113年教育體系資安攻防演練成果報告暨114演練計畫時程報告

網路系統組
邱惠隆

背景

- 教育部於113年底對**全國國立47所大專院校網頁、2所私立大專院校**進行資安攻防演練，以了解演練機關的**資安防護**與**應變處理能力**。
  - 演練實施時間:
    - **113年7月~9月之工作日。**
    - **每二週針對已發佈通報之網站進行複測**

113年教育體系資安攻防演練成果

- 此次本次繳交本校網站清冊共557筆
  - 共計發現**30筆網站漏洞(含複測不通過新增的1筆)**。
  - 其中**2筆**不是已繳交清冊的網站。

中大漏洞統計

弱點名稱	衝擊性	弱點數量	百分比	小計
SQL Injection	重大	2	6.66%	4
	中	2	6.66%	
權限控制失效	重大	1	3.33%	9
	低	3	9.99%	
	資訊	5	16.65%	
危險或過舊的元件	重大	2	6.66%	3
	高	1	3.33%	
XSS	高	1	3.33%	7
	低	5	16.65%	
	資訊	1	3.33%	
弱密碼	高	3	9.99%	5
	低	1	3.33%	
	資訊	1	3.33%	
安全設定缺陷	資訊	2	6.66%	2
合計			100%	30

SQL injection案例(資料庫資料)

```
Parameter: cid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cid=62' AND 8236=8236 AND 'FBTZ'='FBTZ

    Type: stacked queries
    Title: MySQL ⩾ 5.0.12 stacked queries (comment)
    Payload: cid=62';SELECT SLEEP(5)#

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: cid=62' AND (SELECT 4393 FROM (SELECT(SLEEP(5)))UHXu) AND 'xJkU'='xJkU

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: cid=-9586' UNION ALL SELECT NULL,CONCAT(0×71706b7171,0×6e56426264597a5773504d726
7871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[13:24:44] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 10 or 11 or 2016 or 2019 or 2022
web application technology: Microsoft IIS 10.0, ASP.NET 4.0.30319, ASP.NET
back-end DBMS: MySQL ⩾ 5.0.12
[13:24:51] [INFO] fetching current database
current database: 'a[redacted]nt'
[13:24:52] [INFO] fetched data logged to text files under '/home/code/.local/share/sqlmap/out
```

SQL injection防護措施參考

- **Defense in Depth (縱深防禦)**
  - 輸入淨化 (input sanitization)
  - 輸入驗證 (input validation)
  - 參數化查詢 (prepared statement)
  - 最小權限原則 (Principle of Least Privilege)
  - 使用 WAF (Web Application Firewall) 防護
  - 安全程式設計及開發 (SSDLC)

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。

XSS防護參考

Output Encoding (輸出前先做編碼)

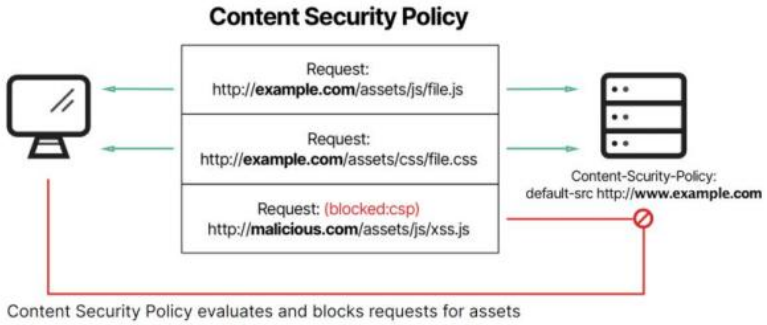
Character	Entity Encoding
"	&quot;
&	&amp;
'	&apos;
<	&lt;
>	&gt;

```
<div class="comment">
<script>alert("XSS")</script>
</div>
```

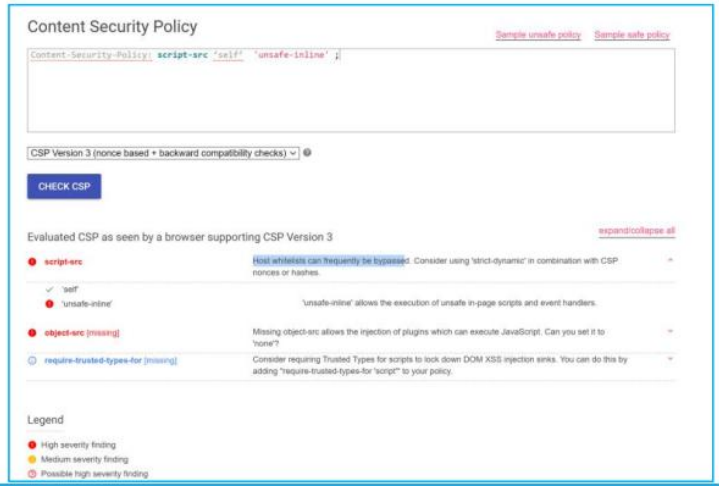
```
<div class="comment">
&lt;script&gt;alert(&quot;XSS&quot;)&lt;/script&gt;
</div>
```

XSS防護參考

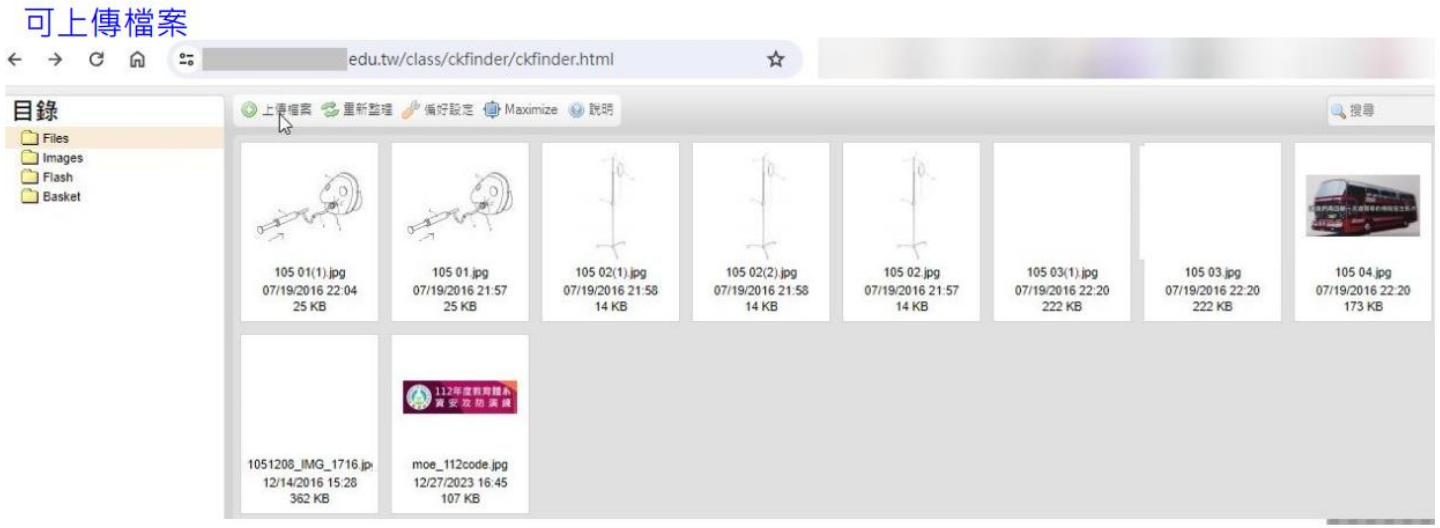
- **Cookie設定HttpOnly屬性**
  - 無法以JavaScript讀取Cookie值
- **設定Content Security Policy**
  - https://content-security-policy.com/



- **CSP 設定不正確，存在可能被繞過風險**
- **https://csp-evaluator.withgoogle.com/**



通過CKFinder漏洞獲取敏感信息



建議:

- **系統開發者**
  - 針對網頁套件之預設路徑進行更改，避免攻擊者可輕易猜測路徑進行存取。
- **系統管理者**
  - 應限制功能頁面之存取來源，若為外部使用者不需使用之功能，應禁止由外部存取該頁面。
  - 應避免直接由外網存取系統管理介面，應統一透過內網或透過VPN連線後，進行系統管理介面操作。

其他相關改善方法

建議:

- **檢視已存在弱密碼問題之系統帳號並定期變更機制**
  - 系統管理權限之帳號須立即變更密碼，且強度至少8碼以上，須符合大小寫英文、數字與符號，四種達成3種以上之高強度密碼。
  - 從系統面重新設計，每180天要求使用者變更密碼，於30至5天前發送系統信件通知且不得符合前3次密碼內容。
- **檢視已存在注入攻擊的程式**
  - 採用參數化（Parameterized）查詢語法並且加強對用戶輸入資料的檢核與驗證；使用最小權限原則 (Principle of Least Privilege)存取資料庫。
- **檢視已存在XSS的程式並使用工具加強檢查注入及XSS等漏洞**
  - 採取輸出前先做編碼，Cookie設定HttpOnly屬性及設定Content Security Policy原則
  - 使用專業的程式碼弱點掃描工具來尋找應用系統所隱含的漏洞，重要系統使用 WAF (Web Application Firewall) 防護。。

其他相關改善方法(續)

建議:

- **伺服端請求偽造點、權限控制失效及安全設定缺陷排除**
  - 檢查系統，移除敏感個資或惡意程式並設定資料夾瀏覽權限及存取來源，關閉不需要的檔案(如phpinfo)與顯示模式，減少資訊暴露的風險。
- **採用SSDLC開發系統**
  - 使用安全的軟體發展生命週期開發系統。
- **進行系統清點**
  - 針對不需要存在的網站及系統，建議將其關閉下線。
- **進行教育訓練**
  - 針對管理及開發人員進行網站建置的安全觀念宣導，隨時進行資安防護，定期更新系統及相關套件。

資安攻防演練分數

❑113年資安攻防演練中大的分數如下:

類別	項目	結果	分數
系統盤點能力(20%)	調查表正確率	557/(557+2)*15-(2*0.5)	13.95
	調查表回復時間	提早 7 時 23 分	5
通報應變作業(20%)	通報登錄時間	300/30	10
	應變處置時間	300/30	10
防護能力(50%)	重大衝擊性弱點比例	[1 - (5 / 559)] * 20	19.82
	高衝擊性弱點比例	[1 - (5 / 559)] * 15	14.87
	中衝擊性弱點比例	[1 - (2 / 559)] * 10	9.96
	低衝擊性弱點比例	[1 - (9/ 559)] * 5	4.92
弱點複測(10%)	複測通過率	(4+5+2)/(5+5+2)*10	9.17
		總計	97.69

114年資安攻防演練時程

114年資安攻防演練:

- **今年(114)7月1日~9月26日施實，敬請各單位提早準備。**

範圍標的

- 實施範圍主要為：**系統、網站、主機**。
  - 使用**演練單位**之**學校校名、網域名稱（DN）**或**網路位址（IP）**，並可透過**外部 Internet 連線**之服務。

114年資安攻防演練時程(續)

- 本校繳交的網站清冊將以資訊資產管理與盤點中的資通系統為主。
  - 請各單位網站負責人務必在資訊資產管理與盤點時新增資產.(5/5~6/13止)
  - 範圍:單位內所有供”網路可存取連線”之大大小小的網站
  - 若是有鎖”只有校內IP”才可存取的網站也請在用途說明欄中填寫(如能用140.115.~存取或172.~開頭的網站)

  - 資產大類-軟體類
  - 資產小類-應用系統軟體

- 如是使用google 協作平台建置之網站，請在”用途欄”輸入”網址”並備註是”使用google site建置”

  - 資產大類-軟體類
  - 資產小類-套裝軟體

114年資安攻防演練時程(續)

- 繳交的網站清冊若於演練期間抽測時連線不到亦可能會被扣分。
- 資安攻防演練結果將會提報至教育部。
  - 每兩年的教育部資安稽核(技術及實地稽核)可能會參考每年的演練結果進行後續抽測。
    - 即使演練結束未確定弱點是否已修復的網站或網頁請勿再上架，
  - 資安專章核定經費亦會參考此報告。

114年資安攻防演練時程(續)

❑ 演練方式：

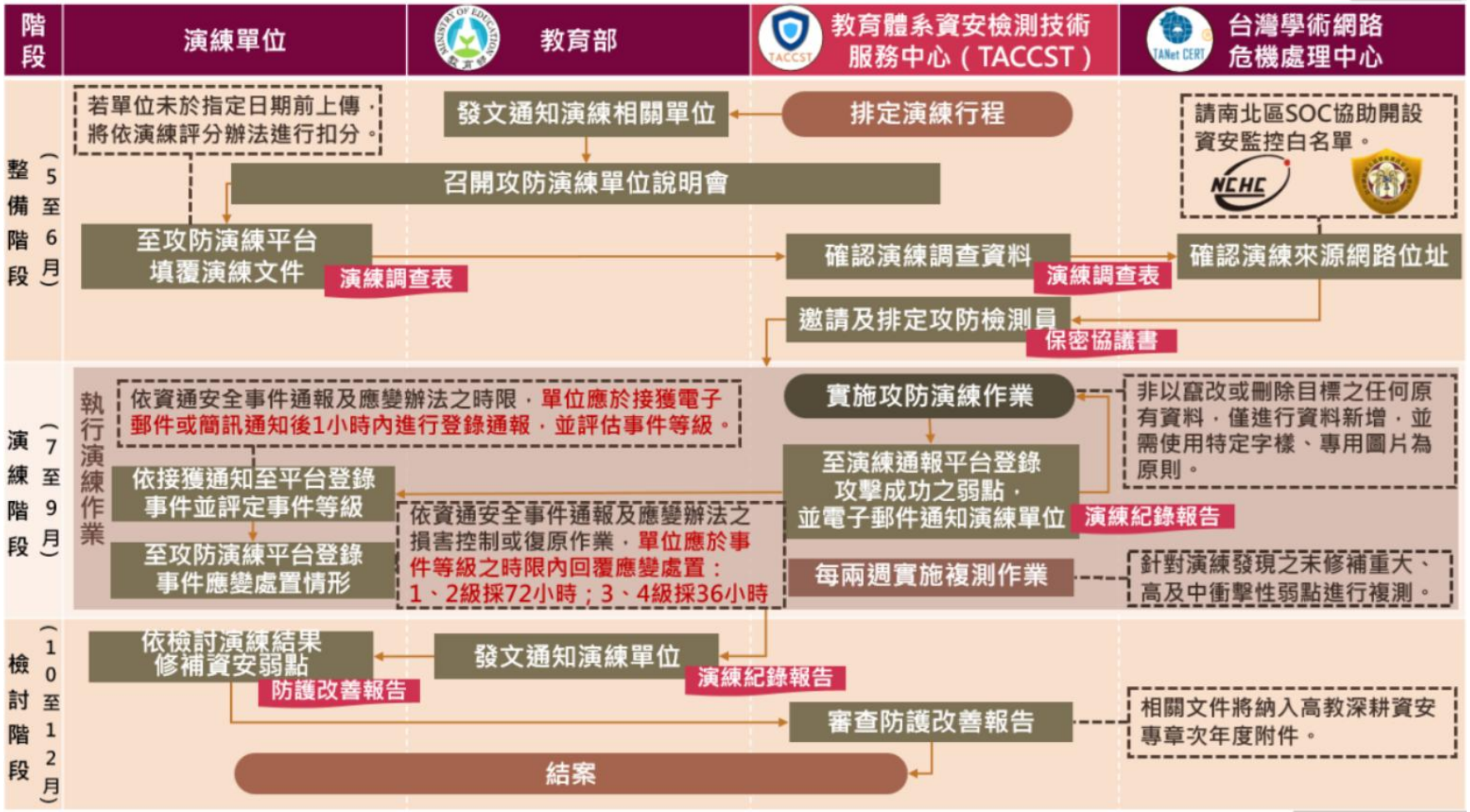
- 教育體系資安檢測技術服務中心（ TACCST）以**白帽駭客身份於外部於網路遠端檢測演練單位之資訊服務**，找出服務存在之弱點，並**通知演練單位於時限內完成資安事件通報、應變、修補程序**。

❑ 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**。

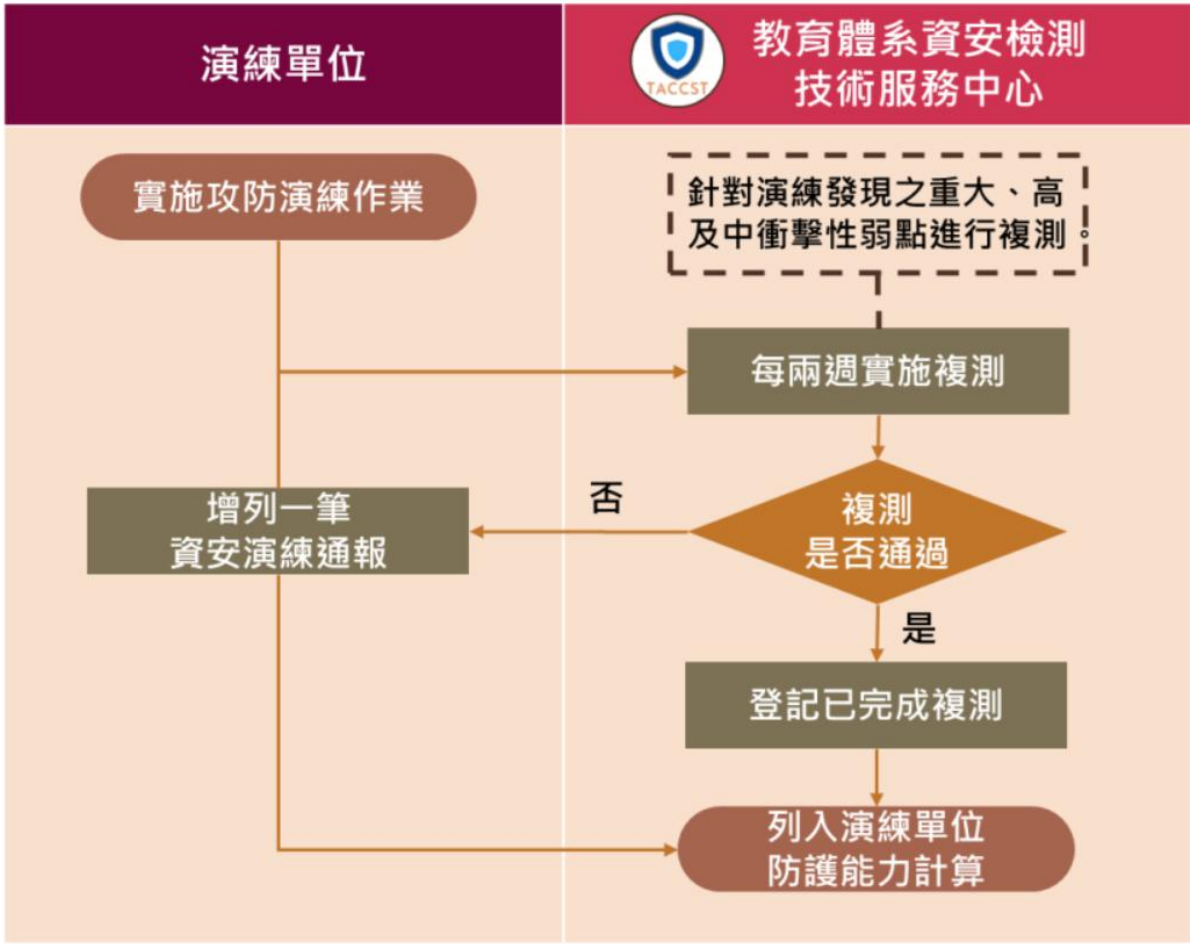
114年資安攻防演練時程(續)

整體流程



114年資安攻防演練時程(續)

複測流程



114年資安攻防演練時程(續)

❑ 注意事項－基本防護作業

演練實施前

- ➢ 請演練單位自行查檢項目：
  - **重新檢視防火牆相關設定是否合宜。**
  - **檢視測試網站與帳號等已確實關閉或移除。**
  - **確認內部使用網站未暴露於外部網際網路。**
  - **過時效性的功能網站請下線或設定於校內IP存取。(如研討會、活動網站)**
  - **主機等相關套件是否已完成更新-若套件已無法更新請做相對應的處理(如設定防火牆阻擋外部連線ssh等)。**
  - **建議網站後台限制管理者的IP存取。**

114年資安攻防演練時程(續)

❑ 注意事項－基本防護作業(續)

演練實施中

- 演練過程不會刻意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， 建議演練單位於演練期間**每日備份重要資料**等防護措施。
- 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**，並維持網站日常連線狀態及日常防護作業，勿刻意阻撓資安攻防演練。

114年資安攻防演練時程(續)

演練單位防護成熟度－衝擊性列表

	嚴重衝擊性弱點	高衝擊性弱點	中衝擊性弱點	低衝擊性弱點	資訊類風險
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

114年資安攻防演練時程(續)

衝擊性判斷基準

- 弱點衝擊性等級主要以衝擊性列表作為判斷標準， 並輔以CVSS分數作為判定參考

演練單位防護成熟度－衝擊性列表

	嚴重衝擊性弱點	高衝擊性弱點	中衝擊性弱點	低衝擊性弱點	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徑誘使其他使用者觸發	寫入攻擊語法取得錯誤或基本訊息

114年資安攻防演練時程(續)

電算中心收到事件通知後會先判斷事件等級，再依相關資訊通知事件單位。

單位回覆時程，自收到電算中心寄的通知信後:

- 一、二級事件請在48小時內回覆電算中心
- 三、四級事件請在24小時內回覆電算中心
  - 請回覆該事件處理情況、若是在以上回覆時間前無法修復，可來信請電算中心先將該網站IP擋住校外連線，待修復後再通知電算中心將其恢復對外連線。
- 電算中心收到回覆後會先確認完成修復後再回報技服檢測中心，若在時間內未回覆者，我們將先行阻擋對外連線服務，待回覆後再解除。
- 收信人員:單位SNMG成員、資通系統的管理者及使用者、單位一級資安執行及稽核小組成員、單位一、二級主管。

114年資安攻防演練時程(續)

檢視演練單位修復重大、高及中衝擊性弱點能力

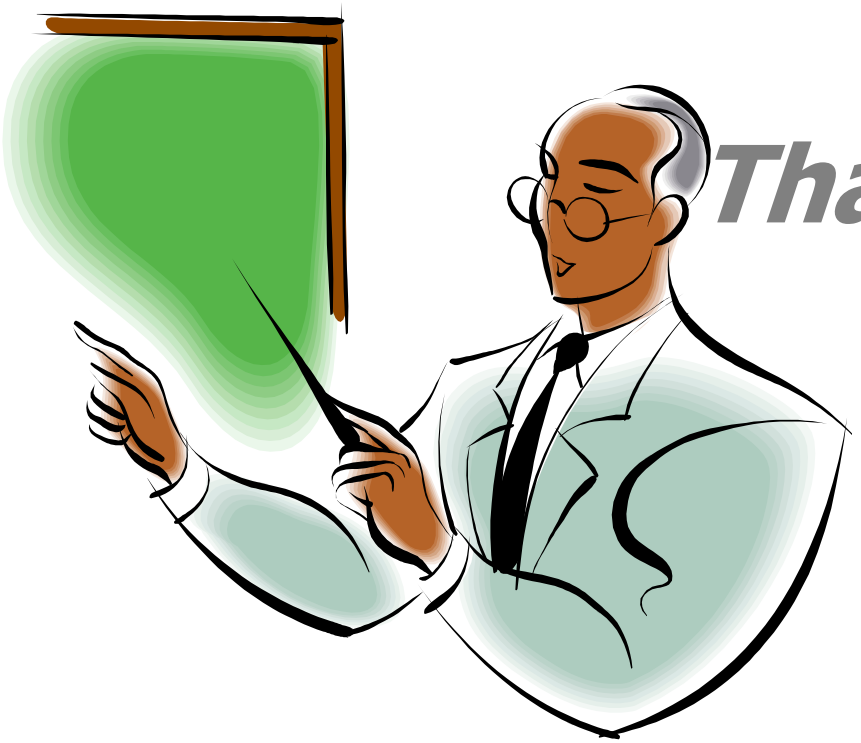
- **複測未通過**表示該系統可連線且原弱點仍存在或任一攻擊組利用原弱點新增之測試帳號、測試程式或攻擊生效之測試語法等仍存在。

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。

備註:在演練期間，因無法確保弱點是否真的修復完成，請通知我們在複測前先行阻擋對校外連線，待複測並確認修復完後才會解除。

感謝演練期間”SNMG成員”及”各單位網頁管理員”等相關人員的即時處理與回覆。



Thank You!