教育部資訊安全人才培育計畫

臺灣好厲『駭』~資安實務導師(Mentor)培訓學員徵選須知

105 年 6 月 21 日教育部資安菁英人才計畫辦公室公告
105 年 7 月 7 日教育部資安菁英人才計畫辦公室修正
106 年 6 月 30 日教育部資訊安全人才培育計畫推動辦公室修正
106 年 8 月 8 日教育部資訊安全人才培育計畫推動辦公室公告
107 年 6 月 20 日教育部資訊安全人才培育計畫推動辦公室修正
107 年 6 月 25 日教育部資訊安全人才培育計畫推動辦公室公告
108 年 7 月 25 日教育部資訊安全人才培育計畫推動辦公室修正
108 年 7 月 30 日教育部資訊安全人才培育計畫推動辦公室公告

一、活動目的

為能培育符合產業需求資安人才，於學校教學理論基礎下，結合國內業界與學界師資，推動資安實務導師(Mentor)制度，以師徒制的方式傳授資安實務技術與資安競賽經驗，培育具資安技術實務能力的人才，快速融入職場環境與培養國際級資安競賽種子選手。

二、徵選方式與報名

1、由本計畫之資安實務導師擔任評選委員，進行兩階段評選：

(1) 第一階段初選（書面審查）：請有興趣參與本培訓活動的學生，提供基本資料表(如附件一)報名，由資安實務導師就其資通訊與資安等技術能力進行書面審查，評選出 30 位進行複選。

報名日期：即日起至 108 年 8 月 26 日(一)下午 5 點截止，請上網 https://tinyurl.com/y3zzlybh 填報並下載報名表，填寫完成後請將報名表 word 檔或 odt 檔上傳 https://tinyurl.com/y284hmt7 或 E-mail 至 samtn125@gmail.com，信件標題：第 4 屆臺灣好厲駭-報名表。

(2) 第二階段複選（口試審查）：將於 9 月 3 日(二)前公布初選通過名單(E-mail 通知)，並於 **9 月 7 日(六)**假國立臺灣科技大學(臺北市基隆路四段 43 號)舉行複選，將以口試的方式與資安實務導師親自面談，最終評選出 16 位學員進行導師培訓。(註：本計畫辦公室得視報名狀況調整初選與複選名額。)

2、以上各階段評選，均由評選委員依據申請學生之資通訊與資安等能力，以及學生欲受輔導之資安領域及目標等評選標準，評選成為培訓學員。

3、評分標準及權重

- 資通訊科技基本技能 40%
- 參加國內外資通訊或資安競賽經驗或獲獎紀錄 40%
- 自我期許 20%

4、評分結果分為兩種培訓模式：

- 通過第一階段初選者：可參加高階培訓模式，擇優者參與第二階段複選者。
- 通過第二階段複選者：可參加導師深度輔導模式及高階培訓模式，第二階段面試未通過者則可參與高階培訓模式。

三、參加資格

1、培訓期間需具備本國籍之國中生、高中職生、大專校院學生及研究生。

2、熟悉程式語言(C++、C、Java、C#、PHP、Python 等)、作業系統(如 Windows、Linux、iOS、Android 等)、作業系統實務(如 Windows、Linux、iOS、Android 等)、伺服器架設、資料庫、網路、資料結構與演算法、資訊安全等資通訊相關技術能力

3、熟悉資安實務技術或曾參加資通訊或資安競賽。

四、培訓時程、主題與訓練方式

1、培訓時程：本年度培訓時程為一年(108 年 9 月~109 年 8 月)

2、培訓主題：本年度培訓之資安實務領域，分為 2 大類主題：

(1) 高階資安實務培訓

- Penetration Test
- Malware Analysis
- Docker-Harden Security
- IOT Security
- Fuzzing
- SCADA Security
- Blockchain Security
- 其他(新趨勢議題)

(2) 高階 CTF 訓練課程

- Advanced binary exploitation
- Advanced Reverse Engineering
- Advanced Web Hacking and exploitation
- Memory Forensics, Network Forensics
- Android Security
- Crypto Analysis
- 其他(新趨勢議題)

上述主題本計畫得依照情況動態調整與增加項目。

3、培訓方式：

依照評分結果分為兩種培訓模式：

(1) 高階培訓模式

- 由計畫辦公室舉辦之系列強化培訓課程，由資深學員及導師進行不同主題的資安實務與 CTF 培訓。
- 部分高階培訓課程為有利於學習，需要學員完成基本測驗，測驗通過後始得參加培訓課程。
- 參與高階培訓模式學員其期末結業評審將由計畫辦公室彙整學員期末培訓報告提交導師會議決議。

(2) 導師深度輔導模式

- 除可參與高階培訓模式課程外，可參加導師深度輔導。
- 資安實務導師經由媒合機制選定欲培訓的學員，培訓學員依資安實務導師所訂立之培訓目標以師徒制方式進行培訓。
- 培訓的方式由資安實務導師及學員共同擬定研究主題，由學生**主動**進行研究並由導師輔導進度與技術，但各培訓導師可依培訓領域的特殊性、學生既有能力與興趣專長等實際狀況進行調整。
- 參與導師深度輔導模式學員其期末結業將由導師進行審查評分。

4、導師會議與**培訓**成果展示：

(1) 不定期召開資安實務導師會議，討論培訓成效及經驗分享。

(2) 學生培訓成果：將藉由參與國內外資安競賽或於國內外資安實務會議投稿或學員成果分享會、期末展示會、專題講座發表等方式，做為培訓成果考核之依據。

五、注意事項

1、 參與本計畫培訓之學員不需繳交培訓費用，本計畫酌予補助資安實務導師的輔導諮詢費用、實驗材料費以及參與本計畫所核定之重要活動報名費、交通費等，但培訓過程所需研讀的參考書籍或個人電腦設備等需由受訓學員自行負擔。

2、 培訓學員需遵循各培訓導師所制定之培訓制度接受培訓，若學員在培訓期間若學習效果不彰或主動退出本培訓計畫時，培訓導師可提送本計畫之資安實務導師會議進行審議，中斷培訓。

3、 培訓學員在培訓期間，需配合參加本計畫主辦或協辦之活動或競賽以及提供培訓成果之展示。

六、資安實務導師 **(依姓氏筆畫排列) (陸續邀請資安專家加入)**

學界及業界專家名單如附件。

七、其他

1、本計畫將不定期提供教育部補助出國參加或觀摩國際資安競賽的資訊，表現傑出的學員將優先考量補助。
2、本培訓學員徵選辦法未盡事宜，經本計畫相關會議決議後公告辦理。
3、108 年 8 月 30 日(五)假臺灣科技大學辦理第三屆臺灣好厲駭培訓成果發表暨產業鏈結交流會，對資安有興趣者歡迎出席與會，詳細活動議程將另行於網站(https://isip.moe.edu.tw)公告與通知。

附件一：

1、學界資安實務導師：

姓名	單位職稱
黃世昆	國立交通大學資工系 教授
查士朝	國立臺灣科技大學資訊管理系 副教授
曾　龍	崑山科技大學資訊工程系 副教授
黃俊穎	國立交通大學資工系 副教授
鄭欣明	國立臺灣科技大學資訊工程系 副教授
鄭振牟	國立臺灣大學電機工程學系 副教授
蕭旭君	國立臺灣大學資訊工程學系 助理教授

2、業界資安實務導師：

姓名	單位職稱
毛敬豪	財團法人資訊工業策進會資安科技研究所 經理
王凱慶	中華電信/中華資安國際 資安專員
吳明蔚(Benson Wu)	奧義智慧股份有限公司 創辦人
吳哲仰(Sean)	Team T5 Senior Researcher
李倫銓(Alan Lee)	聯發科經理/HITCON 臺灣駭客協會 總召集人
邱銘彰 (Birdman)	奧義智慧股份有限公司 創辦人兼執行長

徐千洋(Tim Hsu)	HITCON 臺灣駭客協會 理事長
翁浩正(Allen Own)	戴夫寇爾股份有限公司（Devcore） 執行長
陳仲寬	奧義智慧股份有限公司 Senior Security Researcher
蔡松廷(TT Tsai)	Team T5 創辦人
蔡政達(Orange)	戴夫寇爾股份有限公司（Devcore）顧問
楊安傑(Angelboy)	中央研究院資訊創新研究中心 資安專家
戴辰宇(GD)	Team T5 技術長
叢培侃(PK)	奧義智慧股份有限公司 創辦人
趨勢科技股份有限公司團隊	洪偉淦總經理、張裕敏協理、古炎秋經理等資安技術專家

附件二：

教育部資安人才培育計畫

第四屆資安實務導師(Mentor)培訓學員基本資料表

一、基本資料					
姓名		性別	□男 □女	出生年	民國　　年
就讀學校					
系所					
年級	□國中 □高中職 □大學 □碩士 _____年級				
聯絡電話	手機：　　市話：				
E-mail					

二、專長及能力 (熟悉資訊或資安技能或曾參加資安競賽等)

1、資通訊基本技能：

□程式語言(□C++、□C、□Java、□C#、□Python、□其他_____)

□作業系統(□Windows、□Linux、□iOS、□Android、其他_____)

□網站程式設計(□PHP、□JSP、□ASP.NET、□Ruby on rails、□Python Web、□其他_____)

□資料庫(□MySQL、□PostgreSQL、□MS SQL、□NoSQL、□其他_____)

□網路

□演算法

□資料結構

□資訊安全

□其他：_____

2、新型態資安攻防技術：

□ CTF Competition (資安搶旗競賽)

□ Reverse Engineering（逆向工程）

□ Pwnable analysis (弱點與漏洞分析)

□ Web 攻防技術

□ Crypto analysis(密碼學分析)

□ Misc (mobile, APT, CGC, AEG, ...)

□ 其它_____

3、參加資通訊或資安競賽經驗或獲獎紀錄(如 AIS3、MyFirstCTF、金盾獎或其他國內外 CTF 比賽等)

4、其他

(註：可提出參加競賽獲獎證明、學家專家推薦信、作品等佐證資料供評選委

員做為評分之參考。)

三、欲受輔導之資安實務技術(至多填 2 項)

☐Advanced exploitation

☐Reverse Engineering

☐Advanced Web Hacking

☐Memory Forensics

☐Android Security

☐Crypto Analysis

☐Penetration Test

☐Malware Analysis

☐Docker-Harden Security

☐IOT Security

☐Fuzzing

☐其他_____

四、參與本計畫之自我期許