:S=ALNI_MYsYEg8EWwGS1.1.1693811005.1.0.1693811005.0.0.0
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
5 Accept: */*
6 Accept-Language: zh-TW, zh;q=0.8, en-US;q=0.5, en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: text/xml
9 Content-Length: 99
10 Origin: https://...gov.tw
11 Referer: https://...gov.tw/kw/common/...data.htm
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: close
17
18 <REQUEST>
19 <USER_ID>
20 10
21 </USER_ID>
22 <USER_NAME>
23 </USER_NAME>
24 <USER_ACCOUNT>
25 0...min
26 </USER_ACCOUNT>
27 </REQUEST>
```

主要發文機關資訊

*主要發文機關	政府	<input type="button" value="更新"/>	
郵遞區號	1	*地址	路2號
發文字	<input type="text"/>		
稿署名	局長	<input type="text"/>	
署名	局長	<input type="text"/>	

次要發文機關資訊

次要發文機關1	<input type="text"/>	<input type="button" value="刪除"/>	
郵遞區號	<input type="text"/>	*地址	路2號
發文字	<input type="text"/>		
稿署名	市長	<input type="text"/>	
署名	市長	<input type="text"/>	

聯絡方式

*承辦人姓名	局系統管理者	承辦人單位	局
職稱	<input type="text"/>	*電話	039596321
傳真	<input type="text"/>	電子信箱	le...eqq123@gmail.com

預設匯出目錄

	主檔目錄	附件目錄
TXT(文字檔)	c:\eic\ext...t\bdt\	c:\eic\ext...t\bdt\attach\
DI(電子公文)	c:\eic\ext...t\di\	c:\eic\ext...t\di\attach\

預設電子交換目錄

	主檔目錄	附件目錄	發文紀錄目錄
第一類	發文(加密) c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc
	發文(不加密) c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc
第二類	發文(加密) c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc
	發文(不加密) c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc	c:\Program Files\B...fg\Sc
第三類	全國布告欄		
	對外布告欄		
	對內布告欄		

D編碼方式 big5 Unicode

- 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

- 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)

- 攻擊者創建新帳號，並利用其編輯圖片功能上傳檔案

【自行車資料Bicycle Data】

新增一筆 (可新增多筆資料)(add data) multiple entries may be added

廠牌Brand	車種Vehicle Type	車身顏色Bicycle color	目前車輛狀態Bicycle status	功能 Function
G	公路車	黑	正常	編輯Edit 刪除Delete

* 車身號碼Bicycle Serial Number 111111
(長度不可少於11碼) 車身號碼

* 防竊貼碼Bicycle Prevent Steal Number :A1070000000
(首字為A, 例如:A1070000000 / 長度不可少於11碼)(No fewer than 11 characters) 防竊貼碼貼哪裡(參考範例)Photo (See Example)

請輸入驗證碼 Enter Captcha

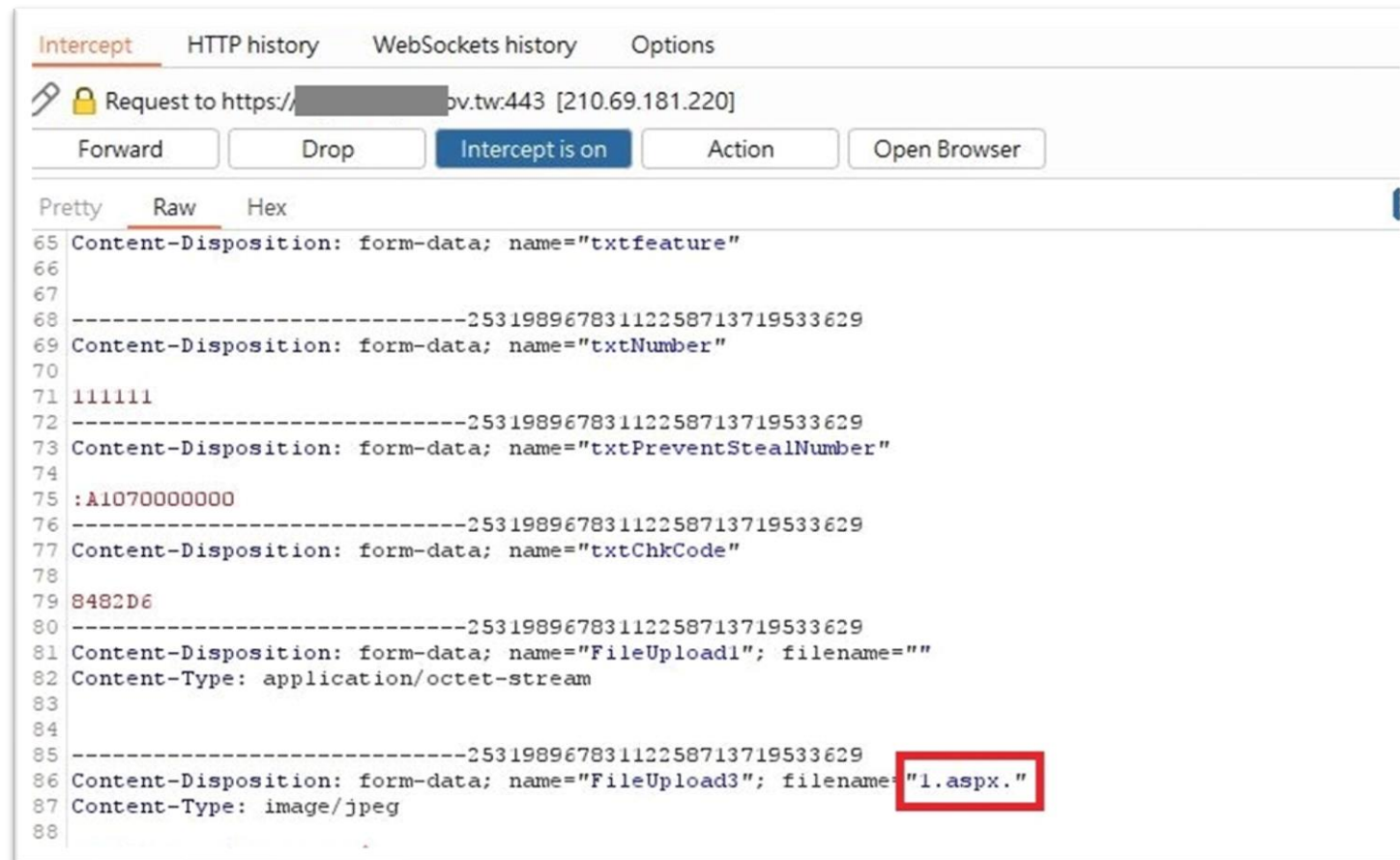
照片參考範例Photo (See Example)

* 照片上傳1Photo Upload 1
瀏覽... 未選擇檔案。
11111_20230822-11.xml

* 照片上傳2 Photo Upload 2

案例4 未確實限制檔案上傳類型(2/3)

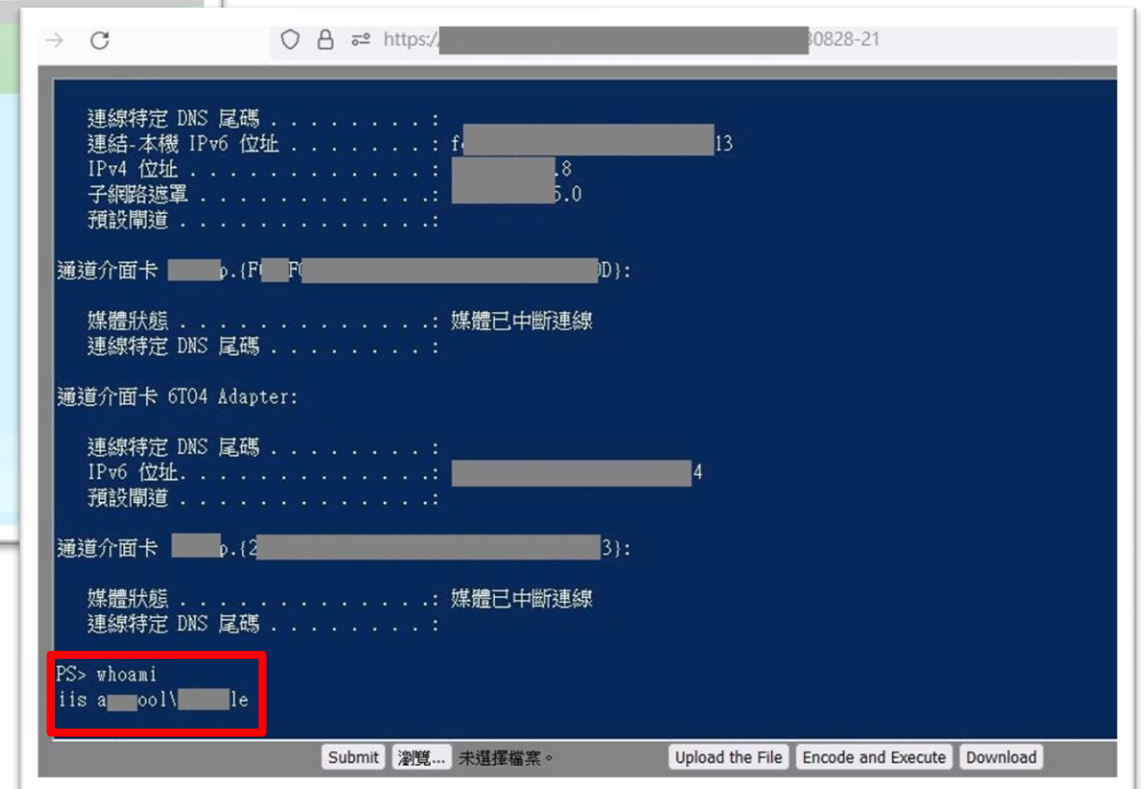
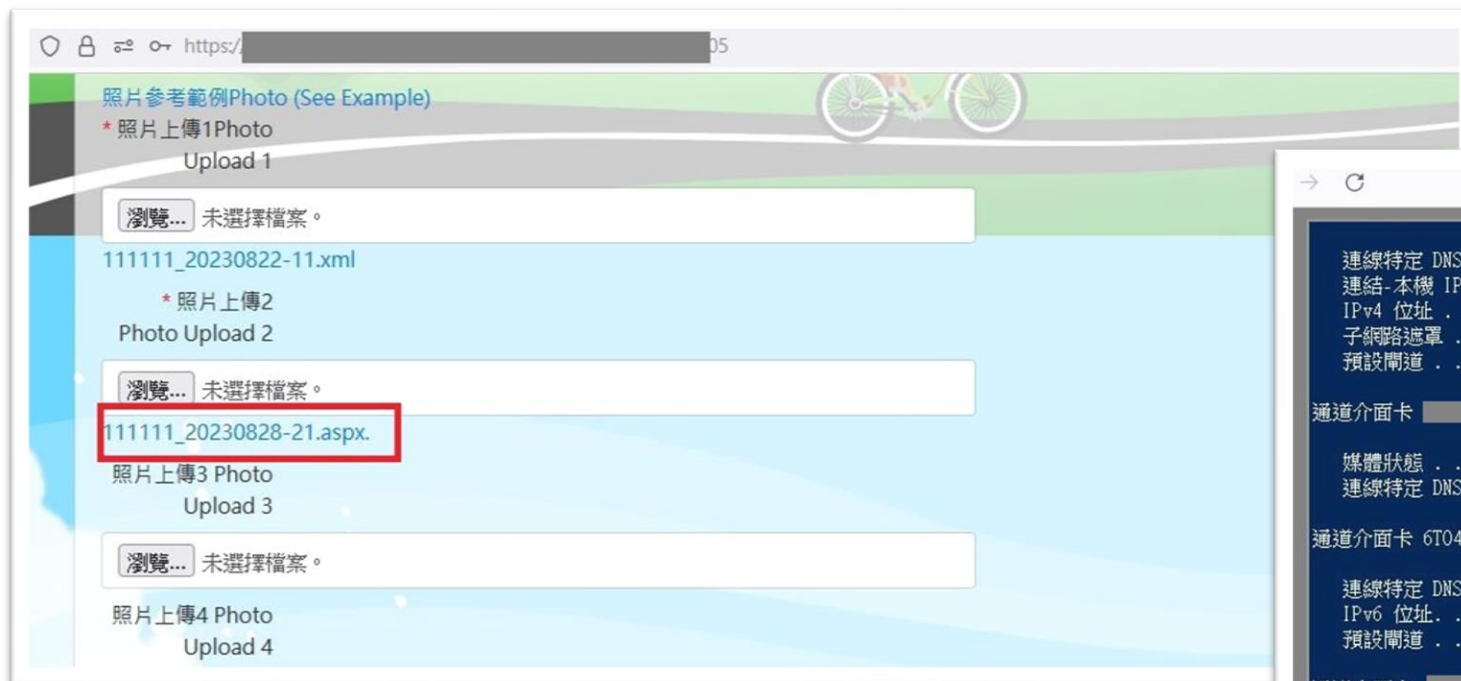
- 利用Burp Suite攔截封包，嘗試修改參數「filename」，將「.jpg」修改成「1.aspx」



```
Intercept HTTP history WebSockets history Options
Request to https://[redacted].tw:443 [210.69.181.220]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
65 Content-Disposition: form-data; name="txtfeature"
66
67
68 -----25319896783112258713719533629
69 Content-Disposition: form-data; name="txtNumber"
70
71 111111
72 -----25319896783112258713719533629
73 Content-Disposition: form-data; name="txtPreventStealNumber"
74
75 :A1070000000
76 -----25319896783112258713719533629
77 Content-Disposition: form-data; name="txtChkCode"
78
79 8482D6
80 -----25319896783112258713719533629
81 Content-Disposition: form-data; name="FileUpload1"; filename=""
82 Content-Type: application/octet-stream
83
84
85 -----25319896783112258713719533629
86 Content-Disposition: form-data; name="FileUpload3"; filename="1.aspx."
87 Content-Type: image/jpeg
88
```

案例4 未確實限制檔案上傳類型(3/3)

- 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



- 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

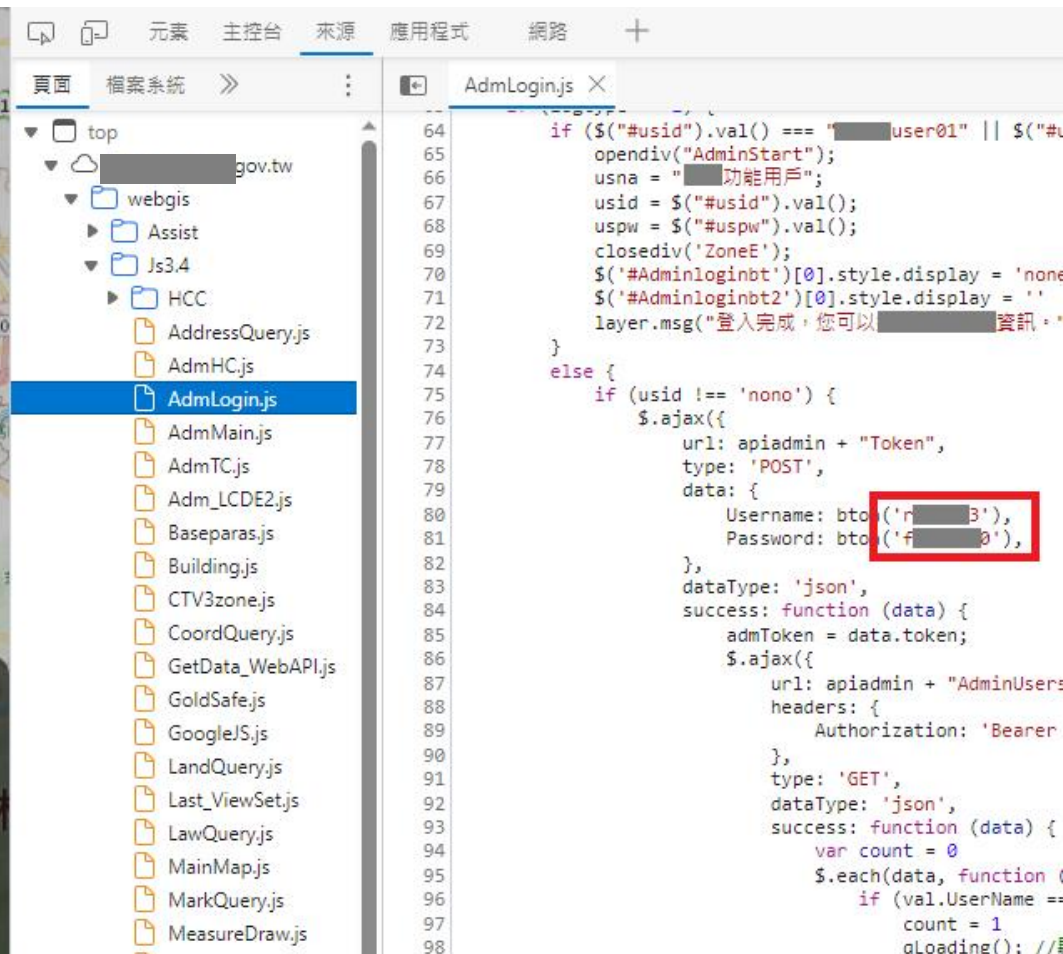
5. 帳號密碼外洩 (加密機制失效)

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)

- 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)

- 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



憑證ID	用戶名	類別狀	機關單	所屬科	職稱	連絡
ro...3	林	A	處	室	工程師	(0)
la...r...	測	A	處	測	系統管	(0)
o...5	鄭	A	處		測量助理	(0)
la...8...	黃	B	地...	科	課長	(0)
la...8...	李	B	事...	科	課員	(0)
la...8...	林	B	事...	科	課員	(0)
la...8...	童	B	事...	科	課員	(0)
la...0...	曾	A	處	科	科員	(0)
la...0...	謝	B	處	科	科員	(0)
la...8...	葉	B	地...		檢查員	0325... 8... z...1 編輯 刪除
la...8...	陳	B	事...	測	檢查員	0325... 8... 8...pa 編輯 刪除

案例5-2 帳號密碼外洩(1/2)

- 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

The screenshot displays the Burp Suite interface with a network request and response. The request is a multipart form-data containing the following fields:

- php HTTP/1.1
- gov.tw
- gth: 1492
- ol: max-age=0
- "Not:A-Brand";v="99", "Chromium";v="112"
- obile: ?0
- 'atform: "Windows"
- ecure-Requests: 1
- ps://.gov.tw
- e: multipart/form-data;
- WebKitFormBoundaryb9paAlpYlqw30z9A
- Mozilla/5.0 (Windows NT 10.0; Win64; x64)
- /537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
- 36
- pplication/xhtml+xml,application/xml;q=0.9,image/avif,
- image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
- ite: same-origin
- ode: navigate
- est: frame
- tps://.gov.tw/ap/login.php?lang=tw
- ding: gzip, deflate
- uage: zh-TW, zh;q=0.9, en-US;q=0.8, en;q=0.7
- close

The response is an HTML page with the following content:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 23 May 2023 07:28:01 GMT
3 X-Frame-Options: SAMEORIGIN
4 Frame-Options: SAMEORIGIN
5 Content-Length: 362
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <html>
10 <head>
11 <meta http-equiv="Content-Type" content="text/html;
12 charset=UTF-8">
13 </head>
14 <body>
15 </body>
16 </html>
17 <script language="javascript">
18 var data=[
19 [-1, "password error!"]
20 ,["3675","765","","",".gov.tw"]
21 ,["1600","","1599","","bm hH" "NewSoft OA","admin"]
22 ,["",""]
23 ,["64"]
24 ];
25 parent.DataReady(window.name, data, "gin");
26 </script>
```

The Inspector panel shows the selected text "bm hH" and the decoded text "ne HG".

案例5-2 帳號密碼外洩(2/2)

- 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

The screenshot displays a web application interface with several key elements highlighted by red boxes:

- 系統設定** (System Settings) menu in the top left.
- 新增成員** (Add Member) button in the top navigation bar.
- 新增員工資料** (Add Employee Information) form with the following details:
 - 成員帳號 (Member ID): **nics112pt70101**
 - 密碼 (Password): **Nics112pt70101@**
 - 密碼確認 (Confirm Password): [Redacted]
 - 姓名(中文) (Name): **王曉明**
- 我的首頁** (My Home) page showing a user profile for **王曉明** (Wang Xiaoming) in the top right corner.
- A notification for **112年 網路攻防演練** (112th Network Defense Drill) in the bottom right area.

- 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

- 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**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

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



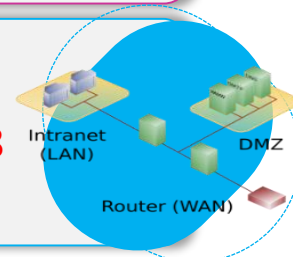
物聯網設備檢測



- 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



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

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



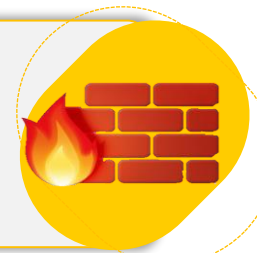
資料庫安全檢測



- 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」

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)

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



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

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)

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

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

發現事項同111年

1 未安裝所有安全性更新項目

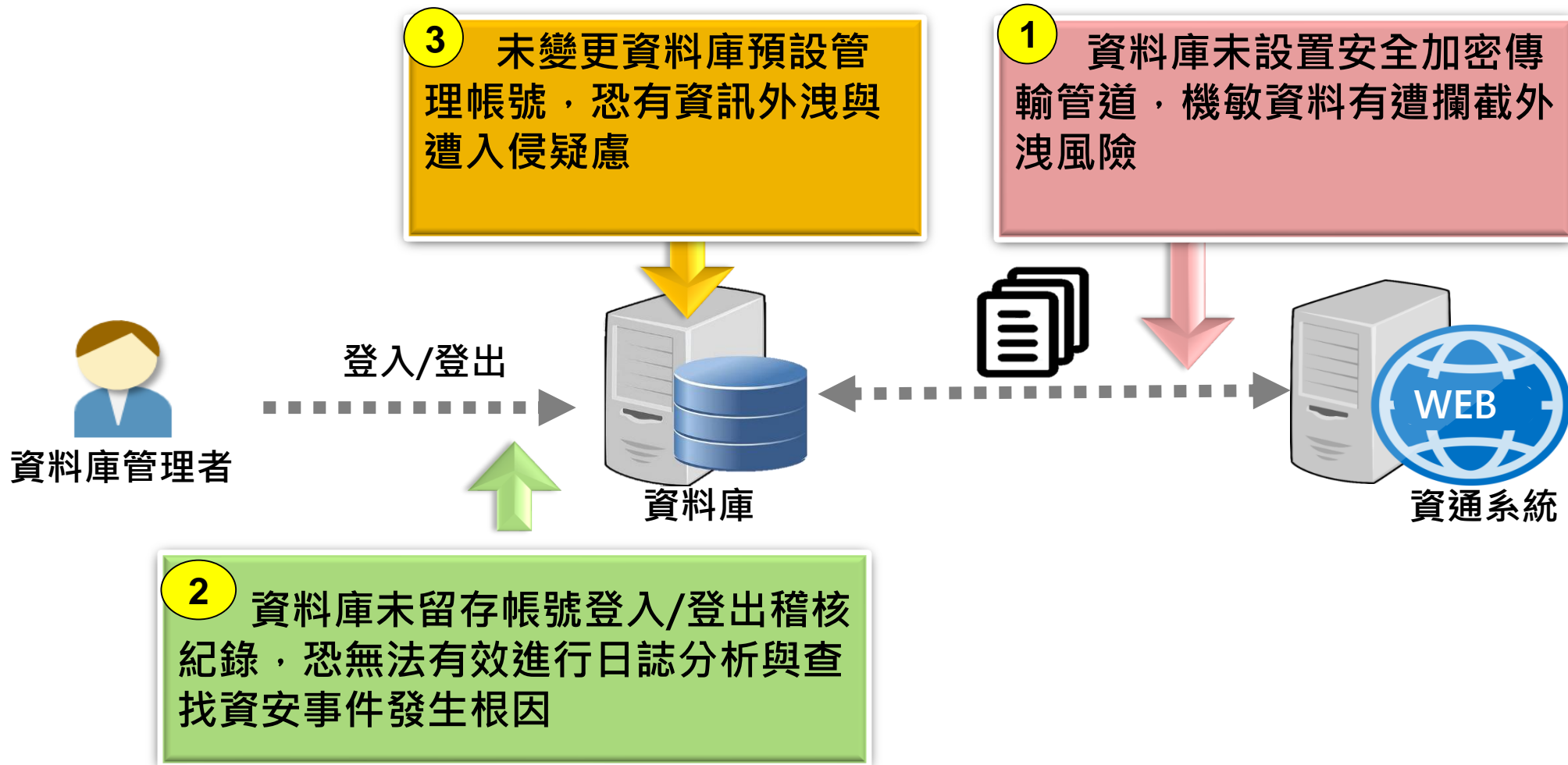


改善建議

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)

發現事項1同111年



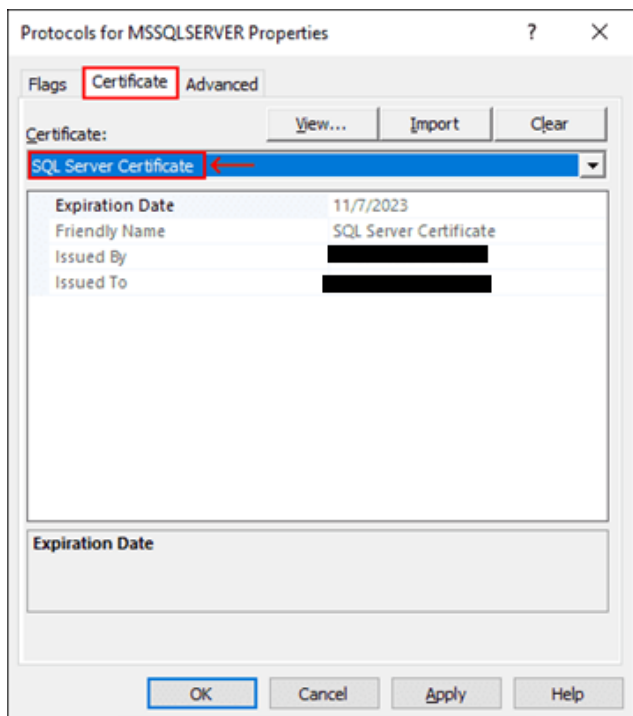
改善建議

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」

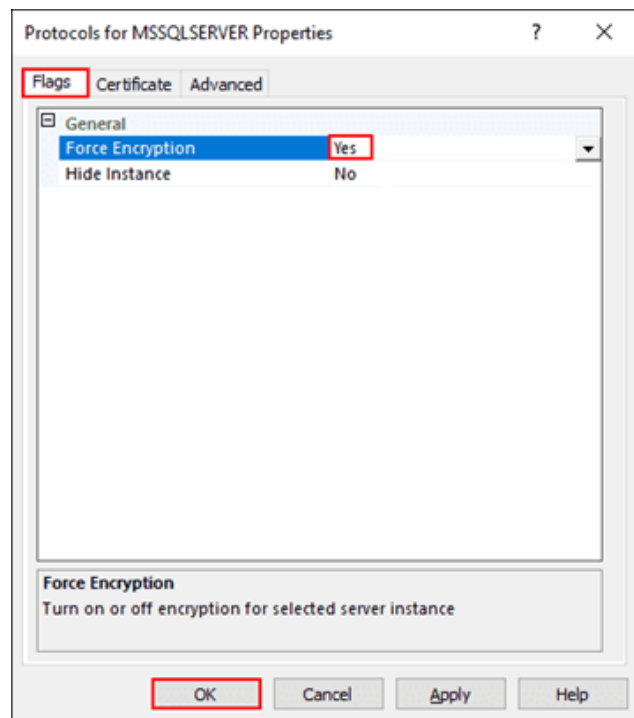
資料庫安全檢測共同發現事項(3/3)

實作範例

- SQL Server 啟用TLS加密傳輸

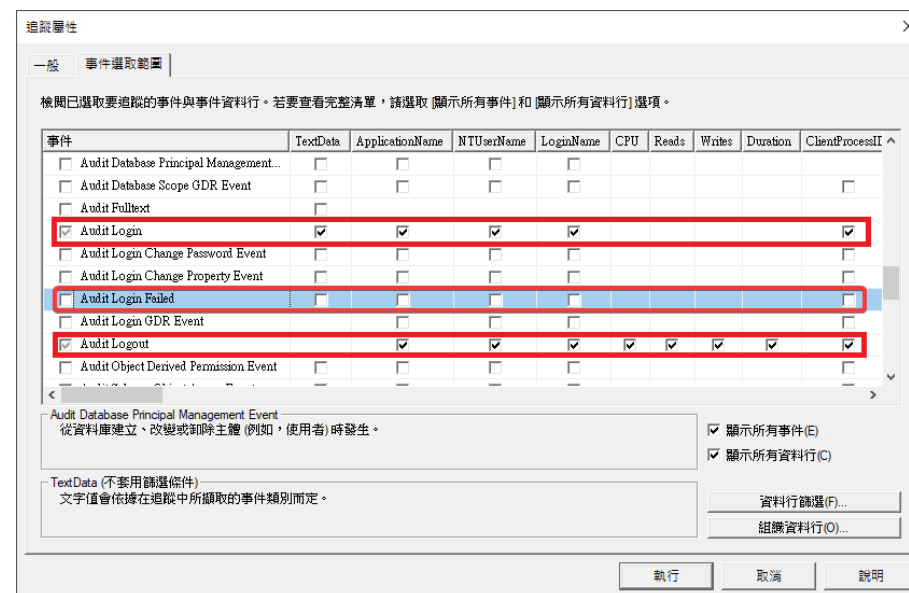


綁定站台加密憑證



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>

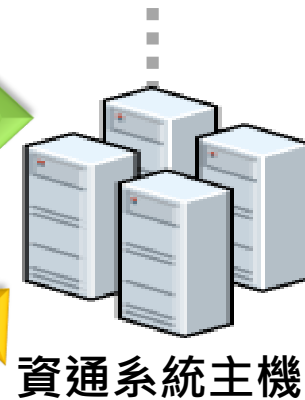
核心資通系統內網滲透測試共同發現事項(1/2)

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

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



資通系統主機

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



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

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

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



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

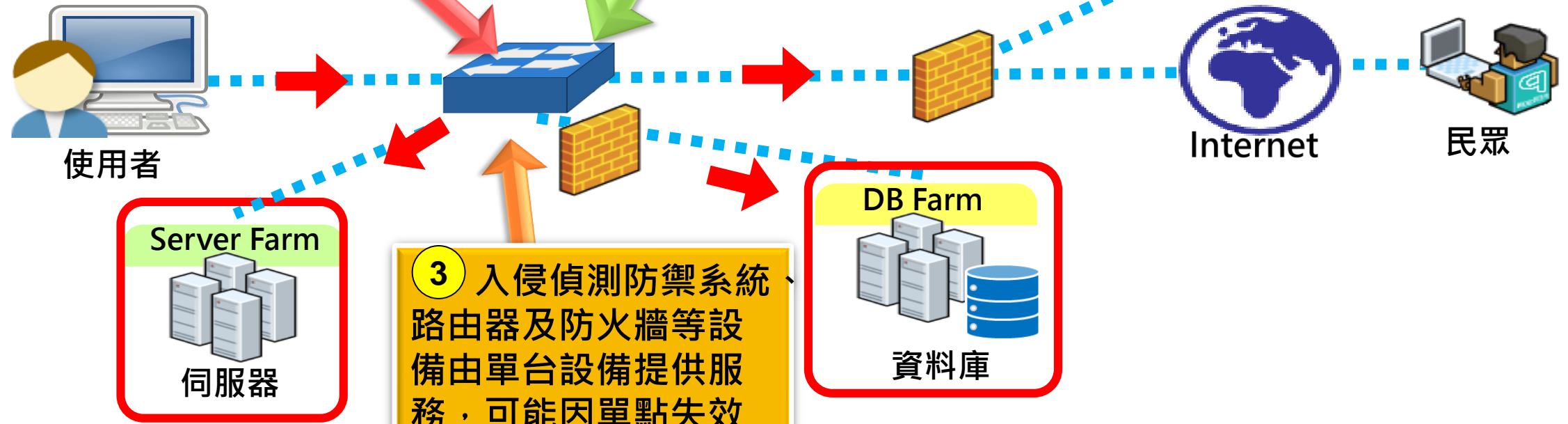
網路架構檢測共同發現事項(1/2)

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

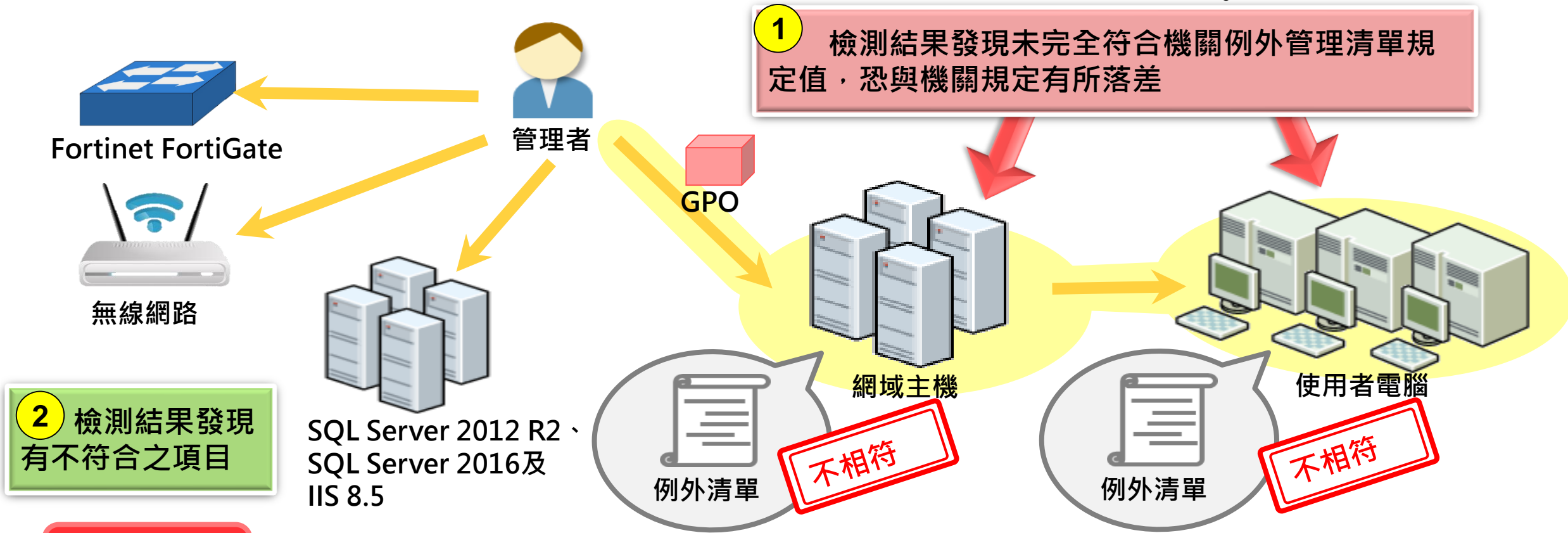


改善建議

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

發現事項同111年



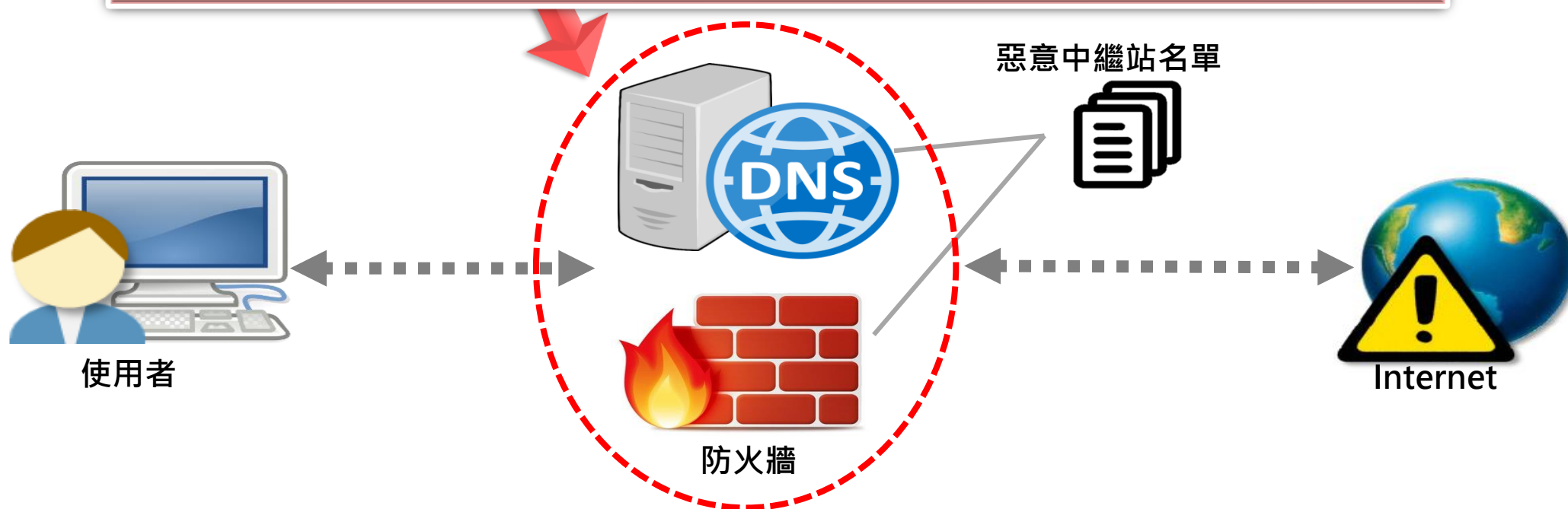
改善建議

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

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

- 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

- 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

