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 — *台灣新竹*

資訊工程碩士 — *2016/07 —2018/06*

- 碩士論文：利用同質異構概念構造 SQL Injection 攻擊語句

國立中山大學 — *台灣高雄*

資訊工程學士 — *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

奧義智慧科技 — *台灣新北*

資深資安研究員 — *2020/04 - 現在*

- 研究新事物並發表資安研究
- 透過調查與分析情資，追蹤發動資安攻擊後面的族群
- 研究並重現新的資安繞過手法並提出相對應的偵測方式以加強我們的產品與服務

台灣積體電路製造股份有限公司 — *台灣新竹*

資訊技術安全處工程師 — *2019/01 - 2020/03*

- 針對資安事件做緊急應變處理 (CIRC)
- 研究最新發表的資安事件報告，且撰寫偵測或防禦規則並套用至對應的資安設備
- 在紅隊演練結束後，根據執行結果審閱資安事項

資通安全研究與教學中心 — *台灣新竹*

計劃助理 — *2018/09 - 2018/12*

- 對合作廠商進行滲透測試
- 研究並開發滲透測試工具

The Declaration of Hacker — *台灣台北*

後端工程師 — *2015/07 —2018/08*

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

資安讀書會 — *台灣高雄*

發起人 — *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 競賽做爲課堂加分項目
- 規劃校內演講及相關活動

Extracurricular Activity

CCoE Taipei 2022 — *台灣台北*

"Advanced Web security & Hands-on Web Pentest" 講師 — *2022/07/09 - 2022/07/10*

- 給予學員實際的練習網頁並一步步指導，而其漏洞涵蓋 OWASP TOP 10 2021 的所有弱點分類
- 分享近年新起的攻擊手法及實際案例

HITCON Training 2016 - 2020

台灣台北

"Making yourself a toolman" 及"Advanced Web security & Hands-on Web Pentest" 講師 — 2016 - 2020

- 帶領學員理解熱門網頁安全工具的內部實作以及進階程度的網頁應用程式安全
- 指導學生撰寫網頁資安工具，特別是弱點掃描類型的工具
- 給予學員實際的練習網頁並一步步指導，而其漏洞涵蓋 OWASP TOP 10 2017 的所有弱點分類
- 分享近年新起的攻擊手法及實際案例

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

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

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

2019	**第一名**, HITCON Defense	台灣台北
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

OWASP 2023 Global AppSec Dublin

愛爾蘭

<Constructing a Precise Dynamic Control-flow Graph for EVM based Smart Contracts> 講者 — 2023/02/16

- 簡述區塊鏈安全，尤其以去中心化應用程式與智慧合約相關的安全性議題爲主
- 透過利用全功能的、可用的以太坊虛擬機（EVM）實現，示範了如何透過一步步的引導與調整建構一個精準的控制流程圖（CFG），並利用它來逐步對基於 EVM 的智慧合約進行逆向工程

VXCON 2022

線上

<AD Attack Paths Demystification> 講者 — 2022/08/27

- 分享我們經手過的 AD 安全案例，並舉出常見的幾種問題與如何處理
- 與聽眾互動並分享我們如何透過機器學習的方式快速辨認可能的攻擊路徑並提供緩解措施

NCA Annual Conference 2021

日本

<The balance between Active Directory Operation & Security in enterprises> 講者 — 2021/12/18

- 談討企業常見的 AD 錯誤、駭客如何利用這些優勢偷走企業內部機密以及解除 AD 常見管理及設定迷思

CYBERSEC 2021

台灣台北

<Let Me Google It for You - Security Concerns in Decentralized Finance (DeFi)> 講者 — 2021/05/06

- 簡述區塊鏈安全及在區塊鏈產業未來中可能發生的資訊安全相關議題，並以近期發生的資安事件舉例
- 介紹相關工具及網頁，以鼓勵聽眾在參與相關活動時能夠有能力做基本的智慧合約審閱

H@ctivitycon, HITCON 2020, ROOTCON 14

美國、台灣及菲律賓

<Discover vulnerabilities with CodeQL> 講者 — 2020

- 介紹 CodeQL 的基本功能，並在會中介紹如何使用進階技巧，包括靜態及污點分析，實際找到常見網頁內容管理系統上的漏洞
- 簡介如何使用 CodeQL 在大型程式碼上，以保持程式碼的簡潔及安全性

AVTokyo 2018, OWASP Global AppSec - DC 2019, ROOTCON 13

日本、美國及菲律賓

<Farewell, WAF - Exploiting SQL Injection from Mutation to Polymorphism> 講者 *2018, 2019*

- 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 *2018/07/18*

- 使用 Vue.js 和 Electron 開發一款應用程式我認爲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 framework for the 21st century> 講者 *2017/11/11*

- 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