114 年度教育體系資安攻防演練之攻防檢測員招募簡章

一、 目的

因應當前資安情勢之嚴峻與挑戰，教育部規劃辦理資安攻防演練，針對教育體系對外網站系統進行滲透測試，以提升教育體系面對網路攻擊時之應處能力，強化資安事件發生時之緊急應變、系統復原及協調管控等能力。同時為提升演練成效及加強技術交流，培養國內資安人才實戰經驗，敬邀本國具有資安專業知能及實務經驗之教學研究界先進共同參與 114 年教育體系資安攻防演練(下稱本演練)。

二、 辦理單位

指導單位：教育部
主辦單位：教育體系資安檢測技術服務中心（國立陽明交通大學），以下簡稱本中心

三、 對象及資格

(一)招募對象：

為本國國籍且具相當資安專業知能之人員，以擔任資安攻防演練攻防檢測員。

(二)具備以下條件者可無須參與前置測驗：

1. CEH Practical/ECSA(CPENT)/OSCP/OSEP/OSWE 等資安相關滲透實務證照
2. 具備國內外資安相關競賽入圍初賽/複賽等具體實績
3. 為教育體系之副級(含)以上資安技術檢測員
4. 曾擔任行政院網路攻防演練攻擊手、教育體系資安攻防檢測員
5. 任職於國家安全局、國防部、法務部調查局、內政部警政署刑事警察局、及國家中山科學研究院等政府機關具備資安實務經驗人員

四、 遴選方式與期程

(一)報名（即日起至 114 年 5 月 27 日(週二)中午 12 時）

1. 由報名人員線上填列自身及推薦人基本資料於「114 年度資安攻防演練之攻防檢測員報名表」，本中心將依此報名資訊聯繫該人員，並副知其推薦人。
   ※報名連結：https://forms.gle/2WLkpL7eqh3LELja9
   (1) **演練日程**：114 年 6 月 30 日(週一)至 114 年 9 月 12 日(週五)之工作天，作業主要集中於週二至週四 9:00-16:00，須以單日場次進行勾選(可多選)，每人至少參與 4 場次，每場上限 20 人，結果通知將一併通知排定結果。
   (2) **實施據點**：台北(共 3 週)及新竹(共 7 週)，詳細實施地點請至報名表中查詢。
   (3) **參與報支**：
   - **交通費：**
     - ✧ **高鐵：**若為實體票證，請於實體票證上簽名，並以實體信件寄回。若為電子票證，請於電子票證上電子簽名，並以電子郵件回傳。※乘坐高鐵建議購買電子票證，報支較為便利。
     - ✧ **台鐵、客運：**以台鐵票價報支。
     - ✧ **計程車：**恕無法報支。
   - **住宿費：**機關所在地距離檢測單位距離超過六十公里，得以報支住宿費，以每日 2,500 元為補助上限，多於費用需自行吸收，需提供住宿收據，收據上日期需為入住當日日期(檢測第一天之日期)並輸入國立陽明交通大學之統一編號(87557573)，以上皆符合，則達到報支要點，

否則本中心有權不予報支。

※相關報支規定請詳閱 114 年教育體系資安攻防演練差旅建議。

2. 為增進攻防檢測員之技術交流，本次報名亦可填覆是否參與技術交流訓練活動。本活動日程為 114 年 6 月 18 日(週三)至 6 月 19 日(週四)，共 2 天，錄取上限 20 人，將依人員滲透實務經歷擇優錄取，最終錄取名單由教育部確認。

(二)前置測驗（114 年 5 月 28 日(週三)至 114 年 6 月 9 日(週一)中午 12 時）

1. 於報名截止後，本中心將以電子郵件寄發前置測驗相關資訊，若書審符合無須測驗資格之報名者將一併通知。
2. 實施前置測驗須請針對目標主機進行檢測，並撰寫攻擊報告，本中心將依據人員撰寫之報告數量與報告品質進行評選。
3. 最終將依據前置測驗結果呈請教育部確認參與名單。

(三)結果通知（114 年 6 月 11 日(週三)下午 4 時）

1. 於遴選完成後，將另行通知遴選結果，並針對通過遴選人員告知線上說明會相關資訊及演練日程排定結果。
2. 若填覆具參與技術交流訓練活動意願，將統一通知交流研討活動報名結果。

(四)說明會（114 年 6 月 16 日(週一)上午 10 時至中午 12 時）

1. 於通過遴選後，將於線上說明會告知攻防檢測員應遵守事項相關守則，須請務必全程參與，若無法參與該說明會將喪失參與資格。
2. 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. 攻擊機統一使用由本中心提供 Windows 與 Kali Linux 雙系統予每位攻防檢測員進行實施，但為安全起見，將限制攻防檢測員不得安裝來源不明之程式，但若為具有公信力之開發團體或一般釋出原始碼之 exploit code 則不在此限。此外，如有重大資安事件釋出之攻擊程式，經本中心確認後亦可做為本次演練使用。

(五)交流研討活動(114 年 6 月 18 日(週三)至 6 月 19 日(週四))

1. 課程日程：

日期	時間	地點
114 年 6 月 18 日(三)至 114 年 6 月 19 日(四)	9:00- 17:00	國立陽明交通大學 新竹光復校區 資訊技術服務中心 1 樓 訓練教室

2. 課程大綱

日程	項目
第一天(114 年 6 月 18 日)	網頁系統認證繞過手法、交流分享時間
第二天(114 年 6 月 19 日)	防護偵測繞過手法、交流分享時間

五、 弱點提繳獎金計算方式

1. 為鼓勵攻防檢測員提繳弱點及提供完整弱點紀錄報告，將依弱點衝擊性累積總積分之排名提供獎金，並於演練結束後依弱點發現紀錄結果提供參與證明書，攻防檢測員亦可申請由教育部採公文方式提供。
2. 攻防演練弱點衝擊性分成重大、高、中、低及資訊類風險 5 個等級，獎金計算原則及規則如下：

衝擊性弱點依累積分數排名		
衝擊性弱點	**積分**	**獎金（排名(人數)：元/名）**
重大衝擊性弱點	15	● 特優(3 名)：40,000 ● 優等(3 名)：20,000 ● 佳作(15 名)：8,000
高衝擊性弱點	8	
中衝擊性弱點	2	
低衝擊性弱點	1	

資訊類風險	0	
規則	※需完成弱點紀錄報告，並累計至少 5 積分即可列入排名。 ※若積分相等，以較高風險程度高者為優先。 ※若為常見或共通性框架或軟體之同一中低弱點，積分每人上限 30 分。 ※攻防檢測員不可繳交自單位之漏洞，如有繳交者，該漏洞發現不列入總分。	

3. 衝擊性判定高低以下表為主要準則：

	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
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	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	-

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性	資訊類風險
	或 OS 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

六、 聯絡窗口

教育體系資安檢測技術服務中心—資安攻防演練專案

- E-Mail：taccst.code@nycu.edu.tw
- ADDRESS：新竹市東區大學路 1001 號 國立陽明交通大學 教育體系資安檢測技術服務中心
- TEL：
  - (03)571-2121 #52885 王小姐
  - (03)571-2121 #52861 廖先生