

蘇學翔

✉ qazbnm456@gmail.com | 📄 qazbnm456 | 📠 syue-siang-su-a2a1098b

“Code is meant to be born to be pretty.”

Education

國立交通大學

資訊工程碩士

台灣新竹

2016/07 — 2018/06

國立中山大學

資訊工程學士

台灣高雄

2012/09 — 2016/01

- GPA: 3.81/4.3
- 榮譽：學業成績優異提早畢業
- 團隊合作：與同學合作改善知名弱點掃描器的效率及準確率

Work & Leader Experience

The Declaration of Hacker

網頁安全研究組組長

台灣台北

2018/06 — 現在

- 學習、瞭解並研究新的攻擊手法及 CVE
- 帶領並指導組員個人或團體研究項目細項

The Declaration of Hacker

後端工程師

台灣台北

2015/07 — 2018/05

- 以 Rails 開發 Wargame 平台，並使用當下流行的 Docker 做為 DevOps 的基礎架構及平台題目的容器
- 目前使用 Rancher 調度容器，並規劃進一步替換為 k8s

資安讀書會

發起人

台灣高雄

2015/07 — 2016/06

- 招募有興趣的學生及同學們每週分享資安相關議題
- 與在校教授合作並舉辦第一次的校內 CTF 競賽做為課堂加分項目
- 規劃校內演講及相關活動

國立中山大學

滲透測試人員

台灣高雄

2013/12 - 2015/01

- 針對校內服務做滲透測試並回報至相關窗口
- 與圖資處維護人員共同修補有問題的服務及隨時針對重大資安事件進行軟體普查

Extracurricular Activity

HITCON Winter Training 2017

ADVANCED WEB SECURITY & HANDS-ON WEB PENTEST 講師

台灣台北

2017/12/05 - 2017/12/06

- 教授進階網頁安全
- 給予學員實際的練手網頁並一步一步指導，而其漏洞涵蓋 OWASP TOP 10 2013 的所有弱點分類
- 分享近年新起的攻擊手法及實際案例

HITCON Winter Training 2017

BROWSER FRONT-END EXPLOITATION 講師

台灣台北

2017/12/04

- 教授關於瀏覽器前端安全的概念及常識
- 給予學員實際的練手項目以實際體驗瀏覽器前端威脅
- 探討各瀏覽器對於某些功能的實作差異及會對瀏覽器安全帶來的影響

行政院國家資通安全會報技術服務中心

台灣台北

WEB SECURITY FOUR-DAY WORKSHOP 講師

2017/09/22 - 2017/09/25

- 網頁安全，從基礎到深入
- 給予學員四天密集的題目訓練及課程

HITCON Training 2016

台灣台北

WEB SECURITY BASIC & ADVANCED 講師

2016/11/28 - 2016/11/30

- 教授網頁安全概念
- 從基礎概念到進階題目以增進學員獨立思考的能力

Bamboofox 戰隊

台灣新竹

成員

2016/06 - 現在

- 在資安領域中增加實力及經驗，特別是在網頁安全及弱點利用領域
- 參與多場 CTF 競賽，包括但不限於 DEFCON Quals, HITCON CTF, SECCON CTF 等
- 週期性地授課予新來的學弟妹們

台大黑客松

台灣台北

參賽者

2015/08

- 建立一個網頁使得使用者除了可以規劃路線以外，也可以透過我們整進來的 Hyperlapse.js 在這個路線上建立一系列連續街景圖，使得使用者有身歷其境的感受

Honors & Awards

國際

2017 決賽, SECCON CTF 2016 Final

日本東京

2016 決賽 & HITCON Taiwan Star 獎項, HITCON CTF 2016 Final

台灣台北

國內

2016 決賽 & 第三名, 金盾獎決賽

台灣台北

2015 決賽, 金盾獎決賽

台灣台北

2014 第四名, F-Secure 獵駭行動

台灣台北

Presentation

AVTokyo 2018

日本東京

<FAREWELL, WAF - EXPLOITING SQL INJECTION FROM MUTATION TO POLYMORPHISM> 講者

2018/11/03

- 介紹一種利用同質異構概念自動化產生攻擊語句的可行方法
- 展示利用上述方法可繞過現行 ModSecurity 最新版本 SQL 注入保護的攻擊語句

OSCON 2018

美國奧勒岡州波特蘭

<BEST PRACTICES FOR CROSS-PLATFORM DESKTOP APPS WITH VUE.JS AND ELECTRON> 講者

Jul. 18th 2018

- 使用 Vue.js 和 Electron 開發一款應用程式我認為是前端新手再好不過的選擇。這場演講旨在將最佳實踐透過實際實作一款小型的類瀏覽器應用程式體現，並希望激發聽眾對於 Vue.js 和 Electron 結合使用的興趣。

AVTokyo 2017

日本東京

<THE AMAZING TOOLMAN - MASTERING THE TOOLS AND PROPOSE A HACKABLE "SWISS ARMY KNIFE" SECURITY

2017/11/11

FRAMEWORK FOR THE 21ST CENTURY> 講者

- 網頁安全滲透測試領域中常用工具介紹
- 自行實作並提出一套萬用網頁滲透測試框架以應付各類情況，而其支援幾乎所有現在網頁瀏覽器能做的事，例如：擴充功能、網頁偵錯、桌面通知等

Modern Web 2017

台灣台北

<VUE.JS + ELECTRON, BUILD YOURSELF A BROWSER!> 講者

2017/08/10 - 2017/08/11

- 投影片前半段主要介紹什麼是 Vue.js 和 Electron，而後半則會利用這兩個工具兜出一個簡單的網頁瀏覽器雛形

SITCON 2016

台灣台北

<DOCKER-WAR : DOCKER BASED WARGAME PLATFORM> 講者

2016/02/27

- 介紹如何使用甫興起的 Docker 搭配 Rancher 開發一套專門練習資安題目的平台

Writing

Rails security

Wooyun drops

作者

2016/03

- 歸納近年發生的 Rails 相關安全議題

國立中山大學

台灣高雄

學士專題報告

2014/09 - 2015/11

- 探討如何改善網頁弱點掃描器的效率及準確度