

# 109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

109年12月

# 大綱

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

NCCST

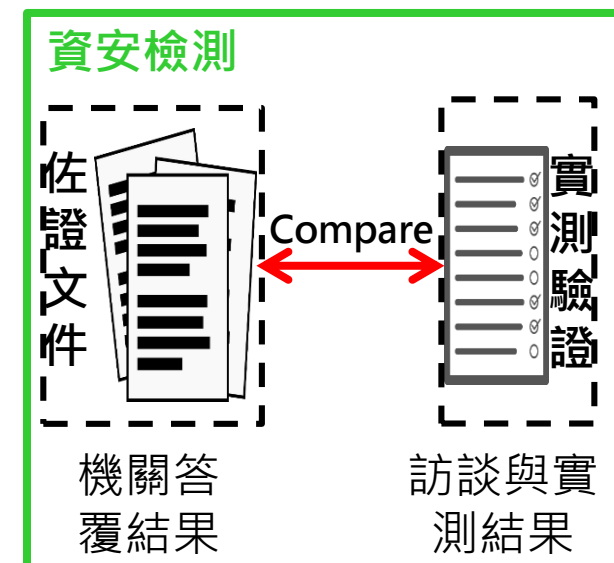
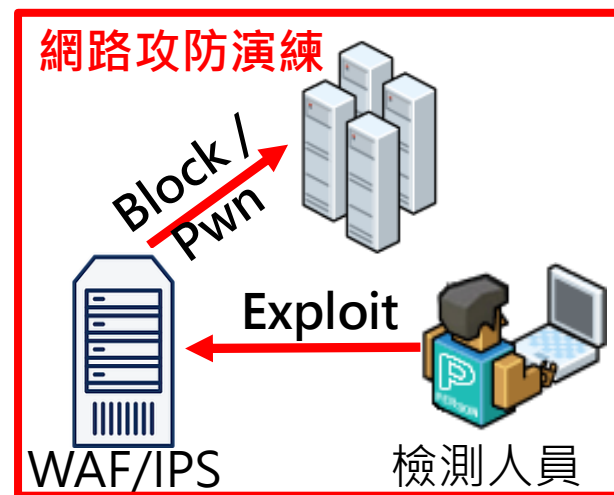
- 前言
- 網路攻防演練發現與建議
- 資安檢測發現與建議
- 結論與建議

NCCST

# 前言



- 技服中心持續透過網路攻防演練與資安檢測，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，109年以核心資料庫技術檢測為重點，檢測項目包含資料庫安全、網路安全、系統安全及主機安全等防護作為

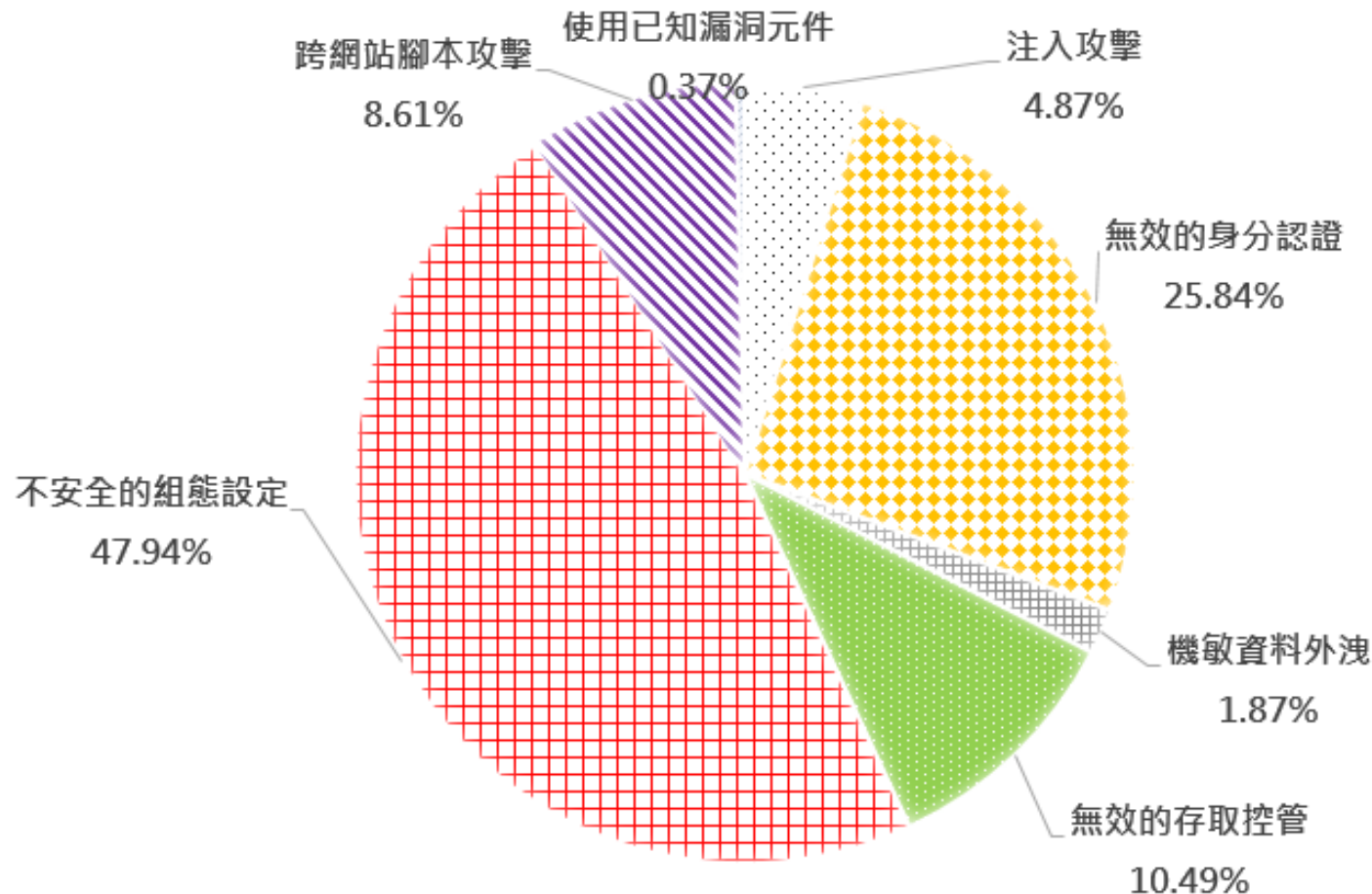


- 前言
- 網路攻防演練發現與建議
- 資安檢測發現與建議
- 結論與建議

NCCST

# 網路攻防演練弱點類型分布

- 綜整109年網路攻防演練攻擊紀錄，其中**不安全**的**組態設定**與**無效的身分認證**筆數比例最高



# 網路攻防演練綜合發現

- 歸納上述弱點類型，其根因可彙整為下列**4項**，建議參考以下**7**個案例介紹，清查機關潛在弱點

項次	發現事項	案例
1	資料庫無限縮存取來源	案例1
2	上線前未落實安全設定檢查	案例2-1至2-3
3	公開預設帳號與通行碼原則	案例3
4	未落實權限檢查	案例4-1至4-2

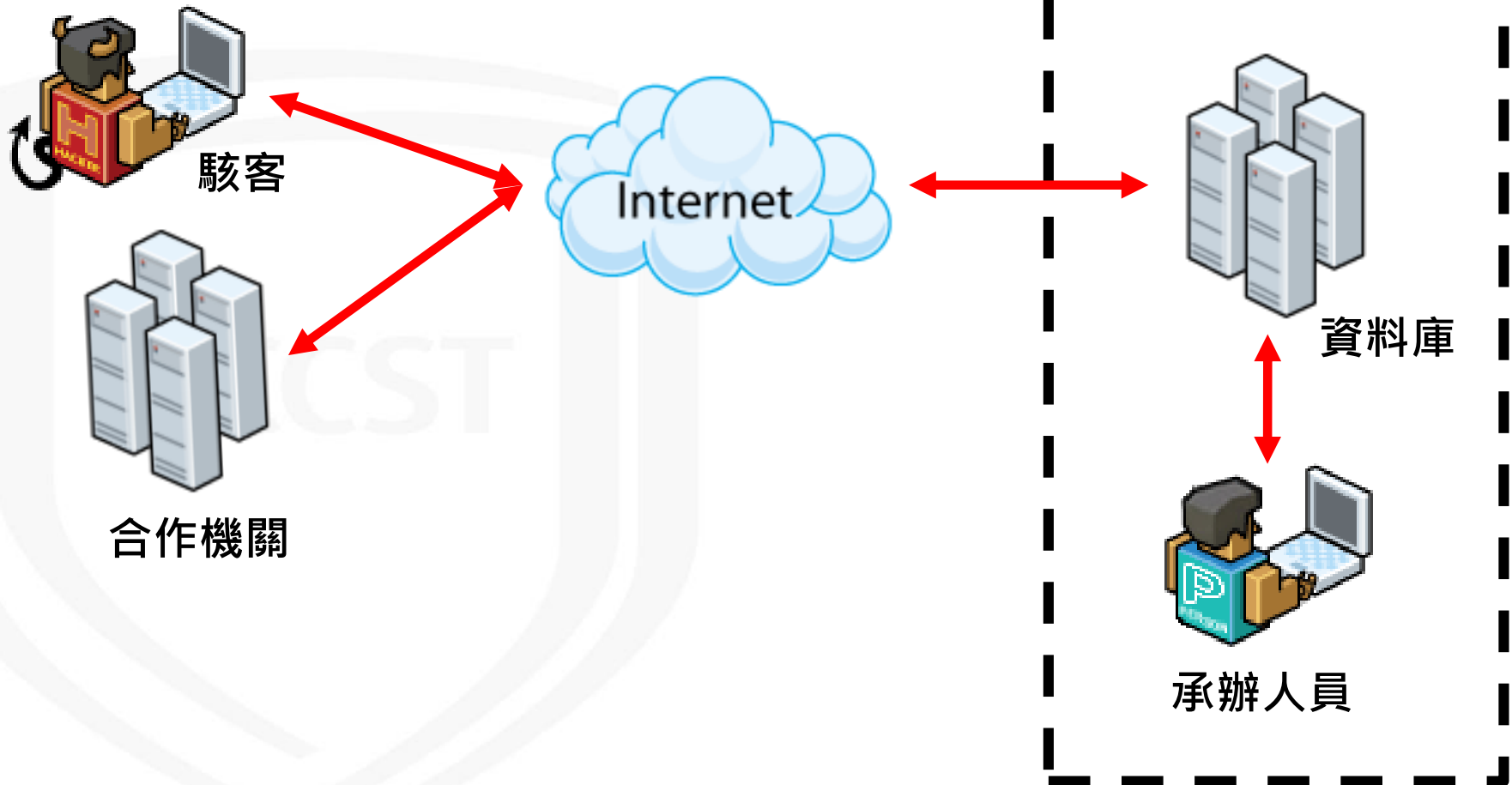
# 1.資料庫未限縮存取來源

NCCST



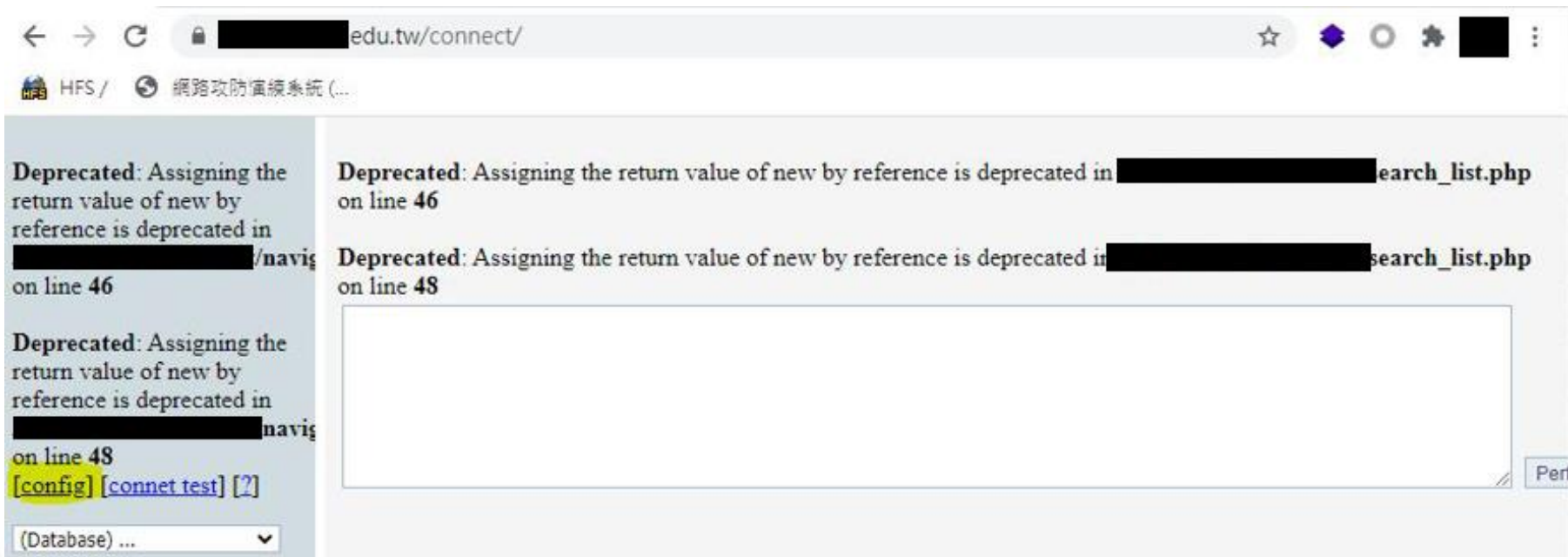
# 資料庫無限縮存取來源樣態

- 取得明文資料庫連線設定，且允許外網來源直接存取資料庫



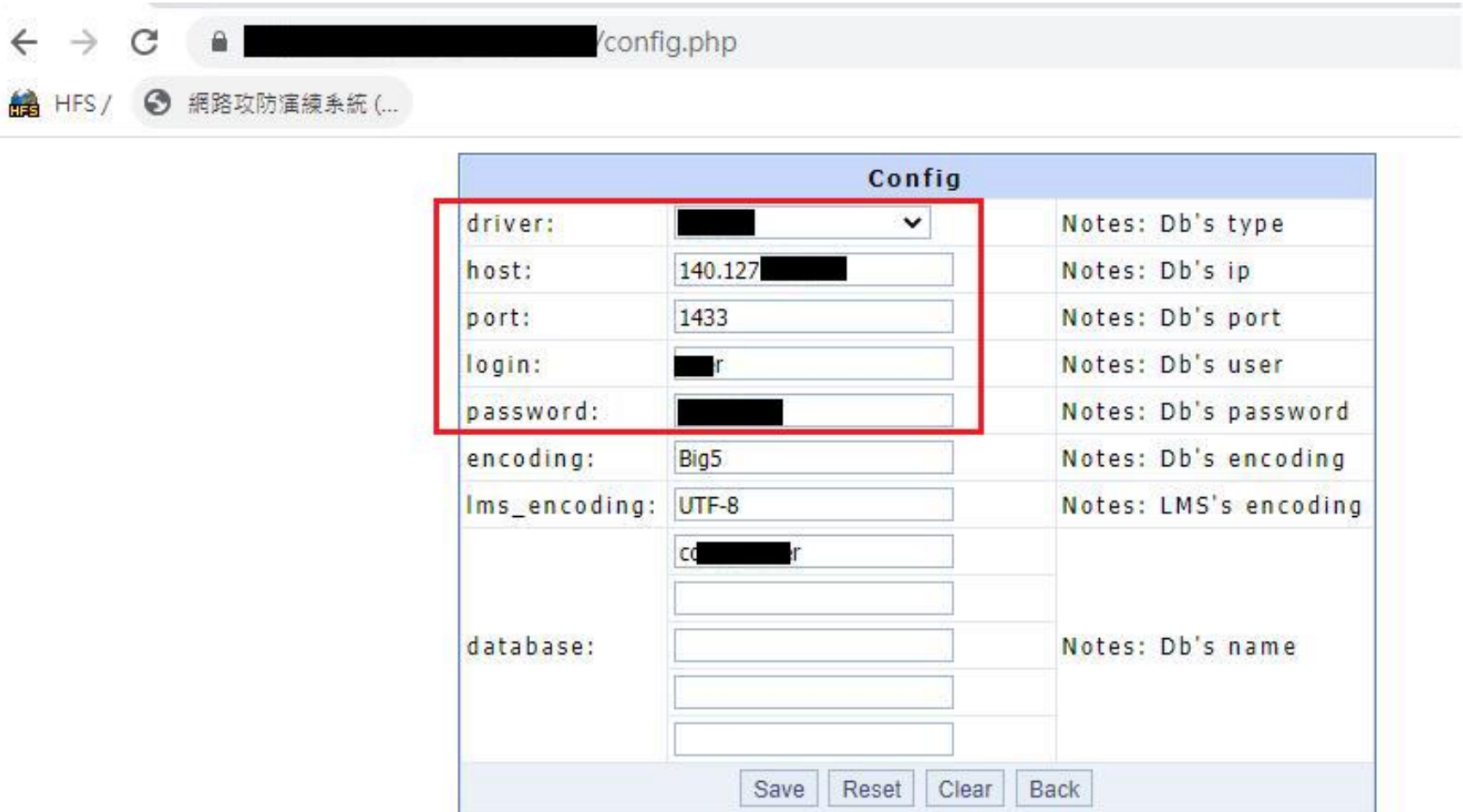
# 案例1 暴露連線設定(1/3)

- 攻擊手嘗試對路徑進行列舉，發現除顯示錯誤外，左下角另有config連結



# 案例1 暴露連線設定(2/3)

- 發現該連結存有資料庫連線設定與明文密碼



← → ↻ 🔒 [REDACTED] /config.php

HFS / 網路攻防演練系統 (...)

Config		
driver:	[REDACTED] ▼	Notes: Db's type
host:	140.127 [REDACTED]	Notes: Db's ip
port:	1433	Notes: Db's port
login:	[REDACTED]r	Notes: Db's user
password:	[REDACTED]	Notes: Db's password
encoding:	Big5	Notes: Db's encoding
lms_encoding:	UTF-8	Notes: LMS's encoding
database:	co [REDACTED] r	Notes: Db's name
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
Save Reset Clear Back		

# 案例1 暴露連線設定(3/3)

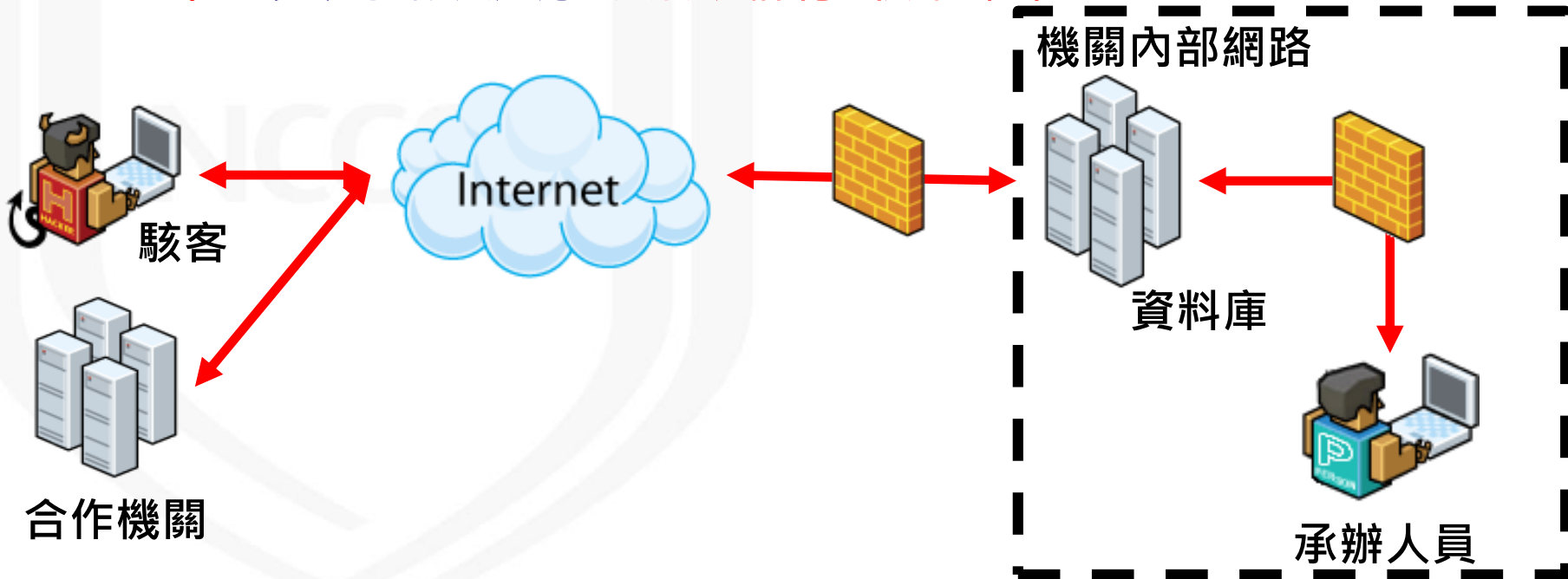
- 成功遠端連線至該資料庫

```
[14:09:26] [INFO] connection to Sybase server '140.127 ..... ' established
[14:09:26] [INFO] testing
[14:09:26] [INFO] confirming
[14:09:26] [INFO] resumed: [['1']]...
[14:09:26] [INFO] the back-end DBMS is
back-end DBMS: Sybase
[14:09:26] [INFO] fetching database names
[14:09:26] [INFO] fetching number of distinct values for column 'name'
[14:09:27] [INFO] using column 'name' as a pivot for retrieving row data
available databases [38]:
[*]      ll
[*]      hrd
[*]      ca
[*]      y
[*]      yc
[*]      lgp
[*]      je
[*]      akka
[*]      ic
[*]      lc
[*]      sngccu
[*]      lc
[*]      nservice
[*]      h
[*]      l
[*]      m
```

# 資料庫未限縮存取來源改善建議



- 資料庫應控管於內部網段，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SA等高權限帳號進行登入及執行AP程式，其餘帳號亦須限縮存取範圍



## 2. 上線前未落實安全設定檢查

NCCST

# 上線前未落實安全設定檢查樣態



- 正式系統保有Git版控資訊，卻未有存取控制，因而可下載網站原始碼，取得資料庫設定或API金鑰
- 未清查設備既有預設帳號與通行碼，導致仍可成功登入低權限帳號，進而暴露防火牆規則
- 使用第三方套件卻未控管後台權限，駭客無需帳密即可上傳檔案至網站公開頁面

# 案例2-1 未限縮Git目錄存取(1/3)



- 攻擊手進行路徑猜測與列舉，確認.git相關路徑存在且可存取

```
← → ↻ 🔒 [REDACTED].gov.tw/.git/config  
[core]  
  repositoryformatversion = 0  
  filemode = true  
  bare = false  
  logallrefupdates = true  
  ignorecase = true  
  precomposeunicode = true  
[remote "origin"]  
  url = [REDACTED]/etutor.git  
  fetch = +refs/heads/*:refs/remotes/origin/*  
[branch "master"]  
  remote = origin  
  merge = refs/heads/master
```



# 案例2-1 未限縮Git目錄存取(2/3)



- 接著透過GitHack或gitdumper等工具，進行網站原始碼打包下載與還原

```
[+] Downloaded: objects/392a587bb52
[+] Downloaded: objects/cde02198c68
[+] Downloaded: objects/bbfa092dc2f
[+] Downloaded: objects/b415e21203f
[+] Downloaded: objects/e03c500cfac
[+] Downloaded: objects/6e02b5cdd91
[+] Downloaded: objects/caf88ddf577
[+] Downloaded: objects/16616b4df65
[+] Downloaded: objects error: unable to read sha1 file of
[+] Downloaded: objects Updated 2640 paths from the index
[+] Downloaded: objects edul2@kali06:~/gitclone/GitTools/git_dump1$ ls -al
[+] Downloaded: objects total 436
[+] Downloaded: objects drwxr-xr-x 59 edul2 domain users 4096 Aug 5 10:09
[+] Downloaded: objects drwxr-xr-x 8 edul2 domain users 4096 Aug 5 10:00
[+] Downloaded: objects drwxr-xr-x 6 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects -rw-r--r-- 1 edul2 domain users 1295 Aug 5 10:08 load.php
[+] Downloaded: objects drwxr-xr-x 7 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects drwxr-xr-x 8 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects -rw-r--r-- 1 edul2 domain users 308 Aug 5 10:08 secrets.json
[+] Downloaded: objects drwxr-xr-x 3 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects -rw-r--r-- 1 edul2 domain users 89 Aug 5 10:08 .json
[+] Downloaded: objects -rw-r--r-- 1 edul2 domain users 27767 Aug 5 10:08 .lock
[+] Downloaded: objects drwxr-xr-x 2 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects drwxr-xr-x 5 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects drwxr-xr-x 3 edul2 domain users 4096 Aug 5 10:08
[+] Downloaded: objects drwxr-xr-x 4 edul2 domain users 4096 Aug 5 10:09
[+] Downloaded: objects drwxr-xr-x 2 edul2 domain users 4096 Aug 5 10:09
[+] Downloaded: objects drwxr-xr-x 8 edul2 domain users 4096 Aug 5 10:09 y_review
[+] Downloaded: objects drwxr-xr-x 4 edul2 domain users 4096 Aug 5 10:09 t
[+] Downloaded: objects drwxr-xr-x 6 edul2 domain users 4096 Aug 5 10:09 c
[+] Downloaded: objects drwxr-xr-x 6 edul2 domain users 4096 Aug 5 10:09 se
[+] Downloaded: objects drwxr-xr-x 7 edul2 domain users 4096 Aug 5 10:09 se
[+] Downloaded: objects -rw-r--r-- 1 edul2 domain users 17846 Aug 5 10:09 se_list.php
[+] Downloaded: objects drwxr-xr-x 5 edul2 domain users 4096 Aug 5 10:09 ce_manage
[+] Downloaded: objects drwxr-xr-x 7 edul2 domain users 4096 Aug 5 10:09 y
[+] Downloaded: objects drwxr-xr-x 4 edul2 domain users 4096 Aug 5 10:09
[+] Downloaded: objects drwxr-xr-x 5 edul2 domain users 4096 Aug 5 10:09 ze
[+] Downloaded: objects drwxr-xr-x 6 edul2 domain users 4096 Aug 5 10:09 x
[+] Downloaded: objects drwxr-xr-x 5 edul2 domain users 4096 Aug 5 10:09 x_manage
[+] Downloaded: objects drwxr-xr-x 4 edul2 domain users 4096 Aug 5 10:09 xact
[+] Downloaded: objects drwxr-xr-x 10 edul2 domain users 4096 Aug 5 10:09 a
```



# 案例2-2 未修改預設通行碼(1/2)



- 攻擊手發現某防火牆可被連線，透過Google搜尋預設密碼，得知Administrator/1234與Monitor/5678兩組預設密碼

fortiwan default password



全部 圖片 影片 新聞 購物 更多

設定 工具

約有 6,160 項結果 (搜尋時間：0.42 秒)

The **default** Username/Password, Administrator/1234 and Monitor/5678, used for V4.

2017年3月5日

www.fortinetguru.com > 2017/03 > fortiwan-web-ui-an...

FortiWAN Web UI and CLI Overview – Fortinet GURU

關於精選摘要 意見回饋

# 案例2-2 未修改預設通行碼(2/2)



- 嘗試使用預設帳號密碼(Monitor/5678)進行登入，發現可成功登入設備並取得防火牆規則設定

The screenshot displays the FortiWAN Web-Based Admin interface. The browser address bar shows the URL `https://210.69.██████████.login.php#`. The page title is "FortiWAN 200B" and the user is logged in as "Monitor@210.69.██████████" on "2020/06/15 14:19:52".

The left sidebar contains a navigation menu with the following items: System, Service, Firewall, NAT, Persistent Routing, Auto Routing, Virtual Server, Bandwidth Management, Connection Limit, Cache Redirect, Multihoming, Internal DNS, DNS Proxy, SNMP, and IP-MAC Mapping. The "Service" menu item is currently selected.

The main content area displays a table of IPv4 Rules. The table has columns for "E", "When", "Source", "Destination", and "Service".

	E	When	Source	Destination	Service
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	Any Address	Any Address	Any
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	210.69.██████████	210.69.██████████	ICMP
<input type="checkbox"/>	<input type="checkbox"/>	All-Time	██████████.ain	Any Address	HTTPS (443)
<input type="checkbox"/>	<input type="checkbox"/>	All-Time	██████████.ain	██████████	Any
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN	Localhost	HTTP (80)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		HTTPS (443)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		SSH (22)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		SNMP (161)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		RIP (520)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		TCP@139
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	WAN		TCP@445
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	Any Address		Any

A login dialog box is overlaid on the table, containing the following fields and buttons:

- Language dropdown: English
- Username input field: Monitor
- Password input field: masked with four dots
- Login button

# 案例2-3 未限縮後台存取權限(1/3)

- 攻擊手利用掃描目錄發現存在ckfinder.html檔案

```
nccst14@kali19:~$ dirb https://          .gov.tw/
1
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Wed Jun 10 12:50:01 2020
URL_BASE: https://          .gov.tw/
WORDLIST_FILES: /usr/share/dirb/wordlists/c

-----
GENERATED WORDS: 4612

---- Scanning URL: https://          .gov.t
==> DIRECTORY: https://          .gov.t
==> DIRECTORY: https://          .gov.t
==> DIRECTORY: https://          .gov.t
==> DIRECTORY: https://          .gov.t
==> DIRECTORY: https://          .gov.t
+ https://          .gov.tw/

-----
nccst14@kali19:~$ dirb https://          .gov.tw/ 'ckfinder/ -
2
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Wed Jun 10 15:28:54 2020
URL_BASE: https://          .gov.tw/          /ckfinder/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.html) | (.html) [NUM = 1]

-----
GENERATED WORDS: 4612

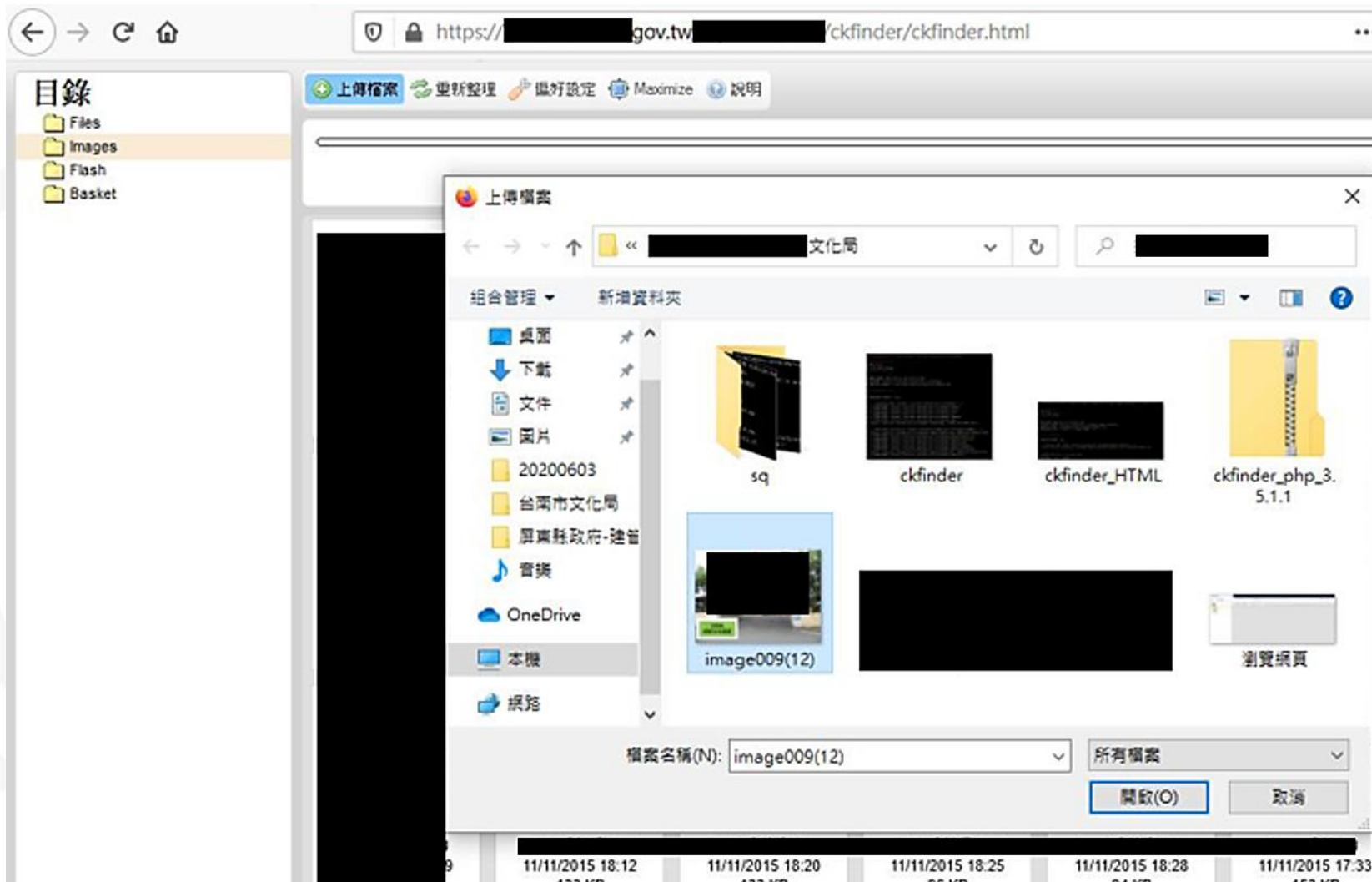
---- Scanning URL: https://          .gov.tw/          ckfinder/ ----
==> DIRECTORY: https://          .gov.tw/          /ckfinder/ckfinder.html (CODE:200
+ https://          .gov.tw/          /ckfinder/ckfinder.html

-----
nccst14@kali19:~$ dirb https://          .gov.tw/          /ckfinder/
-----
END_TIME: Wed Jun 10 15:29:56 2020
DOWNLOADED: 4612 - FOUND: 1
==> DIRECTORY: https://          .gov.tw/          /ckfinder/
==> DIRECTORY: https://          .gov.tw/          /css/
==> DIRECTORY: https://          .gov.tw/          /images/
==> DIRECTORY: https://          .gov.tw/          /includes/
```

# 案例2-3 未限縮後台存取權限(2/3)



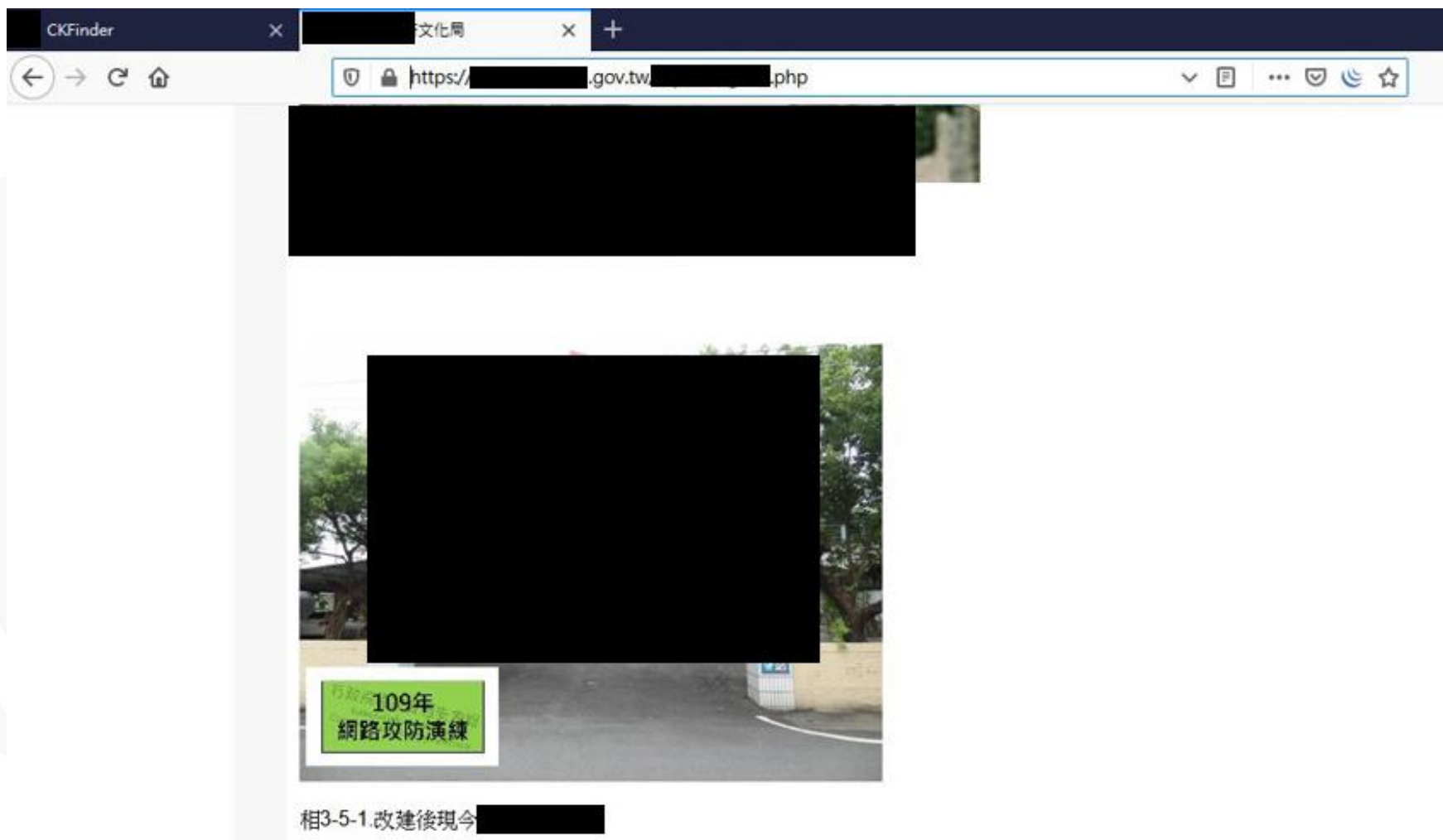
- 上傳經過修改的圖片



# 案例2-3 未限縮後台存取權限(3/3)



- 成功修改公開資料



# 上線前未落實安全設定檢查改善建議



- 建議訂定上線前檢查程序，將開發期間可能因測試而啟用之機制逐一確認關閉或修正
  - 變更預設帳號/測試帳號/管理者帳號等通行碼
  - 停用除錯模式與目錄瀏覽模式
  - 確認版控資訊與第三方套件完成安全設定
  - 系統操作手冊確實遮蔽帳號與網頁路徑等資訊
  - 弱點掃描/源碼檢測/滲透測試之弱點完成修補與複測



# 3. 公開預設帳號與通行碼原則

NCCST

# 公開預設帳號與通行碼原則樣態



- 公文記載帳號清單與共用預設密碼，且受文單位逕行公開於單位網站
- 「首次使用預設密碼登入須變更密碼」機制淪為系統公告性質，程式並未強制要求變更，導致使用者沿用預設密碼

你們的預設帳號密碼  
都在這裡喔!  
但要不要改隨便你



# 案例3 公文洩漏預設規則(1/4)

- 攻擊手透過Google得知，某系統曾有**教育訓練簡報**，並取得該份簡報檔及公文內容(含**預設密碼**)

Untitled - ██████████大學

函. 傳. 地址: ██████████1號. 真: ██████████ ... 附件: ██████████  
██████████系統教育訓練簡報」、學校帳.

██████████.edu.tw > app PDF

██████████大學

附件: 「██████████系統教育訓練簡報」、學校帳. 號(██████████)

file:///██████████弱勢學生獎助學金補助申請-3.pdf

— + 🔍 ↗ 符合一頁大小 頁面檢視

經費學生同意 ██████████ 查調其家庭年所得後，至上開系統填報學生申請經費相關資料。

(三)各技專校院請至上開系統依據**各校帳號(如附件)**、**密碼(各校皆為 ██████████)**登入後(若之前已註冊，請依原本貴校設定之密碼登入)，至「基本資料」項下

# 案例3 公文洩漏預設規則(2/4)

- 檔案附件亦有各校帳號清單

file:/// [redacted] 弱勢學生獎助學金補助申請-3.pdf

— + ↻ ↗ 符合一頁大小 頁面檢視 | A) 大聲朗讀 新增

線上數位公文列印 - 第 20 頁 / 共 29 頁 (正文 29 頁)

文稿頁面 文號： [redacted]

「 [redacted] 系統」帳號清單

序號	學校代號	帳號	承辦人姓名(預設)	備註(登入時·學校明細顯示)
1	[redacted] 3	[redacted] 1	[redacted] 大學	[redacted] 1
2	[redacted] 6	[redacted] 1	[redacted] 大學	[redacted] 1
3	[redacted] 1	[redacted] 1~3 [redacted] 5	[redacted] 大學	[redacted] 1
				[redacted] 2
				[redacted] 3
				[redacted] 4
				[redacted] 5
4	[redacted] 5	[redacted] 4 [redacted] 大學	[redacted] 1	
			[redacted] 2	
			[redacted] 3	
			[redacted] 4	

# 案例3 公文洩漏預設規則(3/4)



- 透過該資料，攻擊手成功登入某所大學(該帳號曾使用過，但系統並未強制要求修改預設密碼)

The screenshot shows a web browser window with the URL [https://\[redacted\].edu.tw/logon](https://[redacted].edu.tw/logon). The page header includes a navigation menu with items: 首頁, 助學金申請, 資料查詢, 資料維護, 統計印表, 基本資料, 其它事項, 登出. The user profile section displays a user icon, ID 108, and status 第1批次, 匯報狀態: (停用). Below this, it shows 目前彙報總筆數: 18筆, 目前線上人數: 1, and a red circle around the text [redacted] 大學您好, 歡迎進入通報系統. A yellow box highlights the 系統說明 section, which contains the following text:

**系統說明**

- 請登入後必須更換新密碼，切勿繼續使用預設密碼，以維資訊安全。
- 倘忘記密碼者，請使用登入頁面忘記密碼功能，倘有疑問煩請來電。
- 請優先使用[谷歌Chrome瀏覽器](#)進行操作。

# 案例3 公文洩漏預設規則(4/4)

- 因此攻擊手除可登入該大學帳號，亦取得承辦人登打之**學生個資**

https://[redacted]ApplyData

[redacted] 申請 [redacted]

學校名稱： [redacted] 大學  
承辦人： [redacted] 大學 聯絡電話： [redacted]

編號	學制	部別	年級	姓名	身分證字號
1	[redacted] 學士班	[redacted] 部	4	施 [redacted]	D22 [redacted]
2	[redacted] 學士班	[redacted] 部	4	蔡 [redacted]	D22 [redacted]
3	[redacted] 學士班	[redacted] 部	4	畢 [redacted]	D22 [redacted]
4	[redacted] 學士班	[redacted] 部	4	薛 [redacted]	D22 [redacted]
5	[redacted] 學士班	[redacted] 部	4	陳 [redacted]	N22 [redacted]
6	[redacted] 學士班	[redacted] 部	4	曾 [redacted]	P22 [redacted]
7	[redacted] 學士班	[redacted] 部	4	許 [redacted]	R22 [redacted]

# 公開預設帳號與通行碼原則改善建議



- 避免以**任何形式**公開帳號與通行碼原則
- 若應**教育訓練需求**，需**事先提供簡報**，則應**準備兩個版本簡報**，**登入資訊等細節**僅於現場講解，並提醒**保密義務**
- **變更預設通行碼**應從**系統面設計**為**強制性機制**，且不可設定為**預設通行碼**，以防遭他人**事先盜用**

## 4.未落實權限檢查

NCCST



# 未落實權限檢查樣態

- 網站透過前端JavaScript語法進行轉導，卻於回應封包夾帶過多資訊，攻擊者可修改JavaScript繞過身分驗證。管理介面亦暴露明文密碼，攻擊者可匿蹤控制系統，或嘗試登入其他系統
- 網站未正確檢查Cookie，攻擊者可透過偽造Cookie，直接取得網站管理者權限，無需取得帳號與通行碼

# 案例4-1 JavaScript轉導語法繞過(1/4)

- 攻擊手瀏覽網頁發現下一層目錄為SYS，並利用目錄列舉工具得知存在/AP/SYS/acct.aspx路徑

```
← → ↻ 🏠 view-source:https://[REDACTED].gov.tw/[REDACTED].aspx  
82     if ($("#Hid_Tag").val() != '') {  
83         ClickTag($("#Hid_Tag").val());  
84     }  
85     else  
86         $("#BtnTag1").addClass('act');  
87 });  
88  
89 function GoFirstLogin(oid) {  
90     if (CheckDevice())  
91         location.href = "SYS/[REDACTED].aspx?oid=" + oid;  
92     else  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000
```

# 案例4-1 JavaScript轉導語法繞過(2/4)

- 實際存取發現係透過JavaScript語法限制未登入使用者存取後臺，遂嘗試利用Burp Suite繞過限制



```
Response from https://[redacted].gov.tw:443/[redacted]acct.aspx [redacted]

Forward Drop Intercept is on Action

Raw Headers Hex HTML Render ViewState

href="javascript: __doPostBack(;&#39;ct100;ContentPlaceHolder1;ListView1;DataPager1;ct102;ct109;&#39;,&#39;&#39;)">10</a>&nbsp;&nbsp;&nbsp;<a
href="javascript: __doPostBack(;&#39;ct100;ContentPlaceHolder1;ListView1;DataPager1;ct102;ct110;&#39;,&#39;&#39;)">...</a>&nbsp;&nbsp;&nbsp;<a
href="javascript: __doPostBack(;&#39;ct100;ContentPlaceHolder1;ListView1;DataPager1;ct103;ct100;&#39;,&#39;&#39;)">000</a>&nbsp;&nbsp;&nbsp;<a
href="javascript: __doPostBack(;&#39;ct100;ContentPlaceHolder1;ListView1;DataPager1;ct104;ct100;&#39;,&#39;&#39;)">0000</a>&nbsp;&nbsp;&nbsp;</span>

[redacted]

</div>

</div>

</div>

<script type="text/javascript">
//
alert('000000000000000000000000'); top.location.href='[redacted]login.aspx';alert('000000000000000000000000'); top.location.href='[redacted]login.aspx';//]]&gt;
&lt;/script&gt;
&lt;/form&gt;
&lt;script&gt;
var js = [redacted]
js.setAtt[redacted]";
js.setAtt[redacted]";
js.setAtt[redacted]";
js.setAtt[redacted]";
document.[redacted]
&lt;/script&gt;
&lt;script src="[redacted]jquery.basictable.min.js" type="text/javascript"&gt;&lt;/script&gt;
&lt;script type="text/javascript"&gt;</pre></div><div data-bbox="968 952 990 975" data-label="Page-Footer">34</div>
```

# 案例4-1 JavaScript轉導語法繞過(3/4)

- 成功進入使用者管理介面，發現密碼欄位依靠 **password** 屬性保護，透過瀏覽器之「開發人員工具」即可得知明文密碼

密碼原則:(1)至少12個字元。

(2)包含大寫及小寫英文及數字及特殊字元(例: [REDACTED])。

(3)不可與使用者帳號相同。

\* 使用者密碼

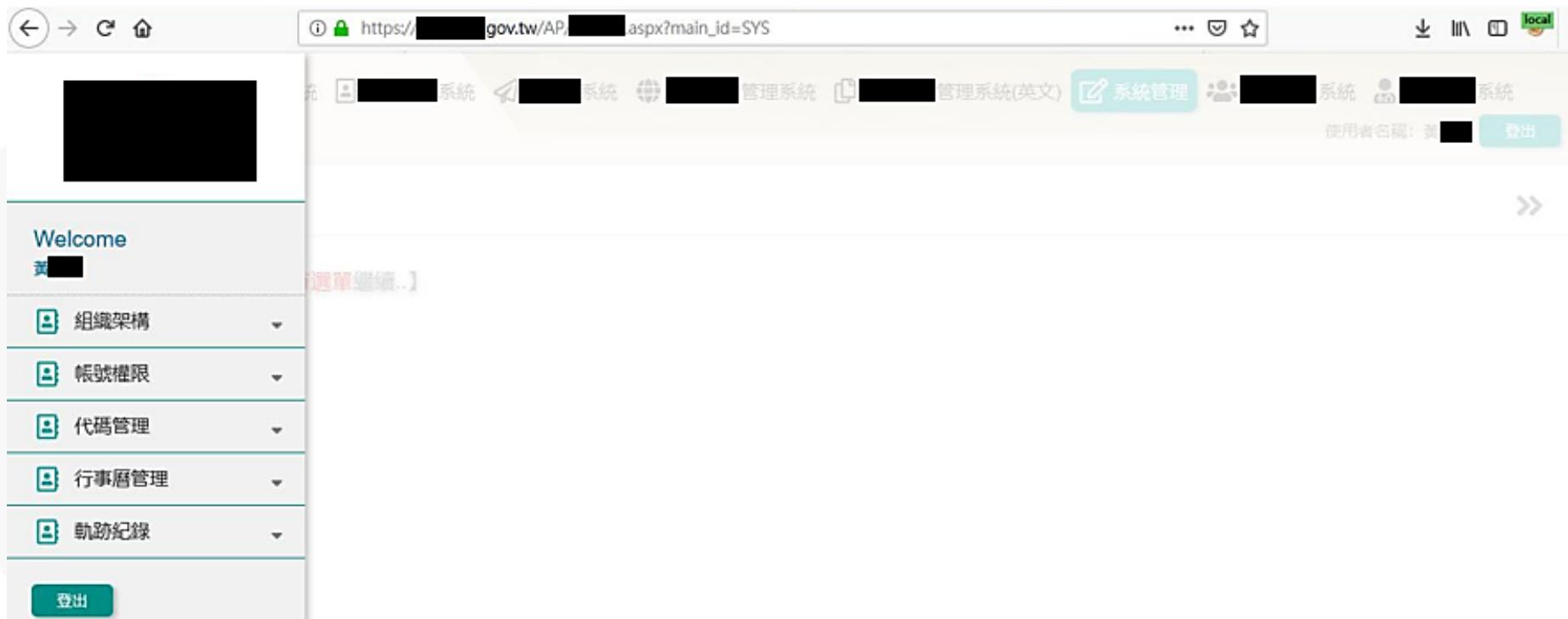
英文姓名

```
▶ <tr> ... </tr>
▼ <tr>
  ▶ <td class="td-pl" style="width: 15%;"> ... </td>
  ▶ <td style="width: 35%;"> ... </td>
  ▶ <td class="td-pl" style="width: 15%;"> ... </td>
  ▼ <td>
```

```
<input id="USER_PASSWORD" name="ctl00$ContentPlaceHolder1$USER_PASSWORD" type="password"
maxlength="50" value="[REDACTED]" style="width:45%;">
```

# 案例4-1 JavaScript轉導語法繞過(4/4)

- 利用取得之密碼資訊，成功登入系統，並取得系統管理者權限



# 案例4-2 Cookie資訊偽造(1/4)



- 攻擊手進行路徑猜測，得知登出頁面路徑，並從html原始碼發現路徑aiadmin

ⓘ 不安全 | ██████████.com.tw/██████████/Logout.php

您已登出 Server !! 謝謝使用  
現在時間 2020-07-14 16:37:30



```
按一下回上一頁，按住可查看記錄  
1 <html>  
2 <head>  
3 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">  
4 <META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">  
5 <META NAME="ROBOTS" CONTENT="NOARCHIVE">  
6 <title>謝謝使用 ██████████ 管理系統</title>  
7 <link href="aiadmin/css/style.css" rel="stylesheet" type="text/css">  
8 <link href="aiadmin/css/table.css" rel="stylesheet" type="text/css">  
9 </head>  
10 <body>  
11 <div id="Box">  
12 <div class="indexhead"></div>  
13 <div class="indexContent">  
14 <table width="60%" border="0" align="center" cellpadding="2" cellspacing="1" class="general">  
15 <tr class="SecondRow">  
16 <td height="22">  
17 <p>&nbsp;</p>  
18 <p><span class="LabelText">您已登出 Server !! 謝謝使用</span></p>  
19 <p><span class="LabelText">現在時間 2020-07-14 16:31:46</span></p>  
20  
21
```

# 案例4-2 Cookie資訊偽造(2/4)



- 存取aiadmin  
頁面會導回  
logout頁面，  
藉由觀察往來  
封包，發現該  
頁面**刪除特定  
cookie內容**

The screenshot shows a web browser at a URL ending in ".com.tw/Logout.php". The page content displays a message: "您已登出 Server !! 謝謝使用" and "現在時間 2020-07-14 16:31:46". Below the browser, the Network developer tool is open, showing the response headers for the "Logout.php" request. The headers include:

```
date: Tue, 14 Jul 2020 08:31:46 GMT
server: Apache
set-cookie: Username=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
set-cookie: ClientID=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
set-cookie: CusName=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
set-cookie: Mode=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
status: 200
```

# 案例4-2 Cookie資訊偽造(3/4)



- 將刪除的cookie新增至瀏覽器，並填入猜測之cookie值，重新檢視頁面後發現可成功登入

The screenshot shows a web browser displaying a management interface. The browser's address bar shows the URL `不安全 | [redacted].com.tw/[redacted]/main.php`. The page content includes a navigation menu with items like "1 系統管理", "2 網站管理", "3 會員管理", "6 點擊統計", and "8 [redacted]". A "系統公告" (System Notice) button is visible. The main content area displays "親愛的 Admin" (Dear Admin) and "歡迎光臨 [redacted] 數位平台管理介面" (Welcome to [redacted] Digital Platform Management Interface). The current time is shown as "現在時間 2020-07-14 16:46:08".

The developer tools 'Application' tab is open, showing a list of cookies. A red box highlights the 'cpsession' cookie, which has a value starting with 'e6a4ea33f...'. The table below shows the details of the cookies:

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Priority
Mode	[redacted]	[redacted]	/	Session	9				Medium
UserName	[redacted]	[redacted]	/	Session	13				Medium
cpsession	[redacted]e6a4ea33f...	[redacted]	/	Session	63	✓	✓		Medium
_ga	GA1.3.724008843.1594696902	[redacted]	/	2022-07-...	29				Medium
timezone	Asia/Shanghai	[redacted]	/	Session	21				Medium
ClientID	[redacted]Web	[redacted]	/	Session	13				Medium
PHPSESSID	[redacted]:b6f	[redacted]	/	Session	41				Medium
oid	GA1.3.1955948389.1594696902	[redacted]	/	2020-07-...	31				Medium



# 案例4-2 Cookie資訊偽造(4/4)



- 透過管理者上傳檔案功能，可成功執行Webshell

```
← → ↻ [redacted].com.tw [redacted]=0cph [cmd+echo+file_get_contents%2B"%2Fetc%2Fpasswd"%29%3B]
 
bi [redacted]n:/sbin/nologin
de [redacted]on:/sbin:/sbin/nologin
ad [redacted]r/adm:/sbin/nologin
lp [redacted]spool/lpd:/sbin/nologin
sy [redacted]sbin:/bin/sync
sh [redacted]utdown:/sbin:/sbin/shutdown
ha [redacted]sbin:/sbin/halt
uu [redacted]:/var/spool/uucp:/sbin/nologin
op [redacted]perator:/root:/sbin/nologin
ga [redacted]mes:/usr/games:/sbin/nologin
go [redacted]opher:/var/gopher:/sbin/nologin
ft [redacted]ser:/var/ftp:/sbin/nologin
db [redacted]en message bus:/sbin/nologin
vc [redacted]ual console memory owner:/dev:/sbin/nologin
ha [redacted]:HAL daemon:/sbin/nologin
ss [redacted]ilege-separated SSH:/var/empty/sshd:/sbin/nologin
na [redacted]ed:/var/named:/sbin/nologin
do [redacted]ovecot:/usr/libexec/dovecot:/sbin/nologin
rp [redacted]nd Daemon:/var/cache/rpcbind:/sbin/nologin
rp [redacted]PC Service User:/var/lib/nfs:/sbin/nologin
ns [redacted]Daemon:/sbin/nologin
my [redacted]ySQL server:/var/lib/mysql:/bin/bash
cp [redacted]k:32007:32009:/var/cpanel/userhomes/cpanel/lexifilter:/usr/local/cpanel/bin/noshell
ro [redacted]root:/bin/bash
no [redacted]body:/sbin/nologin
```

# 未落實權限檢查改善建議

- 建議逐一頁面落實權限檢查機制，且依系統角色差異，明確區分訪客(未登入)、一般使用者及管理者等權限差異
- 資料庫不應儲存使用者明文通行碼，以免系統遭入侵時連帶暴露使用者常用通行碼。若有變更通行碼需求，可透過亂數產生後直接通知使用者

# 大綱

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

NCCST

# 資料庫資安檢測目的

- 為強化政府機關重要資料保護，針對核心資料庫執行技術檢測，並設計以資料庫為核心，結合主機安全、資通系統安全及網路安全等面向之技術檢測框架



## 資料庫安全檢測

確認資料庫本身防護措施，與介接應用系統連線管理之安全性



## 主機安全檢測

確認資料庫主機之帳號管理、權限設定、存取管控及弱點防護情形



## 資通系統安全檢測

針對與資料庫介接之資通系統，確認滲透測試執行結果與弱點修補情形



## 網路安全檢測

確認資料庫之網路安全防護機制，與內外部應用系統介接情形及VPN管理方式

# 資料庫資安檢測項目

## 資料庫安全檢測

透過訪談及設定檢視，檢測資料庫之特權帳號管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全機制，以確認資料庫安全管理與防護狀況

## 主機安全檢測

透過訪談及實際檢視，檢測主機帳號管理、權限設定及存取管控情形，以及透過弱點掃描方式，確認主機相關弱點防護情形

## 資通系統安全檢測

透過檢視滲透測試報告及複測，檢測介接資通系統之權限存取、應用程式與系統弱點及系統通訊保護等項目之防護情形

## 網路安全檢測

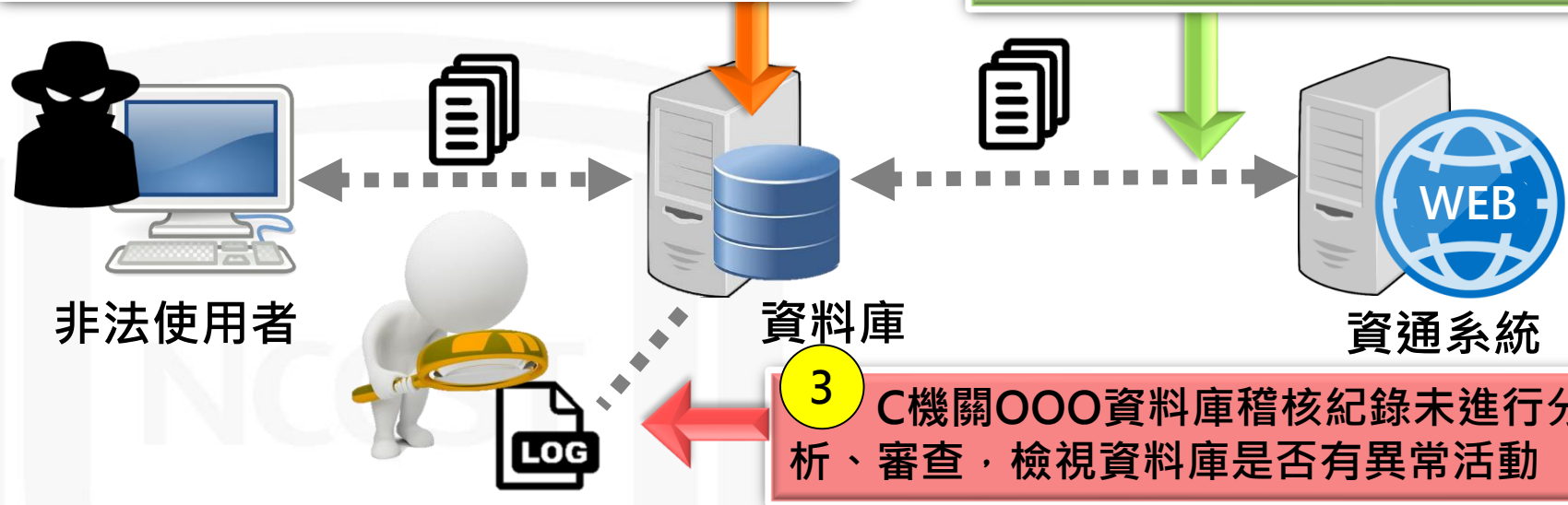
透過訪談及實際檢視，檢測應用系統與資料庫介接情形、VPN連線管理、防火牆規則、遠端連線管理及存取控制等項目之防護情形



# 共同發現事項(1/4)

**1** 經檢測發現A機關OOO資料庫資料為明文資料，未採取適當資料加密、遮罩或混淆機制，機敏資料恐有遭受侵害之風險

**2** B機關OOO分析與管理資料庫未設置安全的加密傳輸管道，機敏資料恐被攔截而曝光



**3** C機關OOO資料庫稽核紀錄未進行分析、審查，檢視資料庫是否有異常活動

## 資料庫安全檢測改善建議：



1. 建議針對資料庫中機敏資料採取加密或欄位內容遮罩、混淆等保護機制，強化資料安全性
2. 建議資料庫應設置安全的加密傳輸方式
3. 建議定期分析資料庫稽核紀錄，發現潛在異常行為，及早因應

# 共同發現事項(2/4)

1 C機關OOO網路網路資料庫主機經檢測發現，Oracle資料庫存在多個漏洞，恐有資安隱憂

2 D機關OOO核心資料庫主機經檢測發現，SSL簽章使用不安全的Hash演算法，連線資訊可能遭受破解而洩漏



3 E機關OOO資料庫主機帳號未啟用帳號與密碼原則設定

4 A機關OOO資料庫主機經檢測發現，SSL使用中強度的加密，防護強度不足有被破解偷窺的風險

## 主機安全檢測改善建議：



1. 資料庫軟應定期進行軟體更新或評估可行之風險控管措施，進行風險管理
2. 使用具有更高安全性的加密簽章方式
3. 針對資料庫主機應強制啟用帳號與密碼原則設定，強化帳號密碼安全性
4. 停止中強度的SSL加密演算法，採行更安全的加密演算法

# 共同發現事項(3/4)

**1** E機關XXX資通系統存在跨網站腳本攻擊弱點未修補，可能竊取使用者Cookie中之機敏資料或將使用者自動引導至釣魚網站



**2** D機關XXX資通系統存在無效的存取控管弱點未修補，恐讓使用者取得其他權限方可使用的功能頁面或下載的檔案等

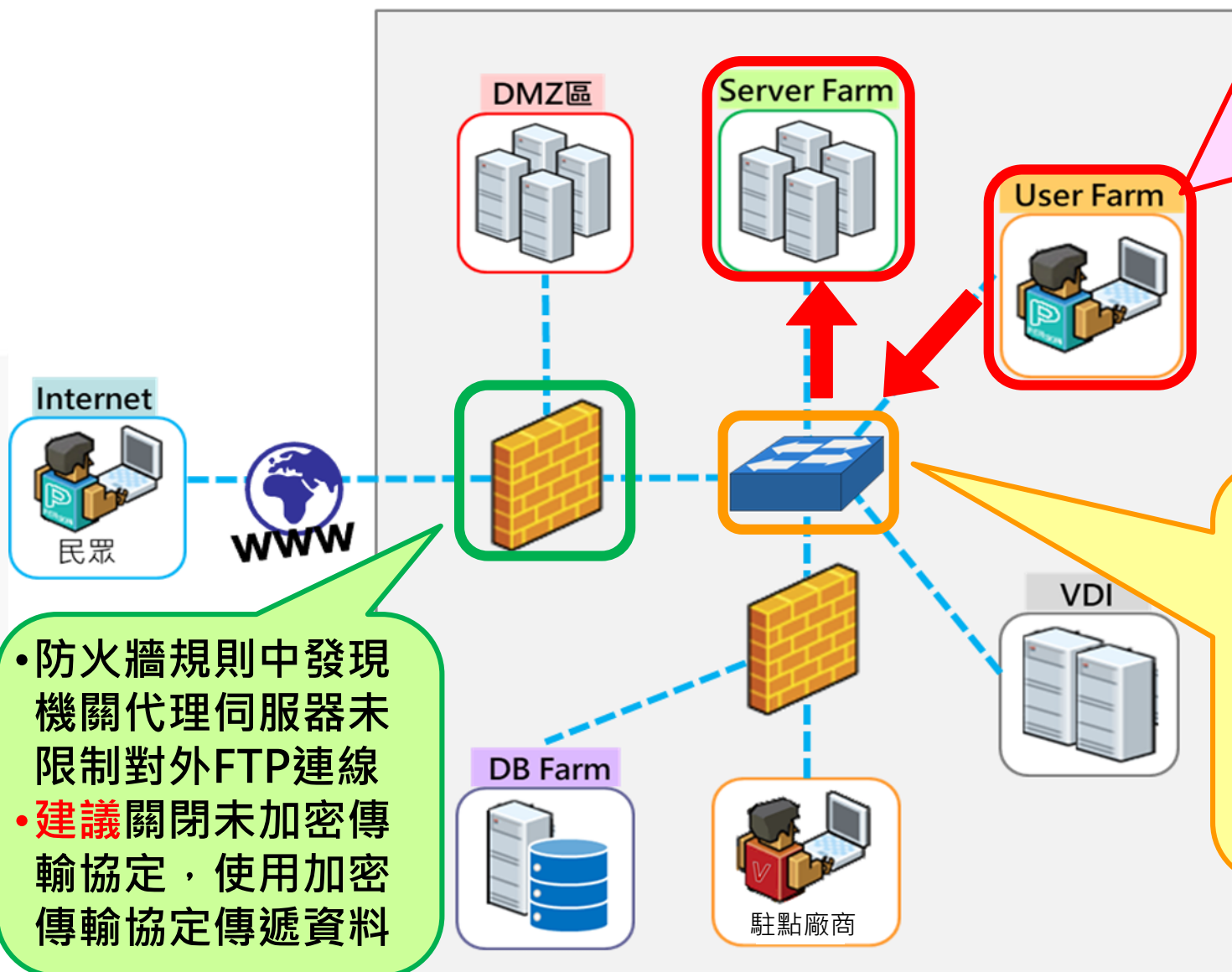
## 資通系統安全檢測改善建議：



1. 過濾可能造成危害的符號及語法輸入，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
2. 建議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



# 共同發現事項(4/4)



- 內網使用者網段與伺服器網段間未有存取控制
- 建議依需求配置網路區域間存取控制

- 核心交換器管理介面，未限制存取之網路位址
- 建議限制僅管理人員IP可存取管理介面

- 防火牆規則中發現機關代理伺服器未限制對外FTP連線
- 建議關閉未加密傳輸協定，使用加密傳輸協定傳遞資料

# 大綱

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

NCCST

# 結論與建議

- 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，同時啟用高強度之協定或演算法

- 加強存取控制措施

- 連網設備、資通系統及資料庫等可透過限縮來源IP或對外服務埠進行網路控管，並搭配帳號權限強化權限區隔

- 建立內部驗證機制

- 資通系統上線前應有基本檢查清單，提醒負責同仁應確認事項；針對弱點修復應檢附驗證結果，確認弱點已無法重現

- 落實資安防護政策

- 應從系統面強制實施防護政策；同時建立稽核制度，定期追蹤未符合資安規範之事件

報告完畢  
敬請指教

NCCST