教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

教育體系資安技術檢測中心
技術檢測與攻防演練分享

國立陽明交通大學 高義智 博士

113年11月

綱要

1. 成立背景與目標
2. 教育體系資安技術檢測作業
3. 教育體系資安攻防演練作業

TACCST

1.成立背景與目標

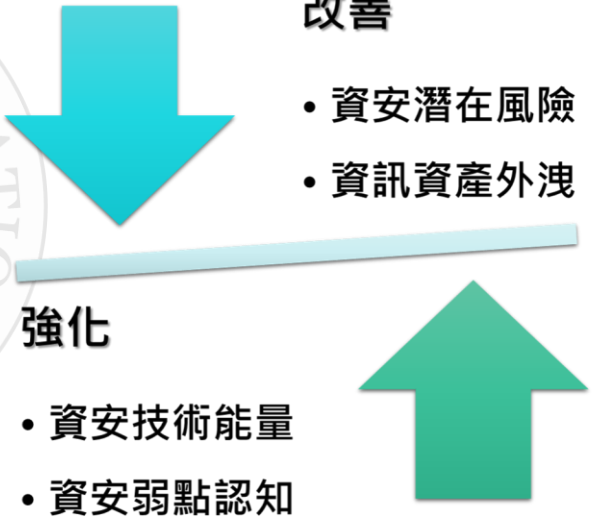
成立背景

根據107年行政院頒布之「**資通安全管理法**」及其子法「**資通安全責任等級分級辦法**」，明確要求各級機關（包括教育單位）應建立的資安防護基準，並應依其資通安全責任等級辦理資通安全應辦事項。

為確保教育體系實施「**資通安全管理法**」及「**教育體系資通安全暨個人資料管理規範**」的完整性及有效性，教育部成立「**教育體系資安檢測技術服務中心**」（**TACCST**）執行**資安技術技術檢測作業**及**資安攻防演練作業**。

目標

本中心**透過在教育體系執行資安技術檢測、資安攻防演練發現潛在問題，降低未來風險發生可能性及影響程度**，保護教育機構重要資產，亦**提升資通安全防護及個資保護之觀念，強化各教育機構資通安全防護工作**。



2.教育體系資安技術檢測作業

2.1 技術檢測概述
2.2 技術檢測流程及內容說明
2.3 技術檢測案例分享

TACCST

2.1 技術檢測概述

- 技術檢測背景說明
- 技術檢測實施對象及時程
- 技術檢測實施項目

1. 背景

教育部為落實資通安全管理法、教育部所管特定非公務機關資通安全管理作業辦法，規劃每年度自所屬公務機關及所管特定非公務機關擇定受稽核對象，委由教育體系資安檢測技術服務中心（TACCST）辦理資安稽核技術檢測作業，查核其資通安全管理法法遵事項符合情形與資通安全維護計畫實施情形，以協助機關改善並強化資通安全防護工作之完整性及有效性。

檢測目的：

- 增進教育體系**資通安全防護環境**
- 強化全國教育體系機關（構）對**資安弱點之認知與維護**
- 提升資安技術檢測**人員能力**

技術檢測實施對象與時程

實施對象

- 國立大專院校 (47間)
- 部屬機關(構) (11間)
- 國民及學前教育署、青年署、體育署

作業時程

- 該年度3月至12月

技術檢測實施項目

項次	檢測項目	檢測子項
1	使用者電腦安全檢測	使用者電腦弱點掃描
		使用者電腦安全防護檢測
2	網路惡意活動檢測	中繼站連線阻擋檢測
3	核心資通系統安全檢測	核心資通系統內網滲透測試
		核心資通系統防護基準檢測
4	網路架構檢測	網路架構檢測
5	目錄伺服器安全檢測	目錄伺服器安全防護檢測
6	物聯網設備安全檢測	物聯網設備安全檢測
7	組態設定安全檢測	組態設定安全檢測
8	資料庫安全檢測	資料庫安全檢測
9	準備作業配合度	應備文件及相關紀錄完整性

2.2 技術檢測流程及內容說明

- 整體實施流程
- 前期整備階段
- 中期檢測階段
- 後期改善階段

TACCST

教育部第二方技術檢測作業流程

機關自評

- 受稽方填寫**「資通安全實地稽核項目檢核表」**、**「受稽方現況調查表」**、**「技術檢測基本資料調查表」**及**「核心資通系統調查表」**等作業表單

技術檢測

- 進行1至3天之技術檢測（部屬機關(構)、國立大專校院適用）
- **技術檢測結果作為實地稽核參考**

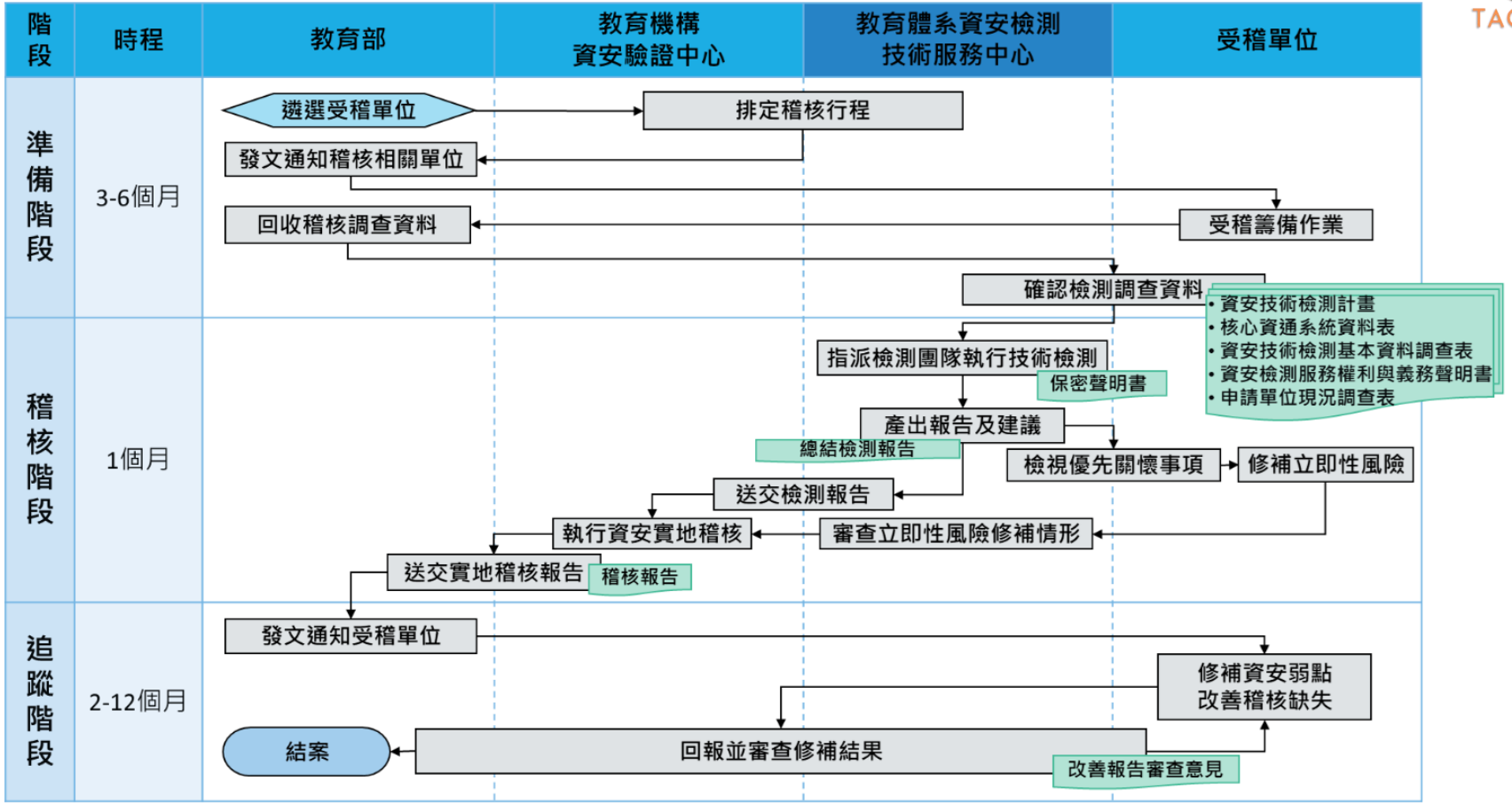
實地稽核

- 由ISCB稽核領隊帶領稽核團隊進行實地稽核

獎勵及改善

- 依受稽方屬性分組，函請表現優良機關行政獎勵相關人員
- 函送資安稽核報告予受稽方，請其就待改善事項研議因應作為及辦理時程

教育部體系第二方技術檢測作業流程

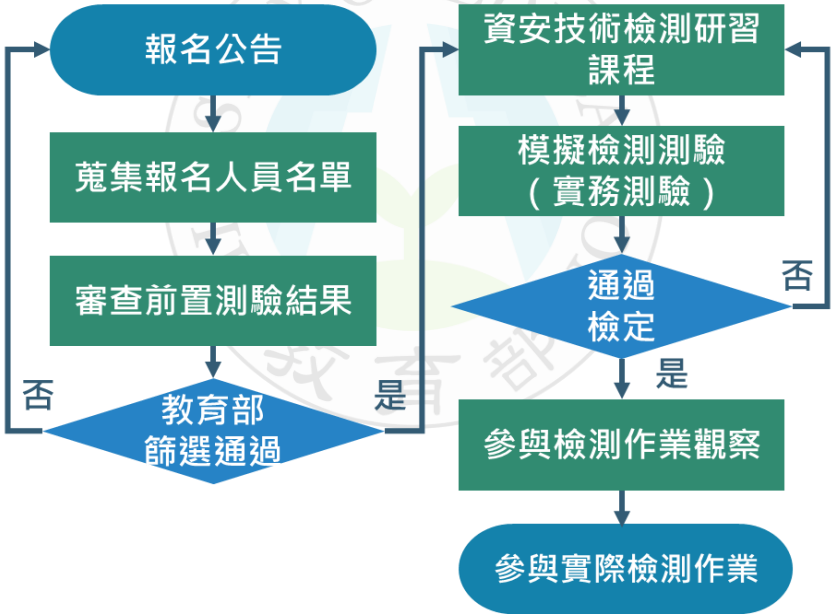


前期整備階段 - 培育新進技術檢測人才

- 目的：持續培育資安人才參與檢測培訓。
- 實施：
  - 【辦理資安檢測技術課程】：因應檢測作業規劃調整課程內容，除針對各檢測項目作業方式及技巧進行深度說明，課程結束前，學員亦需依設計之模擬檢測案例，完成相關檢測報告以驗證其檢測實務能力。

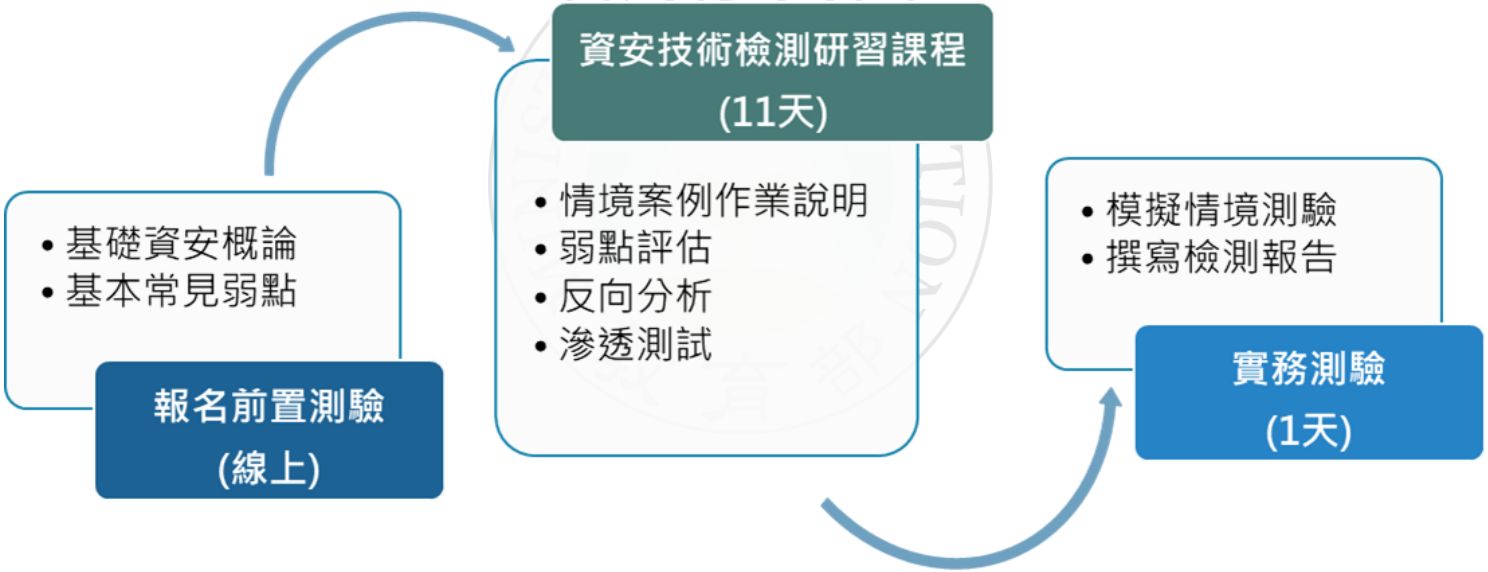
前期整備階段 - 培育新進技術檢測人才

- 辦理資安檢測技術課程流程如下：



前期整備階段 - 培育新進技術檢測人才

- 目的：**持續培育教育體系資安檢測人員**。



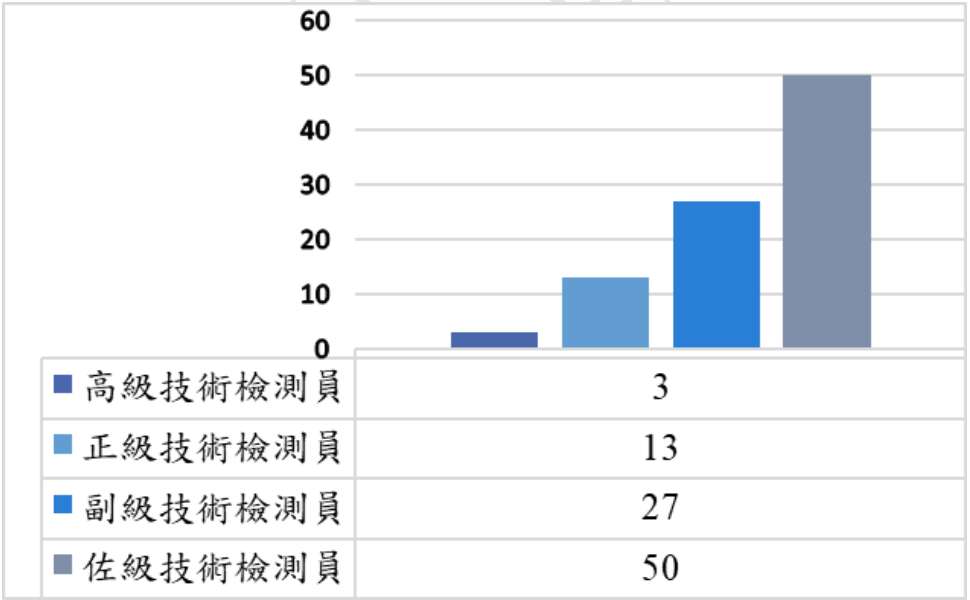
※單位主管需同意學員未來參與技術檢測作業。

前期整備階段 - 強化既有人員技術能量

- 目的：
  - 強化既有技術檢測員能力，提升團隊技術檢測能量。
- 實施：
  - 【與資安專家團隊經驗交流】：邀請資安專家團隊共同參與檢測作業、技術經驗分享，以增進檢測團隊資安技能多元性，如國家資通安全研究院及業界專業資安人員等。
  - 【帶動團隊合作向心力】：透過本中心團隊社群帶動人員向心力，促進檢測人員交流。

前期整備階段 - 技術檢測員統計

- 自108年起，已培育**共93位**技術檢測員



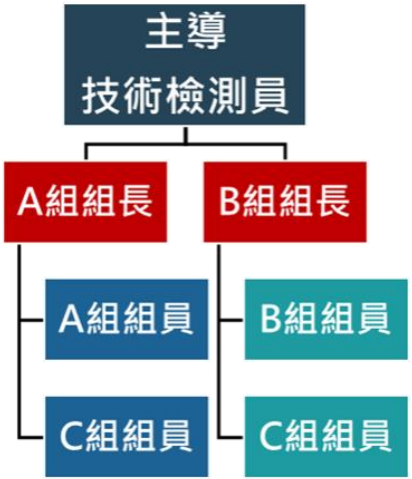
高級技術檢測員	3
正級技術檢測員	13
副級技術檢測員	27
佐級技術檢測員	50

前期整備階段 - 技術檢測平台建置

- 目的：
  - 為提升受稽單位配合作業實施效率，優化技術檢測作業流程。
- 實施：
  - 【受稽單位配合及調查作業系統化】：於本計畫中心網站另新增開發單位配合功能模組，如事前確認調查文件及優先關懷事項等，亦根據技術檢測團隊內部行政作業調整部分功能，如檢視檢測報告及人員審查等。

中期檢測階段 - 技術檢測作業團隊分工

- 目的：
  - 為提升技術檢測合作實施功效，進行技術檢測作業團隊分工。
- 實施：
  - 【建立組長組員機制】：請較具經驗之技術檢測員擔任小組組長，藉由組長協助檢視小組實施進度，協助帶領組員實施檢測作業，以平衡團隊人員能力，激勵及凝聚團隊精神。



中期檢測階段 - 現場實施情形

中期檢測階段 - 技術檢測項目類別

端點安全

- 使用者電腦安全檢測
- 物聯網設備安全檢測

網路安全

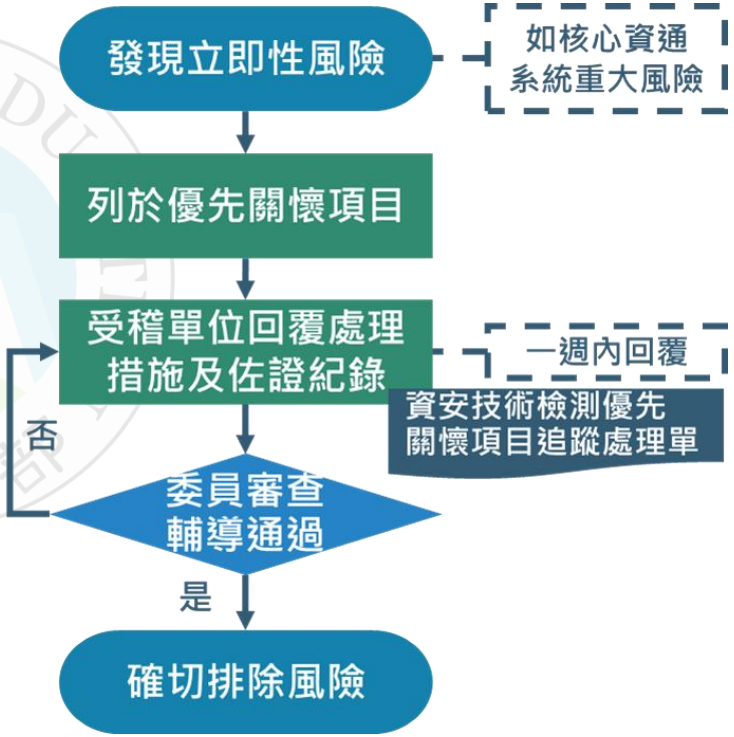
- 網路惡意活動檢測
- 網路架構檢測

系統安全

- 核心資通系統安全檢測
- 資料庫安全檢測
- 目錄伺服器安全檢測
- 組態設定安全檢測

後期改善階段 - 優先關懷項目

- 針對檢測發現之立即性風險列於優先關懷追蹤事項，單位需於檢測作業後一週內回覆處理措施及佐證紀錄，並為確認受測單位改善修補情形將安排委員實施審查追蹤，若單位對於優先關懷追蹤事項之改善實施較為不易，將對其加以輔導，確保立即性風險已排除。



後期改善階段 - 整體改善追蹤

- 目的：
  - 於檢測發現之風險需請單位進行改善修補作業，確切追蹤單位作業實施情形。
- 實施：

【改善追蹤機制】：針對檢測發現之風險，單位需於收到總報告後一個月內回覆處理措施及提供佐證紀錄，且須於三個月內完成整體改善修補，並為確認受測單位改善修補情形將安排委員實施審查追蹤，確保風險已排除。

後期改善階段 - 資安健診作業宣導

- 目的：
  - 針對「全體教育體系資安技術相關人員」強化其對資安之認知與維護，並了解資安健診之重要性。
- 實施：
  - 【辦理教育體系資安健診基礎課程】：為培育教育體系資通相關人員資通安全專業知能，並宣導資安健診作業外，亦透過邀請本中心計畫培訓之技術檢測員授課分享技術檢測經驗及常見缺失改善建議。

2.3 技術檢測案例分享

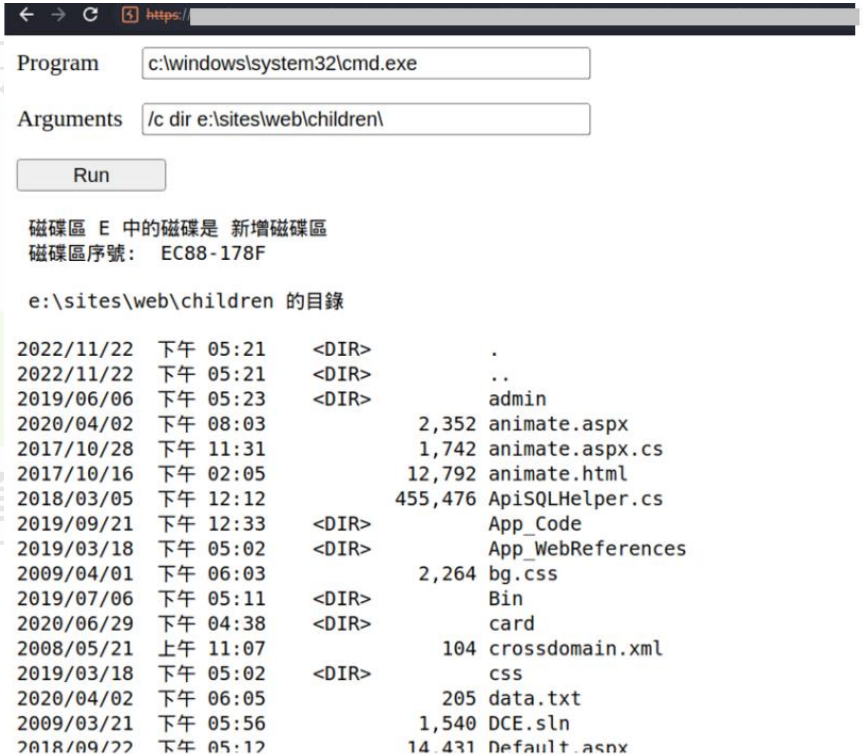
案例分享 - 系統可進行注入式攻擊取得個資

- 檢測員透過SQLinjection可取得系統上之使用者身分證、信箱、姓名。

ID_NO	A_SN	EMAIL	A_DATE	A_TIME	IS_PAY	ATM_NUM	CON_ADR	CON_TEL	ENV_NUM	NAME_CH
E 052	2094000350	sm	94/6/2	NULL	N	118 350	NULL	1391	0	黃
E 052	2094000350	sm	94/6/9	NULL	N	118 350	NULL	1391	0	黃
E 052	2094000350	sm	94/6/9	NULL	N	118 350	NULL	1391	0	黃
E 052	2094000360	sm	94/6/10	NULL	N	118 360	NULL	1389	0	黃
E 052	2094000360	sm	94/6/10	NULL	N	118 360	NULL	1391	0	黃
E 052	2094000360	sm	94/6/10	NULL	N	118 360	NULL	1391	0	黃
E 052	2094000361	sm	94/6/10	NULL	N	118 361	NULL	13	0	黃
E 052	2094000362	sm	94/6/10	NULL	N	118 362	NULL	1389	0	黃
E 052	2094000363	sm	94/6/10	NULL	N	118 363	NULL	1389	0	黃
T 316	2094000364	sm	94/6/13	NULL	N	118 364	NULL	1389	0	陳
T 316	2094000364	sm	94/6/13	NULL	N	118 364	NULL	1389	0	陳
E 052	2094000365	sm	94/7/4	NULL	N	118 365	aaaa	1391	0	黃
E 052	29400378	sm	94/7/22	NULL	N	121 378	NULL	13	0	黃
R 743	29400428	NU	94/9/15	16:29	N	121 428	1	NULL	0	蔡
F 348	29400428	NU	94/9/16	11:14	Y	121 428	NULL	NULL	0	林
C 855	29400429	NU	94/9/29	16:13	N	121 429	NULL	NULL	0	田
C 855	29400429	NU	94/9/29	16:15	N	121 429	NULL	NULL	0	田
N 099	29400429	SP EDU.TW	94/9/30	10:57	N	121 429	NULL	1389	0	洪
N 099	29400429	SP EDU.TW	94/9/30	10:57	N	121 429	NULL	1389	0	洪
N 099	29400429	SP EDU.TW	94/9/30	10:57	N	121 429	NULL	1389	0	洪

案例分享 - 系統可上傳webshell，取得控制權

- 檢測員透過在網站上傳websdhell，可直接取得server控制權，執行任一指令。



案例分享 - 印表機使用弱密碼取得個資

- 印表機開啟ftp服務，且該服務使用弱密碼，可取得印表機之檔案，如護照影本。

案例分享 - 監視器不安全之設定

- 外部網路可直接查看校內監視器。

3. 教育體系資安攻防演練作業

3.1 背景說明
3.2 演練架構及內容說明
3.3 實施成果

3.1 演練概述

- 攻防演練背景說明
- 實施對象、時程及範圍
- 弱點測試方式

背景說明

教育部為落實資通安全管理法、資通安全事件通報及應變辦法之規定。規劃每年對**教育體系國立大專院校**及**私立大專院校**實施資安攻防演練，並由教育體系資安檢測技術服務中心（TACCST）協助辦理，以**了解演練單位遭受資安攻擊時其內外部防護與通報應變實施情形。**

演練目的：

- 強化大專院校資安防護工作之**完整性**及**有效性**
- 增進發生資安事件時之**緊急應變**、**系統復原**及**協調管控**等能力
- 檢討防護改善**降低資安風險**

112/113年度實施對象與時程

實施對象

- **教育部（試辦）**
- 國立大專院校（共47間）
- **部分私立大專院校（2間）**

作業時程

- 112年度：11月至12月，為期5週。
- 113年度：7月至9月，為期10週。

112/113年度實施範圍

範圍標的

- 使用演練單位之**學校校名、網域名稱**或**IP**，並可**透過外部Internet連線之服務(實施範圍主要為：網站、主機)**。
- 113年度實施範圍納入實驗室網站。
- 114年度擬納入IoT 設備檢測

弱點測試方式

演練方式：

- 教育體系資安檢測技術服務中心（TACCST）以**白帽駭客身份於外部於網路遠端檢測演練單位之資訊服務**，找出服務存在之弱點，並**通知演練單位於時限內完成資安事件通報、應變、修補程序。**

測試類型：

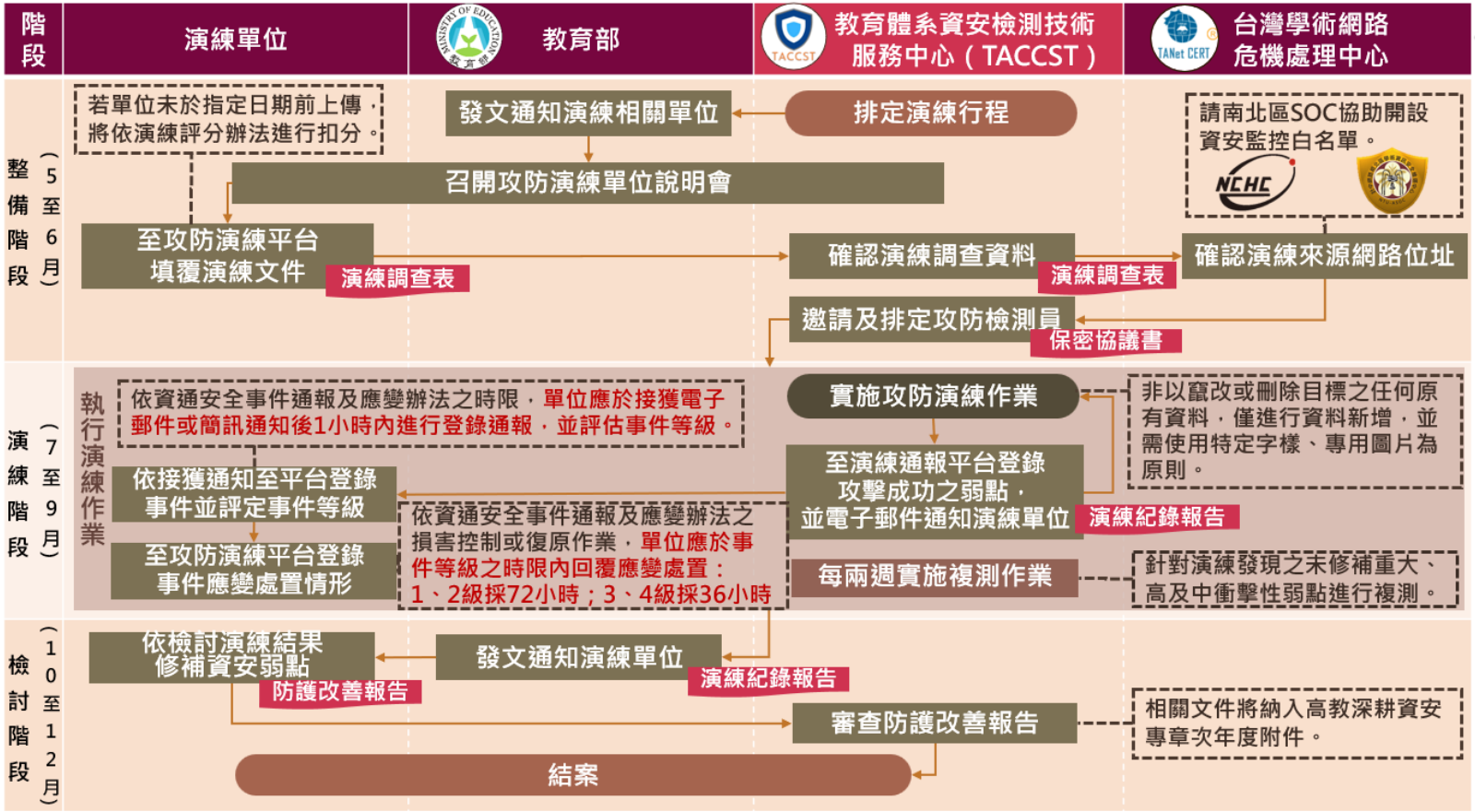
- 不限定檢測手法或類型，惟演練過程中為避免影響網站系統維運及人員社交爭議，**不採用DoS、DDoS及社交攻擊等手法**。

3.2 演練架構及內容說明

- 整體實施流程
- 前期整備階段
- 中期演練階段
- 後期檢討階段

TACCST

整體實施流程


階段
演練單位
教育部
教育體系資安檢測技術服務中心（TACCST）
台灣學術網路危機處理中心
整備階段（5至6月）
若單位未於指定日期前上傳，將依演練評分辦法進行扣分。
發文通知演練相關單位
排定演練行程
請南北區SOC協助開設資安監控白名單。
召開攻防演練單位說明會
至攻防演練平台填覆演練文件
演練調查表
確認演練調查資料
演練調查表
確認演練來源網路位址
邀請及排定攻防檢測員
保密協議書
演練階段（7至9月）
執行演練作業
依資通安全事件通報及應變辦法之時限，單位應於接獲電子郵件或簡訊通知後1小時內進行登錄通報，並評估事件等級。
實施攻防演練作業
非以竄改或刪除目標之任何原有資料，僅進行資料新增，並需使用特定字樣、專用圖片為原則。
依接獲通知至平台登錄事件並評定事件等級
至演練通報平台登錄攻擊成功之弱點，並電子郵件通知演練單位
演練紀錄報告
至攻防演練平台登錄事件應變處置情形
依資通安全事件通報及應變辦法之損害控制或復原作業，單位應於事件等級之時限內回覆應變處置：1、2級採72小時；3、4級採36小時
每兩週實施複測作業
針對演練發現之未修補重大、高及中衝擊性弱點進行複測。
檢討階段（10至12月）
依檢討演練結果修補資安弱點
防護改善報告
發文通知演練單位
演練紀錄報告
審查防護改善報告
相關文件將納入高教深耕資安專章次年度附件。
結案

攻防演練三階段

- **整備階段**
  - 演練前說明會
  - 檢測員招募
  - 檢測環境建置
  - 演練平台建置
    - 漏洞管理功能
    - 檢測員排行榜
    - 漏洞統計
- **演練階段**
  - 挖掘資安弱點
  - 演練事件通知
  - 資安事件等級判定
  - 資安漏洞復測
- **檢討階段**
  - 防護檢討
  - 檢測發現與建議

前期整備階段 - 演練前說明會

- 112/113年度，北中南各辦理3場演練前說明會，對實施單位佈達今年度攻防實施範圍及相關細則，協助單位演練更加了解演練目的及需配合之事項。

北部

中部

南部

前期整備階段 - 檢測員招募

招募對象

- **本國國籍且具資安檢測實作專業知能之人員**

主要來源

- **既有檢測員**：曾任行政院、教育體系攻防演練檢測員、教育體系資安技術檢測員
- **新進檢測員 (需符合以下條件之一，並經由審查後入選)**：
  - **滲透實務證照**：如 CEH Practical/ECSA(CPENT)/OSCP/OSEP/OSWE
  - **資安競賽經驗**：國內外資安相關競賽入圍初賽/複賽等具體實績。
  - **通過本中心前置測驗**

前期整備階段 - 檢測環境建置

動態IP對外攻擊

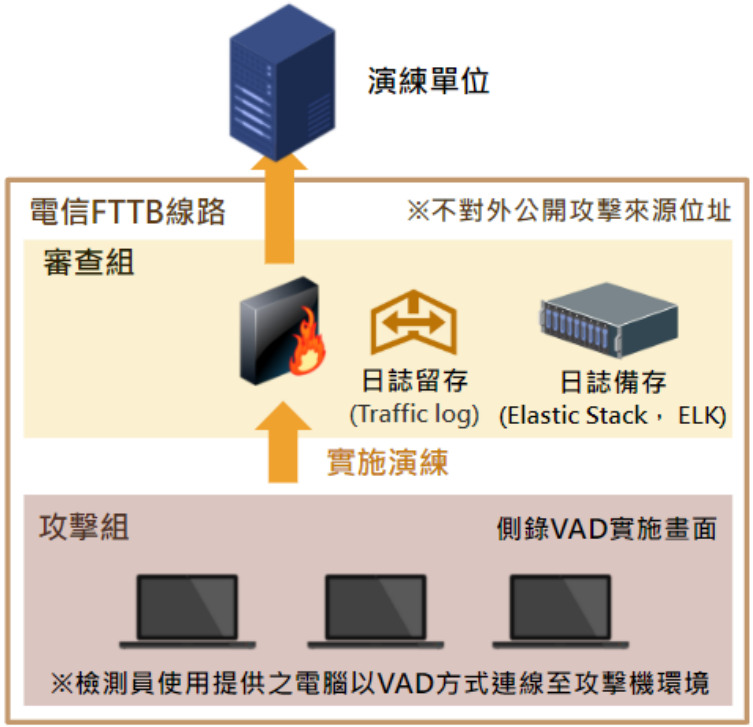
- 不定期切換攻擊來源IP，以繞過演練單位防護機制。

監管攻擊組操作

- 建置安全連線環境，並於演練期間全程監控流量及螢幕錄影。

留存完整紀錄

- 留存完整演練紀錄，以利異常事件發生時查檢。



前期整備階段 - 演練平台建置

- 因演練期間所發現的漏洞皆需完整、精確、即時地紀錄通知，以利後續受測單位修補緩解措施，本中心依整體實施流程及需求，建置教育體系資安攻防演練平台。

前期整備階段 - 演練平台建置

漏洞管理功能

1. **漏洞提交**：檢測員**透過平台詳細紀錄每筆漏洞發現**之攻擊手法。
2. **漏洞審核**：審查員**透過平台審查檢測員所提報之每筆漏洞**，審核通過後將認列為演練資安事件。
3. **漏洞通知**：工作人員**透過平台發送電子郵件/簡訊通知受測窗口演練資安事件**。
4. **漏洞排除**：受測窗口**透過平台回報資安事件處置情形**。
5. **復測漏洞**：審查組**透過平台通知受測窗口復測結果**。

前期整備階段 - 演練平台建置

統計功能

1. **檢測員排行榜**：為鼓勵攻防檢測員提繳弱點，將依提報漏洞貢獻度提供獎金，檢測員可於平台以匿名制及時查看排名。
2. **漏洞統計**：管理者可於平台查看各項統計資訊，如：漏洞類型、衝擊性等級、各受測單位漏洞數量。

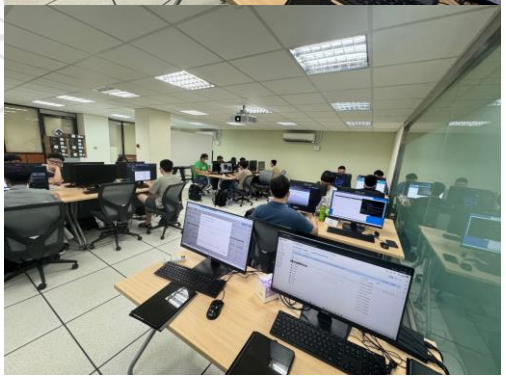
中期演練階段 - 挖掘資安弱點

作業時程

- 113年7月至9月，為期10週
- 每週平均實施7個單位

作業方式

- 攻擊手於演練期間，透過本中心場域環境，以灰箱測試手法發掘單位潛在資安弱點。



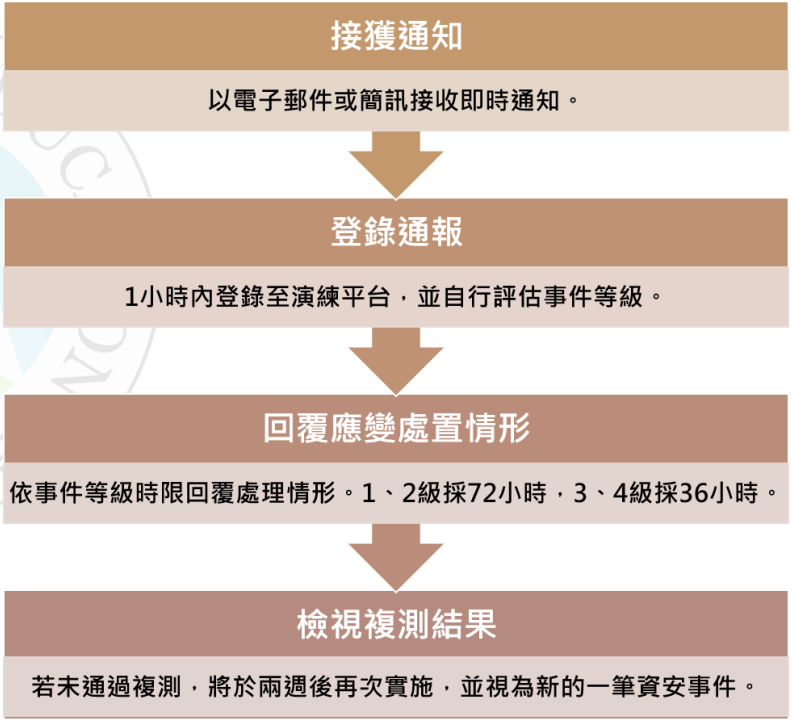
中期演練階段 - 挖掘資安弱點

通知方式

本中心將以**電子郵件**為主，**簡訊**為輔方式通知演練單位窗口。

單位通報/應變

1. 單位於接獲通知1小時內登入演練平台進行通報。
2. 依資安事件等級，1、2級採72小時，3、4級採36小時進行應變。



中期演練階段 - 資安事件等級判定

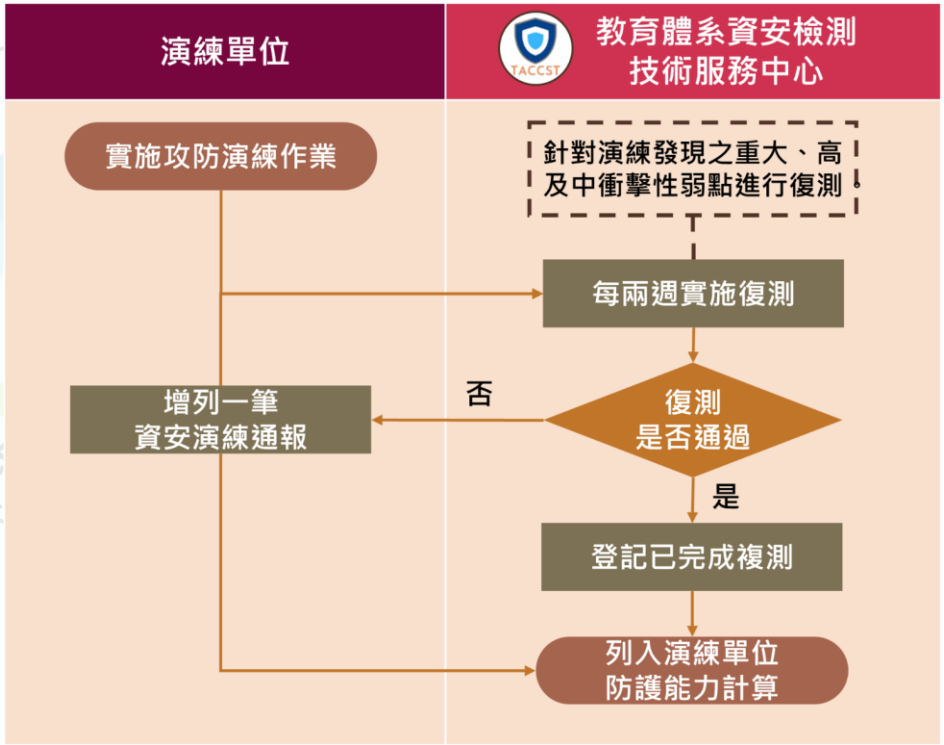
類別	機密性（資訊洩漏）		完整性（資訊/資通系統遭竄改）		可用性（業務/資通系統運作遭中斷）	
影響程度 / 業務性質/資通系統別	洩漏程度		竄改程度		可否於可容忍時間內回覆	
	輕微	嚴重	輕微	嚴重	輕微	嚴重
非核心業務	1 級	2 級	1 級	2 級	1 級	2 級
非核心資通系統			1 級	2 級		
未涉及 CI 維運之核心業務	2 級	3 級	2 級	3 級	2 級	3 級
未涉及 CI 維運之核心資通系統			2 級	3 級	2 級	3 級
涉及 CI 維運之核心業務	3 級	4 級	3 級	4 級	3 級	4 級
涉及 CI 維運之核心資通系統			3 級	4 級	3 級	4 級
一般公務機密、敏感資訊	3 級	4 級	3 級	4 級		
國家機密	4 級	4 級	4 級	4 級		

※國家關鍵基礎設施(Critical Infrastructure, CI)

中期演練階段 - 資安漏洞復測

復測通過標準

- 網站可連線，弱點已修復無法復現。
- 網站可連線，有弱點之功能/網頁已不存在。
- 網站已下架，無法存取有弱點之功能/網頁。



後期檢討階段 - 防護檢討

總報告

- 本中心於演練結束後，將依單位彙整演練發現於總報告，由教育部函文通知攻防演練單位結果。

防護改善報告

- 演練單位除需針對遭攻擊成功之弱點進行漏洞修補外，亦需針對通報發現進行檢討，且提繳防護改善報告，本中心將實施一次性審查作業，其相關文件皆納入高教深耕資安專章次年度附件。

後期檢討階段 - 檢測發現與建議

- 於112年度舉辦實體與線上共兩場次研討會，分享攻防演練中常見的漏洞，以及如何針對各類型漏洞進行預防、緩解、修補。

北部　　南部

3.3 實施成果

- 檢測人員統整
- 漏洞類型統計
- 案例分享

112/113年度參與人員

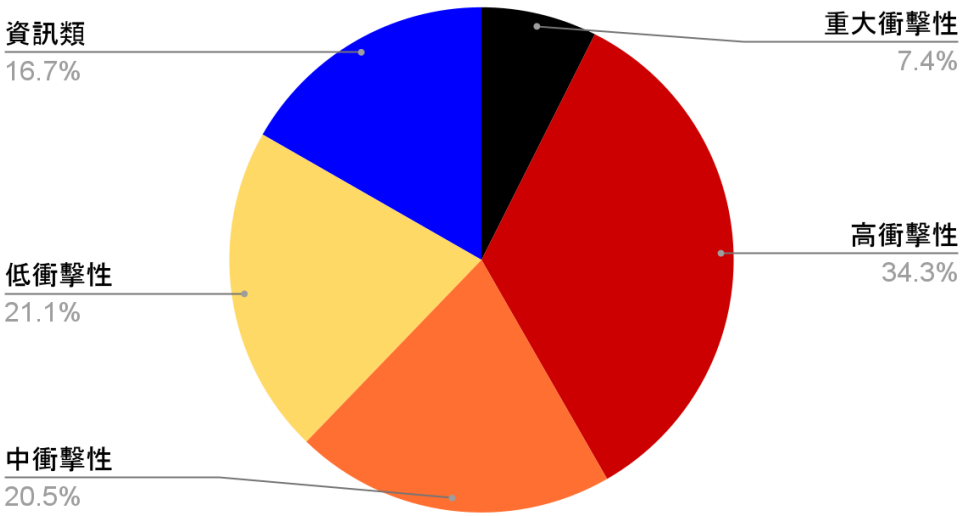
- 112/113年度共**107位**參與教育體系資安攻防演練。

類型	單位	112年度(人)	113年度(人)
既有檢測員	公務機關	14	10
	業界	0	1
	學生	0	8
新進檢測員	公務機關	7	17
	業界	3	7
	學生	13	27
總計		**37**	**70**

112年度實施成果 - 共發現741筆風險

- 從8236筆單位提供之系統清冊進行抽測，共發現741筆風險。

衝擊性等級圓餅圖



類型	數量(筆)
資訊類	124
低衝擊性	156
中衝擊性	152
高衝擊性	254
重大衝擊性	55
總計	741

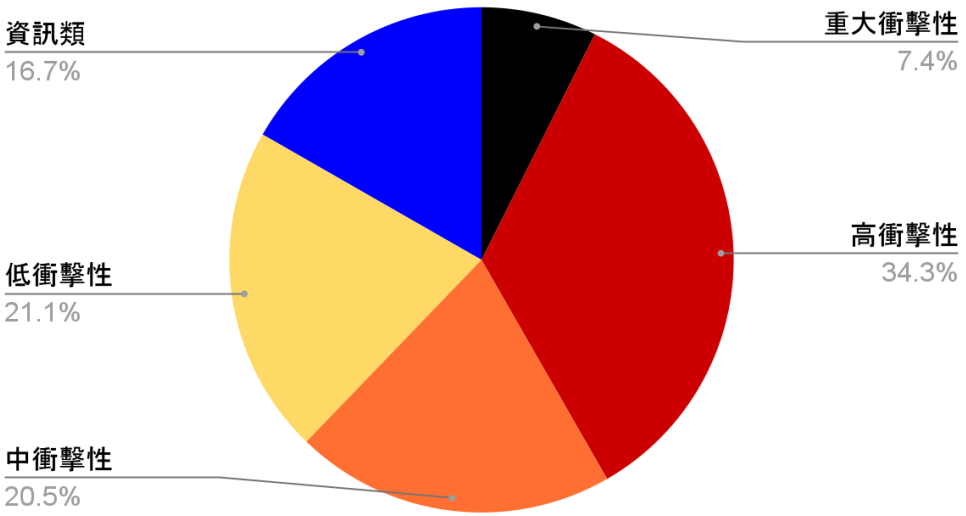
112年度實施成果 - 常見發現類型

類型	百分比(%)
A03:2021- Injection 注入式攻擊	45
A01:2021- Broken Access Control 權限控制失效	25
A05:2021- Security Misconfiguration 安全設定缺陷	10
A10:2021- Server-Side Request Forgery(SSRF) 伺服端請求偽造	6
A07:2021- Identification and Authentication Failures 認證及驗證機制失效	5
A04:2021- Insecure Design 不安全設計	5
A02:2021- Cryptographic Failures 加密機制失效	2

113年度實施成果 - 共發現601筆風險

- 從12867筆單位提供之系統清冊進行抽測，共發現601筆風險。

衝擊性等級圓餅圖



類型	數量(筆)
資訊類	102
低衝擊性	203
中衝擊性	52
高衝擊性	116
重大衝擊性	128
總計	601

112年度實施成果 - 常見發現類型

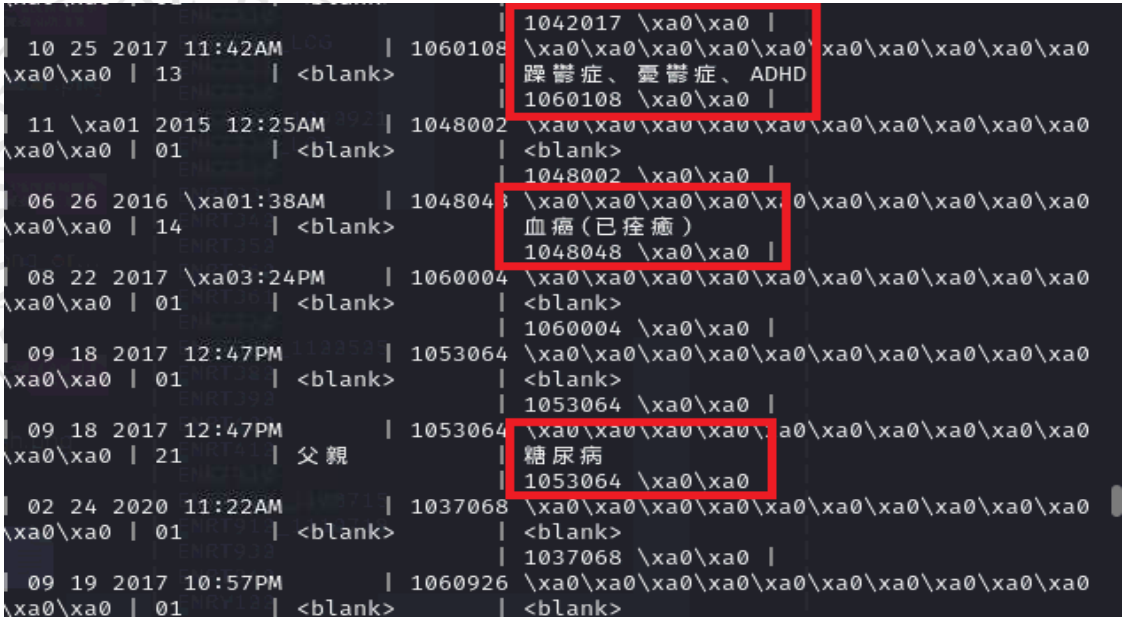
類型	百分比(%)
A03:2021- Injection 注入式攻擊	46
A01:2021- Broken Access Control 權限控制失效	20
A06:2021- Vulnerable and Outdated Components 危險或過舊的元件	13
A05:2021- Security Misconfiguration 安全設定缺陷	7
A07:2021- Identification and Authentication Failures 認證及驗證機制失效	7
A04:2021- Insecure Design 不安全設計	4
A10:2021- Server-Side Request Forgery(SSRF) 伺服端請求偽造	3

案例分享 - 權限控制失效取得個資

- 系統不需權限驗證即可下載考生身分證影本。

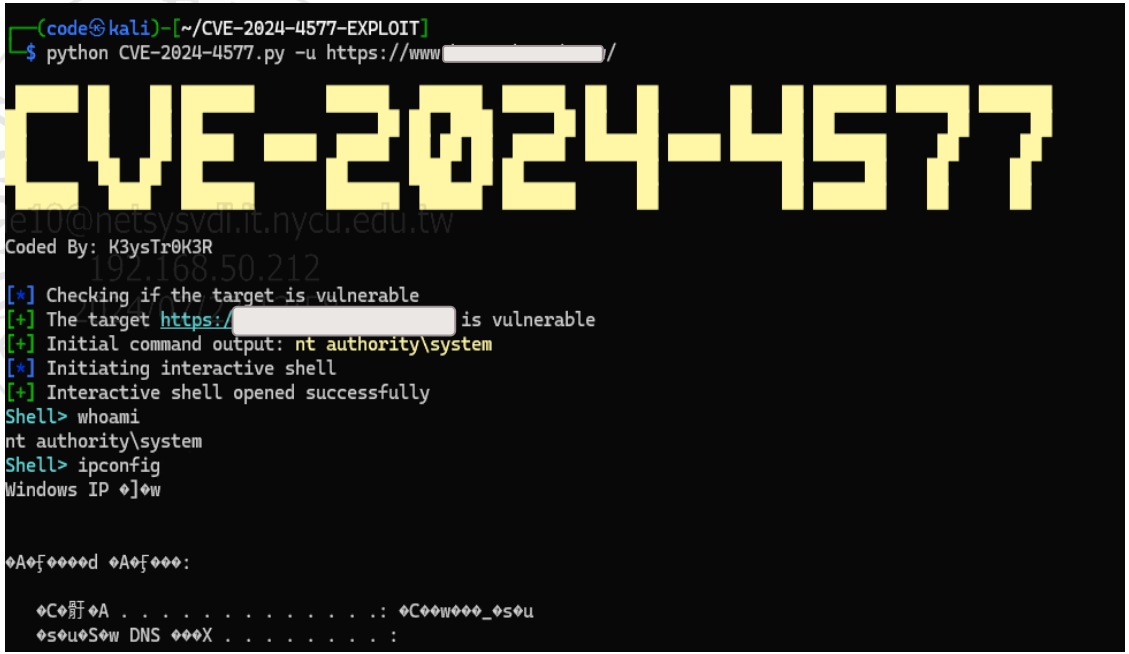
案例分享 - 注入式攻擊取得醫療紀錄

- 透過SQL injection可取得資料庫中醫療特種個資



案例分享 - 透過CVE取得主機控制權

- 因部分系統使用較舊元件版本，可透過腳本取得主機完整控制權。



教育體系資安檢測技術服務中心

Taiwan Academic Network Center for Cyber Security Technology

感謝大家攜手合作！
為教職員生提供資通安全環境

taccst@nycu.edu.tw