教育部先進資通安全實務人才培育計畫

臺灣好厲駭 讓你更厲害

匯集國內業界與學界資安專家與參賽選手聯手打造

臺灣好厲駭

高階資安人才培訓平台

實務導向指導
專家師徒傳承

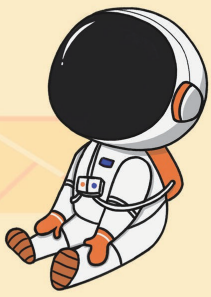
第六屆培訓學員徵選活動

◆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
.....

◆高階資安實務培訓

Penetration Test
Malware Analysis
Docker-Harden Security
IOT Security
Fuzzing
SCADA Security
Blockchain Security
.....



參加辦法與活動簡章：https://tinyurl.com/TWISIP

報名日期：即日起至110年8月16日中午12點止

聯絡窗口：崑山科技大學資訊工程系陳小姐

E-mail：happyhacking2017@gmail.com

FB粉絲頁：TAIWANHolyHigh

FB粉絲頁

活動簡章

計畫名稱：子3計畫：資安扎根與實務導師制度培育計畫

執行團隊：曾龍/崑山科技大學資工系副教授、陳麒元/國立宜 蘭大學資訊工程學系副教授、劉政鑫 /臺中工業高級中等學校資訊科科主任

教育部先進資通安全實務人才培育計畫

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
109 年 7 月 21 日教育部資訊安全人才培育計畫推動辦公室修正
109 年 7 月 22 日教育部資訊安全人才培育計畫推動辦公室公告
110 年 7 月 15 日教育部先進資通安全實務人才培育計畫推動辦公室修正
110 年 7 月 20 日教育部先進資通安全實務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，評選出數位進行複選。

報名日期：即日起至 110 年 8 月 16 日(一)中午 12 點截止，請上網填報並下載報名表 https://tinyurl.com/TWHH6，填寫完成後請將報名表 word 檔或 odt 檔上傳 https://tinyurl.com/TWHH6f 或 E-mail 至 samtn125@gmail.com，信件標題：第 6 屆臺灣好厲駭-報名表。

(2) 第二階段複選（口試審查）：將於 8 月 23 日(一)前公布初選通過名單(E-mail 通知)，並於 8 月 27 日(五)舉行複選，將以線上口試的方式與資安實務導師親自面談，最終評選出數位學員可進行導師媒合，合成功後進行導師培訓。(註：本計畫辦公室得視疫情狀況調整線上或實體

口試且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%
- 參加資安活動(含本計畫舉辦活動)之學習態度及積極度 20%
- 參加國內外資通訊或資安競賽經驗或獲獎紀錄 20%
- 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，擇優者可參與第二階段複選者。
- 通過第二階段複選者：第二階段面試通過者可媒合導師，媒合成功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與媒合未成功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(自 110 年 9 月 1 日至 111 年 8 月 31 日止)

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

- 通過第一階段初選者即可參與。
- 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

- 需通過第二階段面試且經導師媒合成功者。
- 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、**培訓**成果展示：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。

5、結業證書：所有學員於期末繳交自評報告書，由計畫辦公室彙整學員活動參與度、積極度及貢獻度提供給導師審查，審查通過者可取得結業證書。

五、注意事項

1、 參與本計畫培訓之學員毋需繳交培訓費用，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。

附件一：

1、學界資安實務導師：

姓名	單位職稱
查士朝	國立臺灣科技大學資訊管理系 教授兼系主任 兼資通安全研究與教學中心主任
黃世昆	國立交通大學資訊工程學系 教授
黃俊穎	國立交通大學資訊工程學系 教授
曾　龍	崑山科技大學資訊工程系 副教授
鄭欣明	國立臺灣科技大學資訊工程系 副教授
蕭旭君	國立臺灣大學資訊工程學系 副教授

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 資安鑄造廠總經理
王凱慶	中華資安國際股份有限公司資深工程師
吳 明 蔚 (Benson Wu)	奧義智慧股份有限公司 創辦人
吳哲仰(Sean)	TeamT5 杜浦數位安全有限公司 Senior Researcher
李倫銓(Alan Lee)	聯發科經理/ HITCON CTF 戰隊領隊與競賽負責人

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)	CYBAVO 博歐科技有限公司 技術長
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 Research Team 資深研究員
陳孝忠	資安技術顧問
曾智平(Kenny)	TeamT5 杜浦數位安全有限公司 Senior Researcher
蔡松廷(TT Tsai)	TeamT5 杜浦數位安全有限公司 創辦人兼執行長
蔡政達(Orange)	戴夫寇爾股份有限公司（DEVCORE）首席資安研究員
楊安傑(Angelboy)	戴夫寇爾股份有限公司（DEVCORE）資安研究員
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

第六屆資安實務導師(Mentor)培訓學員基本資料表

一、基本資料			
姓名		性別	□男 □女
就讀學校		系所	
身分別	□國中 □高中 □高職 □五專 □大學 □研究所		
年級	□一年級 □二年級 □三年級 □四年級 □五年級		
聯絡電話			
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)

(低：少有接觸。中：知曉基礎理論，有過實作經驗。高：實際操作熟練)

1、資通訊基本技能與理解程度：

作業系統

□Windows (理解程度：□低 □中 □高)

□Linux (理解程度：□低 □中 □高)

□iOS (理解程度：□低 □中 □高)

□Android (理解程度：□低 □中 □高)

□其他_____ (理解程度：□低　□中　□高)

程式語言

□C++ (理解程度：□低　□中　□高)

□C (理解程度：□低　□中　□高)

□Java (理解程度：□低　□中　□高)

□Python (理解程度：□低　□中　□高)

□其他_____ (理解程度：□低　□中　□高)

網站程式設計

□PHP (理解程度：□低　□中　□高)

□JSP (理解程度：□低　□中　□高)

□ASP.NET (理解程度：□低　□中　□高)

□Ruby on rails (理解程度：□低　□中　□高)

□Python Web (理解程度：□低　□中　□高)

□其他_____ (理解程度：□低　□中　□高)

資料庫

□MySQL (理解程度：□低　□中　□高)

□PostgreSQL (理解程度：□低　□中　□高)

□MS SQL (理解程度：□低　□中　□高)

□NoSQL (理解程度：□低　□中　□高)

□其他_____ (理解程度：□低　□中　□高)

2、CTF 搶旗大賽技術：

□ Reverse Engineering（逆向工程）(理解程度：□低　□中　□高)

□ Pwnable analysis (弱點與漏洞分析) (理解程度：□低　□中　□高)

□ Web 攻防技術 (理解程度：□低　□中　□高)

□ Crypto analysis(密碼學分析) (理解程度：□低　□中　□高)

□ Misc**(**PPC,Forensics…..) (理解程度：□低　□中　□高)

□其他_____ (理解程度：□低　□中　□高)

3、資安實務技術：

□滲透測試(Penetration test) (理解程度：□低　□中　□高)

□數位鑑識(Forensics) (理解程度：□低　□中　□高)

□惡意程式分析與威脅獵捕(Threat Hunting) (理解程度：□低　□中　□高)

□金融資安與區塊鏈安全　(理解程度：□低　□中　□高)

□IOT Security 與基礎關鍵設施場域實測　(理解程度：□低　□中　□高)

□雲端安全(Cloud Security) (理解程度：□低　□中　□高)

□人工智慧與資訊安全　(理解程度：□低　□中　□高)

□其它_____ (理解程度：□低　□中　□高)

三、積極學習之佐證

(請提出佐證資料，本計畫辦公室將以此作為重大評審資格)

1、參加資通訊競賽經驗或獲獎紀錄

□APCS (_____年度，成績：_____)

□其他：_____ (_____年度，成績：_____，隊名：_____)

2、參加資安競賽經驗或獲獎紀錄

□神盾獎　　(_____年度，成績：_____，隊名：_____)

□金盾獎　　(_____年度，成績：_____，隊名：_____)

□MyFirstCTF　(_____年度，成績：_____，隊名：_____)

□AIS3 EOF CTF (_____年度，成績：_____，隊名：_____)

□Balsn CTF　(_____年度，成績：_____，隊名：_____)

□Bamboofox CTF(_____年度，成績：_____，隊名：_____)

□Hitcon CTF　(_____年度，成績：_____，隊名：_____)

□國外 CTF 比賽(CTF 名稱：_____，_____年度，成績：_____，

隊名：_____)

□CTFtime LINK：_____

□其他：_____(CTF 名稱：_____，_____年度，成績：_____，

隊名：_____)

3、參加其他競賽經驗或獲獎紀錄

□其他：_____ (_____年度，成績：_____)

4、資安活動參與紀錄 HITCON Training

□HITCON Training (年度_____課程名稱_____) □AIS3(年度_____)

□校園資安深耕營 (日期_____課程名稱_____) □教育部人才培訓計畫資安暑訓營(年度_____)□其他(_____)

5、□學家或專家推薦信(第一位：_____，第二位：_____)

6、□作品或資安相關證照（_____）

7、□其他：_____

如表格不敷使用，請自行增加

四、自我期許

□能學以致用，發揮所長，精研更多項資安技術能力

□能參加資安競賽(含 CTF)取得好成績

□幫助升學　　□增加就業能力

□其他自我期許詳述_____

五、參與本計畫你想要學習哪些技術

1、CTF 搶旗大賽技術：

□ 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(PPC,Forensics…..) □其它_____
2、資安實務技術：
□滲透測試(Penetration Test) □惡意程式分析與威脅獵捕(Threat Hunting)
□IOT Security 與基礎關鍵設施場域實測 □雲端安全(Cloud Security)
□人工智慧與資訊安全 □Advanced Exploitation □Memory Forensics
□Penetration Test □Docker-Harden Security □Fuzzing
□其他_____
六、附件(可附上個人技能/學習成果等能證明自我能力之簡報)

註 1：個人資料使用同意書:

(1)本計畫蒐集之個人資料僅提供本計畫活動所用，並將遵從個人資料保護法，不得洩漏或供作其他用途。

(2)個人資料得依個人資料保護法第三條之規定，行使下列查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理或利用、請求刪除之權利。

(3)個人資料依個人資料保護法第三條之規定，請求停止蒐集、處理或利用或請求刪除前，本計畫得依循個人資料保護法及相關法令之規定，於個人資料提供之範圍與目的內使用該等個人資料。