國立臺中科技大學資安與個資抓漏活動

一、活動目的：

透過學生參與學校指定網站的資訊安全及個人資料保護之檢測，發現該網站資安防護與個人資料保護風險，提升學生對資訊安全及個人資料保護的重視及技術能力，同時協助學校網站進行資訊安全防護，預防潛在的漏洞帶來的資訊安全及個人資料保護風險。

二、參加資格：本校各學制在校生，每組報名人數 3 人以上，每人僅限參加一個組別，不得重覆報名。

三、活動日期：114 年 4 月 21 日(一)至 5 月 16 日(五)止。

四、檢測範圍：本校校外實習管理系統 https://cscin.nutc.edu.tw/。

五、參加方式：

於活動期間內發現檢測範圍網站之資訊安全或個人資料保護弱點後，將報名資料及通報規範填寫於活動表單 https://forms.gle/HekzSyDXDTRYat7J9

通報規範包含以下欄位：

(一) IP 位址：檢測時使用的 IP 位址。

(二) 檢測網址：檢測時完整的網址（含完整的 QueryString）。

(三) 漏洞說明：請以圖文詳細說明檢測漏洞的過程。

(四) 修補建議：修補漏洞建議的方法。

六、注意事項：

(一) 檢測範圍僅限於本校校外實習管理系統網站。

(二) 禁止下列行為：

1. 禁止對網站造成破壞性攻擊（如 DDoS、Fuzzing 及 High-Bandwidth 攻擊）。
2. 禁止未經允許存取或更改系統資料。
3. 禁止影響其他使用者正常操作或服務。
4. 禁止以實體存取本校設備。
5. 禁止以社交工程方式取得系統權限。

(三) 檢測範圍之外的網頁發現漏洞，將不列入評分範圍。

(四) 發現漏洞後，不得公開或私下分享。

(五) 檢測中發現之機密資料及個人資料不得公開揭露。

(六) 如遇緊急狀況，本校得終止活動，並公告於電算中心網頁，恕不各別通

知參加者。

七、本活動漏洞分級及獎勵金額說明：

漏洞分級	漏洞影響說明	獎金額度	範例
高	發現檢測範圍網站之漏洞，可由該漏洞進入本校內部網路或造成本校資訊安全嚴重程度實質影響之攻擊行為。	3,000 元	● 取得網站系統管理者權限 ● 取得機密檔案或個人資料 ● 取得內部主機完整權限 ● 其他嚴重等級攻擊
中	發現檢測範圍網站之漏洞，可由該漏洞影響該網站正常運作之攻擊行為。	2,000 元	● 遠端執行程式碼 ● SQL Injection ● Cross-site scripting ● 於網站上建立檔案 ● 篡改網站內容 ● 其他中等風險攻擊
低	發現本校檢測範圍網站任何符合OWASP Top 10之漏洞且並未對服務系統造成任何實質影響。	1,000 元	● 提升系統安全性設定 ● 作業系統漏洞 ● 程式邏輯漏洞 ● 其他漏洞

備註：

(一) 每組可以提交多筆漏洞，但僅有一次獲獎資格，不得重複領獎。於領獎時需核對身分證並填寫領據，方可領取獎金。

(二) 若主辦單位判斷提交漏洞如無資安或個資相關，將不給予獎金。

(三) 若相同漏洞由不同參加者提交，僅限最早提交者具獲獎資格，提報時間以活動表單填寫時間為準。

(四) 總獎金上限為 30,000 元禮券。如果符合漏洞提報者的總獎金超過此上限，將根據提報時間排序獲獎資格。若最後一組獎勵金不足以支付漏洞分級獎金時，主辦單位將按餘額分配。

(五) 主辦單位保有最終審核權利，若參加者不符合活動規定，或經第三人檢舉確實利用攻擊程式或其他違反活動公平性方式，意圖影響活動，主辦單位得立即取消其參加或獲獎資格，並要求賠償損失。若行為涉及違法，主辦單位保留法律追訴權利。

(六) 活動規則如有任何疑問，主辦單位保有最終變更活動細節（參加方式及贈品內容、數量等）之權利，參加者同意完全依照及遵守主辦單位之任何決定，絕無異議。活動如有未盡事宜，悉依主辦單位相關規定及解釋辦理，且不另行通知。

八、聯絡方式：

如有任何問題，請聯繫活動負責人
聯絡人：教學資訊組洪小姐
電子郵件：cc12@nutc.edu.tw
電話：04-22195523