

# 蘇學翔

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

“Code is pure and neutral, but it reflects what a programmer is.”

## Education

### 國立交通大學

資訊工程碩士

- 碩士論文：利用同質異構概念構造 SQL Injection 攻擊語句

台灣新竹

2016/07 - 2018/06

### 國立中山大學

資訊工程學士

- 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

台灣高雄

2012/09 - 2016/01

## Work & Leader Experience

### 奧義智慧科技

資安研究經理

- 進行資安研究並在相關場合發表新發現
- 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
- 帶領團隊開發新工具，以提供在數位資產上挖掘漏洞、發現錯誤配置的新世代解決方案

台灣新北

2020/04 - 現在

### 台灣積體電路製造股份有限公司

資訊技術安全處工程師

- 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

台灣新竹

2019/01 - 2020/03

## Extracurricular Activity

### HITCON Training 2024

“網頁安全之從 WEB 2.0 跨到 WEB3” 講師

- 基礎及進階網頁安全授課
- 區塊鏈介紹及教導基礎 Web3 安全

台灣台北

2024/07/17 - 2024/07/19

### HITCON X NICS

“枕戈待旦，網站應用程式安全實戰” 講師

- 進階網頁安全授課

台灣台北

2023/10/21 - 2023/10/22

### HITCON X NICS

“養精蓄銳，網站應用程式安全比試” 講師

- 基礎網頁安全授課

台灣台北

2023/07/22

### CCoE Taipei 2022

“ADVANCED WEB SECURITY & HANDS-ON WEB PENTEST” 講師

- 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

台灣台北

2022/07/09 - 2022/07/10

## 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

### FIRST Cyber Threat Intelligence Conference 2024

柏林

<SOURCE POLLUTION ATTACK - A HIDDEN THREAT IN CYBERSECURITY> 講者

2023/04/17

- 在這場演講中討論了來源污染的風險。如果任何來源的內容容易被篡改，這將可能導致資訊混亂、不明確的下載，甚至災難性的安全事件，例如 DoS 攻擊（偽造 GeolIP）和任意程式碼執行等。

### 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為主
- 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