教育部 113 年度對國私立大專院校資安攻防演練計畫

113 年 5 月

壹、 依據

資通安全管理法(以下簡稱資安法)及資通安全事件通報及應變辦法、資通安全責任等級分級辦法。

貳、 目的

一、透過政府、學術及研究機構共同合作，辦理教育體系資安攻防演練計畫，以檢測教育體系國立及私立大專院校對外系統之資安防護能力。

二、為檢視及強化教育體系國立及私立大專院校面對資通系統發生資安事件時之緊急應變、系統復原及協調管控等能力，以檢討教育體系整體資安防護措施，並研討資安防護精進作為。

參、 演練總期程

113 年 5 月至 113 年 12 月

肆、 執行單位

本計畫由教育部發起，並委由教育體系資安檢測技術服務中心辦理(以下簡稱檢測中心)，以統籌編成資安攻防演練團隊(以下簡稱演練團隊)，負責規劃與執行資安攻防演練各項事宜。

伍、 資安攻防演練作業

由本演練團隊辦理資安攻防演練，以因應近期資安威脅樣態，並納入最新版本之開放式網頁應用安全計畫(Open Worldwide Application Security Project, OWASP)前 10 大網站應用(Web Application) 及應用程式程式設計介面(API)等資安弱點為原則進行測試，實際演練單位資安防護

與應變處理能力。

(一)演練期間

113 年 7 月至 113 年 9 月之工作日，共 3 個月

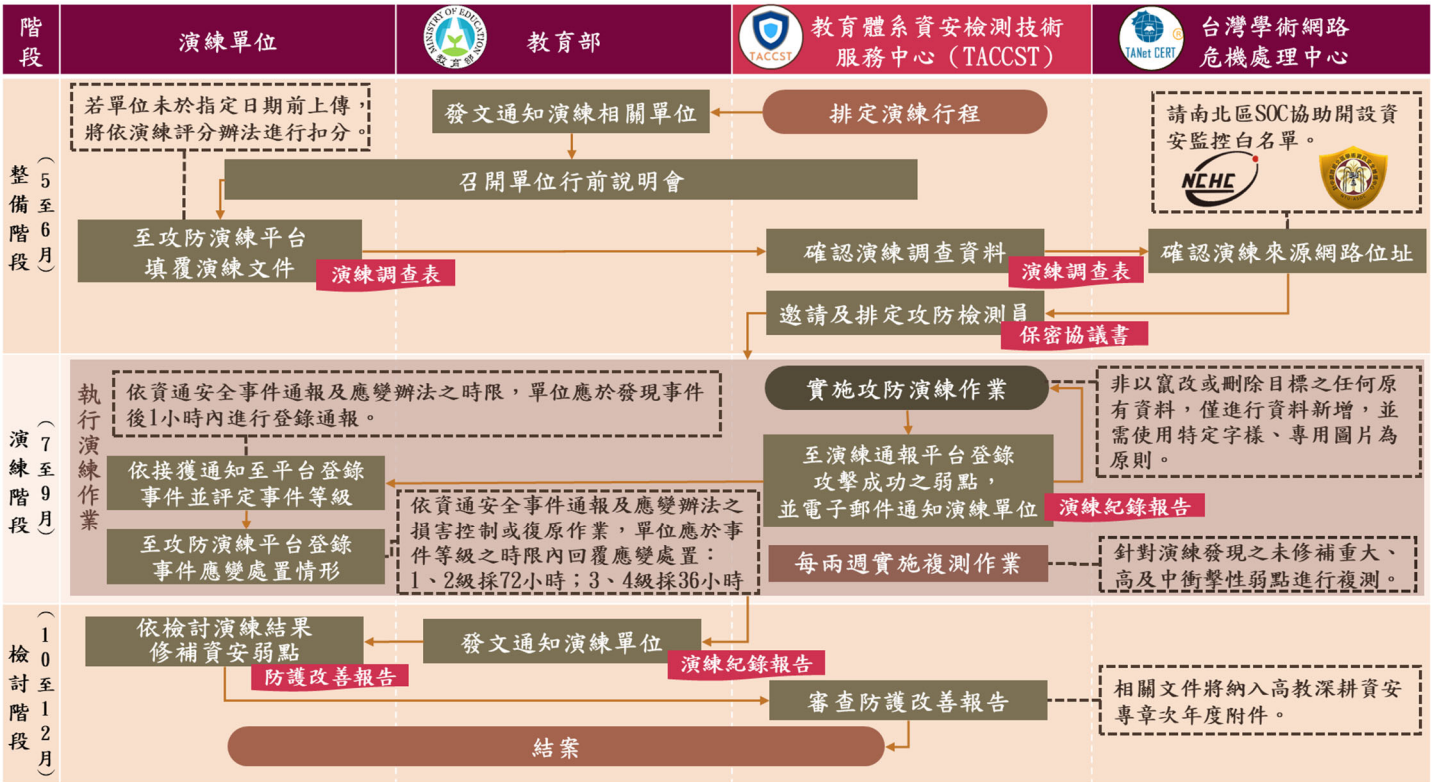
(二)演練對象

全國立大專院校（共 47 間）及私立大專院校（共 2 間），總計共 49 間。

(三)範圍標的

使用演練單位之單位名義、網域名稱（DN）或網路位址（IP），並可透過外部 Internet 連線之服務型網頁，演練中所有發現皆實施演練通報並全數列入計分。

(四)執行方式



陸、 整備階段

資安攻防演練開始執行前，演練單位及演練團隊應先整備以下事項：

一、演練單位整備事項

資通安全長應督導演練單位辦理資安教育訓練或相關防護事宜，包含：

(一)指派演練期間聯絡窗口，演練單位推派主要及次要演練窗口(共兩名)於 113 年 5 月 10 日（週五）起至「教育體系資安攻防演練平台」（以下簡稱演練平台，網址：https://code.moe.edu.tw/）註冊或登入，並於 113 年 6 月 21 日（週五）晚上 24 時前於該平台填報演練調查相關資料。若未於指定日期前至規定之平台繳交，將依演練評量辦法(詳見附件)進行扣分。

(二)演練期間，演練團隊如有任何需釐清或待溝通之事項，將統一聯絡單位所指派之主要及次要演練窗口，並由主要窗口彙整及回復，避免演練期間需向各項受測系統之維運人員進行聯繫。

(三)建議做好系統備援，並定期備份重要資料，備份過程中，必須驗證備份檔案的正確性與可用性。

(四)訂定系統與資料回復作業程序，並進行復原測試，於系統回復後，測試相關功能與資料是否回復。

(五)進行通報聯絡測試，以確保通報管道暢通。

二、演練團隊整備事項

(一)召開工作會議

就本計畫演練團隊、分工原則、執行模式及執行範疇等詳予說明與討論，並定期檢視整備工作之進度。

(二)編成演練團隊

依據本計畫演練團隊之組織架構與任務分工，編成各演練團隊分組。

(三)作業環境與監控環境整備

由檢測中心負責規劃、建置資安攻防演練作業環境與監控環境，並提供所需之軟硬體設備。

(四)彙整演練單位相關資料

由檢測中心負責辦理演練單位前置資料蒐集與彙整，為確認演練單位提供之系統調查表內容之正確率，演練單位得以在演練開始前進行清查作業並由單位確認清查結果。

柒、 演練階段

一、演練作業

(一)資安攻防演練由檢測中心以不提供攻擊來源 IP 搭配弱點掃描或滲透測試等方式進行，模擬駭客實際攻擊手法，嘗試取得演練單位內部機敏資料或資通系統控制權限等攻擊方式，藉此檢視單位對外服務型系統網站之機密性或完整性防護能力。

(二)檢測中心執行攻擊發現弱點需將攻擊流程寫至演練平台，經檢視內容是否符合規範，如禁止竄改或刪除攻擊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。若符合則將完成攻擊以紀錄至攻防演練紀錄平台產生攻擊報告，若不符合則將請攻防檢測員補齊資料直至符合規範。

1. 特定字樣

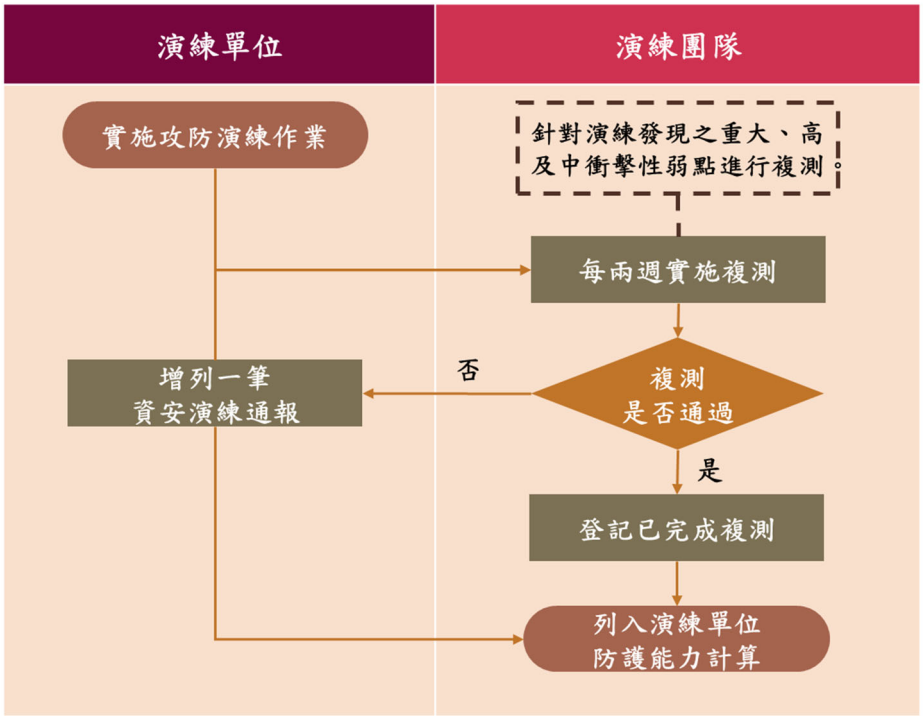
(1) MOE_113CODE
(2) 113 年度教育體系資安攻防演練

2. 專用圖片

二、複測作業

(一)為確保單位確實實施應變損害及復原作業，僅針對資安攻防演練發現之嚴重、高及中衝擊性弱點進行複測，並於每兩週針對未修補之漏洞進行實施。

(二)複測不通過表示系統可連線且該弱點或其衍伸弱點仍存在，經中心確認未通過後將重新發布一筆新警訊通知單位，並視為新的弱點攻擊紀錄，且列入資安攻防演練之防護能力成績計算。



三、監控審查作業

(一)檢測中心應全程記錄攻擊過程以做為證據留存，並不定期抽查攻擊組之攻擊作業是否符合規定。

(二)檢測中心須檢視提繳之攻擊紀錄，以判定攻擊是否成功，若成功即登錄至演練通報平台，並以電子郵件通報為主、簡訊為輔通知演練單位窗口。

(三)如有缺少加註本次演練特殊字樣之情形，經演練單位主動通知後，檢測中心可代為加註，但不協助其修改通報內容，並於備註欄位加註修改時間。

(四)經檢測中心認定攻防檢測員未依規定辦理時，應立即停止該員攻擊作業，並由中心視情節嚴重性決定是否取消該員資格。

四、資訊設備與資料管制作業

(一)未經檢測中心人員同意，相關人員不得將資訊設備攜出或攜入演練場所。

(二)資安攻防演練相關資料或物品應存放於保密箱(櫃)中，由檢測中心專人負責保管。

(三)資安攻防演練作業場所應設置碎紙機處理作廢之資料文件。

(四)資安攻防演練作業執行結束，由檢測中心負責點收相關人員所繳還之軟硬體設備與作業資料(含複製物)等，同時銷毀作廢之資料文件。

(五)本次演練相關之作業表格、紀錄等紙本及電子檔資料，由檢測中心統一保存。

五、作業原則

資安攻防演練作業之執行以不影響演練單位業務正常運作為原則。

六、申訴流程

如演練單位對收到攻擊成功通報存有疑義時，可檢附佐證資料於演練平台向檢測中心進行申訴，單位申訴案件由教育部承辦窗口及檢測中心進行複審，並由檢測中心擔任單一窗口回復申訴結果。

另申訴處理時程與相關注意事項如下：

(一)演練單位於收到通報後，如有申訴需求須於 5 個工作天內至攻防演練平台填報攻防演練申訴，並檢附佐證資料，若演練單位送交超過 5 個工作天，檢測中心得不受理申訴案件。演練團隊窗口最遲於 5 個工作天內回復申訴結果。因應演練單位可能有多次回復以補足佐證資料之情形，故檢測團隊回復申訴之起算日以單位最後一次回復時間為計算時間點。

(二)申訴期間請演練單位照常依照通報應變流程進行應變處置措施，勿因申訴作業而停止應變流程。

(三)申訴所附之佐證資料記載內容不得晚於該筆攻擊成功紀錄時間，常見佐證資料如個資聲明同意書、系統紀錄、會議文件及軟硬體手冊等。

(四)每筆攻擊成功通報申訴次數以 1 次為限，經演練團隊回復申訴結果後，該筆警訊申訴即算結束，不再接受任何補充之佐證資料。

(五)若該筆通報申訴通過，將由檢測中心分別刪除攻擊紀錄、通報單等紀錄。

(六)為避免洩漏檢測組來源 IP，檢測中心不回復任何通報結果。請單位自行針對通報內容進行對應處置措施，如：刪除非法帳號、攻擊語法及攻擊程式等。

捌、 演練單位配合事項

一、 演練單位

資安攻防演練期間，演練單位應確實辦理資安防護作業，並依通報應變相關作業程序，辦理資安事件通報及系統弱點修補。

(一)基本防護作業

1. 演練過程不會針對網站進行破壞性測試，惟為避免發生非預期狀況，導致系統發生當機或資料毀損等情事，演練單位於演練期間應做好系統備援與定期（建議每日）備份重要資料等防護措施。

2. 演練單位可利用防火牆、入侵防禦系統及防毒軟體等偵測工具，檢視網路、系統有無異常狀況，並維持系統日常連線狀態及日常防護作業，勿刻意阻撓資安攻防演練。

3. 演練實施前，單位可重新檢視防火牆等相關設定是否合宜、檢視測試系統與帳號等已確實關閉或移除，以及確認內部使用系統未暴露於網際網路。

(二)通報應變作業

1. 演練單位若因檢測中心攻擊行為，致受測目標遭受影響，應依資安法辦理通報應變作業。

2. 演練期間若發現遭受攻擊成功，應於資通安全事件通報及應變辦法規定時間內，至演練平台進行應變處置回覆。若因故填報錯誤，仍須自行至通報應變網站重新登錄事件內容，惟登錄時間以通報應變網站系統記錄時間為主。

3. 演練單位須依資通安全事件通報及應變辦法之損害控制或復原作業時限，進行事件應變處置作業。

玖、 檢討作業

為精進資安防護作為，演練單位及演練團隊應檢討本次演練執行情形。

(一)「演練單位」執行事項

1. 演練單位應儘速檢討遭攻擊成功原因，並完成系統弱點修補。

2. 遭攻擊成功單位應檢視整體資安防護機制，並自行至演練平台中下載資安防護改善計畫範本，資安防護改善計畫填寫完畢後請上傳至演練平台，

得由演練單位資通安全長召開會議檢討改善情形，並追踪改善及落實情形。

3.「資安防護改善計畫」之撰寫範圍為重大、高、中、低衝擊性攻擊紀錄(衝擊性判斷原則請參見附件)，演練單位應整併所屬單位之處理情形。

(二)「演練團隊」執行事項

1. 依資安攻防演練執行成效，討論攻防手法與規劃。

2. 依演練評分辦法(詳見附件)評選防護表現績優與良好單位、待加強單位；攻防檢測員則依評選檢測表現為特優、優等與佳作人員。

3. 召開資安攻防演練檢討會議，研提後續辦理此類演練應注意事項與改進建議。

壹拾、 獎懲及後續作業

一、 單位及人員獎勵

(一)評分標準

依演練單位排定成績，其成績計算方式依演練評分辦法(請參見附件)；演練總成績前 3 名者列為表現績優單位(若有同分情形，採併列方式)。

(二)本次演練結果表現績優及良好單位，由教育部建議單位給予人員行政獎勵。

二、 待加強單位部分

(一)對於演練結果待加強之單位，請單位落實各項改善措施，以強化資安防禦能量。

(二)針對資安攻防演練所發現之弱點，經警訊通知未確實改善者，將由教育部協請各該學校單位資通安全長持續督導改善，無正當理由而不作為者，請演練單位進行檢討。

(三)前揭單位將優先納入明年稽核受稽單位。

壹拾壹、 附件

一、 資安攻防演練評量辦法

為了解演練單位資安攻防演練期間之表現，規劃訂定演練單位防護成熟度評量規則，針對各演練單位執行「系統盤點能力」、「通報應變作業」、「防護能力」及「弱點複測」等 4 項工作類別表現進行評量，各評量類別、項目及占比如表 1。

▪表 1、演練單位評量配置

總計	類別	評量項目	評量占比
防護成熟度(100)	系統盤點能力(20)	調查表正確度	15
		調查表回復時間	5
	通報應變作業(20)	通報登錄時間	10
		應變處置時間	10
	防護能力(50)	重大衝擊性弱點數	20
		高衝擊性弱點數	15
		中衝擊性弱點數	10
		低衝擊性弱點數	5
	弱點複測(10)	複測通過率	10

評量配置詳細說明如下：

(一)系統盤點能力(20%)

為檢視單位於對外服務系統與連網裝置之掌握程度，將根據調查表填覆情形，依「調查表正確度」與「調查表回復時間」等 2 項進行評分。

得分 = 調查表正確度分數 + 調查表回復時間分數

1. 調查表正確度(15%)

- 調查表正確度分數 = (填報系統筆數 − 系統錯誤筆數)/(填報系統筆數 + 系統遺漏筆數) * 15 – (系統遺漏筆數*0.5)
- 系統遺漏筆數採單筆扣分制，最多扣至調查表正確度得分為 0。
- 系統錯誤筆數指為針對演練單位填覆資料無法正常連線網站服務頁面，如以下情形：
  - 服務協定錯誤，如瀏覽器預設採用 HTTP 協定，惟系統限制僅能使用 HTTPS 協定連線。
  - 雖可連線但為預設頁面，如顯示為 IIS 或 Tomcat 等。
  - 錯誤頁面，無法瀏覽第一個可公開存取之網頁頁面。
  - 連線服務埠填寫錯誤，如填覆 Port:8080 開啟，實則 Port:8080 關閉，但有開啟 Port:8888，且可正常連線至 Port:8888。

2. 調查表回復時間(5%)

- 依單位回復最後一次上傳至演練平台本計畫團隊日期為準，單位更新調查表則將採計最後一次寄送時間為準。

▪表 2、調查表回復時間評量標準

調查表回復時間	得分(5)
期限內回復(截止日 24 時前)	5
超過 1 至 2 個工作日	4
超過 3 至 5 個工作日	3
超過 5 至 7 個工作日	2
超過 7 至 10 個工作日	-2

超過 10 個工作日以上	-5

(二)通報應變能力(20%)

為檢視演練單位因應實際事件執行通報應變程序與處理表現，將依「通報登錄時間」及「應變處置時間」等 2 項進行評分。

得分 = 通報登錄時間分數 + 應變處置時間分數

1. 通報登錄時間(10%)

因警訊已由教育體系資安檢測技術服務中心採電子郵件與簡訊等以即時方式通知資安窗口，於本演練視為知悉，將檢視演練單位知悉資通安全事件後是否依熟練完成通報應變程序。

通報登錄時間(X) ※應於知悉後 1 小時內完成	分數 (10)
準時通報(0 < X ≤ 1 小時)	10
1 小時 < X ≤ 3 小時	7
3 小時 < X ≤ 6 小時	5
6 小時 < X ≤ 10 小時	4
15 小時 < X ≤ 20 小時	2
20 小時 < X ≤ 24 小時	1
24 小時< X	-3

由演練單位至演練平台登錄評估等級，以資通安全事件通報及應變辦法作為參考，相關資安事件等級評估如下表：

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)						

2. 應變處置時間(10%)

(1) 檢視演練單位是否依資通安全事件通報及應變辦法規定時限內完成警訊之應變處置。

(2) 得分 = 依演練單位事件應變處置時間落於表 3 區間。

(3) 視演練單位是否依事件等級對應之時限內至演練平台填報警訊之應變處置。若該等級有多筆事件，則採單筆處置最長事件應變處置時間計算，評量標準如表 3。

▪表 3、事件應變處置評量標準

1、2 級事件應變處置時間(X) ※應於知悉後 72 小時內完成	3、4 級事件應變處置時間(X) ※應於知悉後 36 小時內完成	分數 (10)
0 < X ≤ 72 小時	0 < X ≤ 36 小時	10
72 小時 < X ≤78 小時	36 小時 < X ≤39 小時	7
78 小時 < X ≤84 小時	39 小時 < X ≤42 小時	6
84 小時 < X ≤90 小時	42 小時 < X ≤45 小時	5
90 小時 < X ≤96 小時	45 小時 < X ≤48 小時	3
96 小時 < X ≤102 小時	48 小時 < X ≤51 小時	-3
102 小時 < X	51 小時 < X	-5

(三)防護能力(50%)

為檢視演練機關對外服務系統之防護網路攻擊能力，依「重大衝擊性弱點比例」、「高衝擊性弱點比例」、「中衝擊性弱點比例」及「低衝擊性弱點比例」等 5 項進行評分，各弱點比例採小數點後兩位四捨五入。

得分 =(重大衝擊性弱點比例得分*20)+(高衝擊性弱點比例得分*15)+(中衝擊性弱點比例得分*10)+(低衝擊性弱點比例得分*5)

■ 等級衝擊性弱點得分 =

(1 –(重大衝擊性弱點數量 / 系統弱點總數))* 20 +

(1 –(高衝擊性弱點數量 / 系統弱點總數))* 15 +

(1 –(中衝擊性弱點數量 / 系統弱點總數))* 10 +

(1 –(低衝擊性弱點數量 / 系統弱點總數))* 5

■ 弱點衝擊性等級主要參考表 4，輔以 CVSS 得分如表 6，以作為之級距判定，相關範例如表 5。

▪表 4、衝擊性列表

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性	資訊類風險
SQL 權限	透過資料庫語法取得資料庫(明文/密文)帳密或資通系統明文帳密	透過資料庫語法取得資料庫機敏資料或資通系統密文帳密	透過資料庫語法取得資料庫欄位資料(不含機敏/帳密)	透過資料庫語法或錯誤訊息取得資料庫欄位名稱	透過資料庫語法僅取得錯誤或基本訊息
AP 讀寫權限	具有可寫入 OS 特權路徑之權限	具有可寫入 Web 目錄、非 OS 特權路徑或讀取 OS 特權路徑檔案之權限	具有可讀取 Web 跨目錄或非 OS 特權路徑檔案之權限	僅可讀取當前 Web 目錄檔案之權限	-
惡意語法與提權	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者並可擴散至其他系統	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者	成功寫入攻擊語法或竄改頁面，但受影響之頁面限定已登入之任一使用者	• 成功寫入攻擊語法或竄改頁面，但受影響之頁面限定該登入使用者 • 攻擊語法須透過其他途	寫入攻擊語法取得錯誤或基本訊息

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性	資訊類風險
				徑誘使其他使用者觸發	
帳號權限	●取得 OS 管理者權限或足以證明權限等同 system、root 或 sysadmin 之帳號 ●取得資通系統防護需求為高等級之管理者(或帳號控管)權限或 OS 一般使用者權限	取得資通系統防護需求為中或普等級之管理者(或帳號控管)權限或 OS 一般使用者權限	取得資通系統(分級不限)業務單位使用者權限但不具帳號控管功能	取得資通系統(分級不限)一般使用者權限	-
資料外洩與存取控管	●取得特種個資(病歷、醫療、基因、性生活、健康檢查及犯罪前科) ●取得國家機密文書(未達解密條件者)	●取得一般個資且重複攻擊成效具有可預期性 ●取得一般公務機密文書(未達解密條件者)	取得部分一般個資且重複攻擊成效具有不可預期性	取得非機敏但非公開資料	取得非機敏但不可進一步利用之資料

表 5、衝擊性範例

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性	資訊類風險
SQL 權限	透過資料庫語法取得資料庫使用者密碼。	透過資料庫語法取得一般個資(不限筆數)。	透過資料庫語法取得資料庫欄位內容，但無個資。	透過資料庫語法或錯誤訊息取得資料庫欄位名稱。	透過資料庫語法僅取得錯誤或基本訊息
AP 讀寫權限	在 /root/ 或 C:\Windows\system32 寫入檔案。	●寫入任意檔案在 Web 目錄或/tmp/。 ●透過攻擊語法遠端讀取 shadow 或 win.ini。	●跨網站目錄讀取網頁原始碼。 ●透過攻擊語法遠端讀取 passwd。	僅可讀取當前目錄網站原始碼。	-

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性	資訊類風險
惡意語法與提權	儲存型跨網站腳本攻擊(SXSS)或竄改之頁面內容，且任何人(無需登入)皆可觸發語法或瀏覽竄改內容，並有其他系統同步進而造成影響擴散。	儲存型跨網站腳本攻擊(SXSS)或竄改之頁面內容，且任何人(無需登入)皆可觸發語法或瀏覽竄改內容。	儲存型跨網站腳本攻擊(SXSS)或竄改之頁面內容，任一登入使用者皆可觸發語法或瀏覽竄改內容。	●儲存型跨網站腳本(SXSS)攻擊弱點，惟僅影響該登入使用者。 ●反射型跨網站腳本(RXSS)攻擊弱點	寫入攻擊語法取得錯誤或基本訊息
帳號權限	●取得 root、Nt Authority\System、Domain Admins、Local Administrators、sa 帳號。 ●資通系統管理者(資通系統防護需求等級為高)。	●取得 domain users、local users 帳號。 ●資通系統管理者(資通系統防護需求等級為中/普)。	資通系統業務管理同仁權限(具部分網站管理功能)。	資通系統一般使用者權限。	-
資料外洩與存取控管	取得可識別之個資，且內容包含病歷、醫療、基因、性生活、健康檢查及犯罪前科。	檔案上傳後系統自動重新命名，且以上傳時間或順序作為檔名，透過列舉檔案名稱即可取得他人個資。	●透過竄改 Cookie 值取得他人個資，但 Cookie 值同帳號且帳號不具有規律性。 ●透過 Google Hacking 所取得之機敏文件。	取得機關內部未公開文件。	取得非機敏但不可進一步利用之資料。

▪ 表 6、CVSS 衝擊性弱點

衝擊性弱點	CVSS 3.1
重大衝擊性弱點	9.0 - 10.0
高衝擊性弱點	7.0 - 8.9
中衝擊性弱點	4.0 - 6.9
低衝擊性弱點	0.1 - 3.9

(四)弱點複測(10%)

1. 複測通過標準

- 網站可連線，弱點已確實修復。
- 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。

2. 複測未通過

- 為檢視演練單位修復重大、高及中衝擊性弱點能力，複測未通過表示該系統可連線且原弱點仍存在或複測過程中任一利用原弱點新增之測試帳號、測試程式或攻擊生效之測試語法等仍存在。
- 演練團隊確認弱點複測未通過時，將依原弱點攻擊紀錄衝擊性，重新發布新警訊，列入防護能力成績計算，並於次雙週進行複測。

3. 評量分數

- 複測僅針對演練單位之重大、高及低衝擊性弱點進行複測。若演練單位無重大、高及中衝擊性弱點，則本項弱點複測得分為 10 分。

得分 = 複測通過率 * 10

- 弱點總數 = 重大衝擊性弱點總數+高衝擊性弱點總數+中衝擊性弱點總數
- 複測通過率 =(弱點複測通過數 / 弱點總數)