

# 曾緯淳 Mason Zeng

資安研究 · 生成式 AI 開發 · 紅隊自動化 · CTF 出題

臺北市，臺灣 | ohmygodmason@gmail.com | github.com/masonzeng702550 | masonzeng702550.github.io

## 摘要

高中資安研究者與生成式 AI 開發者，專注於 AI / LLM 安全、Web 安全、滲透測試與紅隊自動化。獨立完成多模型提示注入偵測研究（逾三萬次測試、論文正式發表），並開發多代理自動化攻防系統，於國內外 CTF 取得前段名次。三項中華民國新型專利發明人；教育部 AIS3 培訓學員；曾任行政院與教育部資安攻防演練攻擊手與檢測員。

## 技能

- 程式語言：Python、C++
- 資訊安全：Web 安全、密碼學、滲透測試、AI / LLM 安全、CTF
- AI / 開發：生成式 AI 應用、LLM 應用、多代理系統、網頁前端、硬體實作
- 其他：網路管理、專案管理、跨域整合、技術寫作與講授

## 經歷

- 資安攻防演練 攻擊手 / 檢測員 — 行政院國家資通安全研究院 · 教育部 2025
- 行政院國家資通安全網路攻防演練 攻擊手；教育體系資安攻防演練 檢測員
- CTF 出題者 — FHFCTF、THJCC CTF 2024, 2026
- 為兩場資安競賽設計 Web 與密碼學題目，涵蓋題目情境、部署與解題驗證
- 工讀生 — 新興科技教育遠距示範服務計畫 —

## 專題與專案

- 多模型協同偵測提示注入攻擊（研究論文） 2026
- 提出以三個異質商用 LLM 投票協同偵測的架構，補足單一模型易被繞過的盲點
- 長文本偵測率約 87%、短指令約 99.8%，全面超越任一單一模型；逾 30,000 次測試
- 獨立完成文獻探討、實驗設計、系統實作與數據分析；獲全國高中小論文競賽 資訊類 優等，並於研討會正式發表
- 自動化紅隊多代理攻防系統 2025–2026
- 主控代理調度、並行工作代理依題型分工、共享記憶與可自我演化規則
- 三層決策機制（安全底線 / 可調規則 / 模型推理）與內建授權倫理規範
- AIS3 Pre-Exam 個人第 14 名（3912 分）；UMDCTF 總排名第 72、學生組第 22
- 工業控制系統（ICS）資安靶場 — 教育部 AIS3 2025
- 以自製硬體打造低成本 ICS 實體靶場，解析 OT 通訊並設計由淺入深的攻防流程
- Trashform 影像辨識回收系統（PWA） —
- 拍照即辨識廢棄物，依各縣市規則提供拆解與分類指引；與環保組織 RETHINK 合作
- Aircraft Marshaller 停機線指揮員模擬器 —
- 瀏覽器端即時手勢辨識結合 3D 導引，作為航空地勤標準手勢教材（影像不上傳）

## 教育

- 臺北市數位實驗高級中學（T-School） 2023–2026（預計畢業）
- 新北市私立南山高級中學附設國中部

## 競賽榮譽

- 2025 IEYI 世界青少年發明展 臺灣選拔賽 金牌（臺灣代表隊） / 世界決賽 銀牌
- 全國高級中等學校小論文競賽 資訊類 優等（2026）

- 113 年度資安技能金盾獎 決賽 鋒芒畢露獎
- 2025 CDX 資安攻防推廣交流賽 第 5 名
- UMDCTF 國際賽 公開組 72 / 763、學生組 22 / 146
- 2025 MyFirstCTF 第 26 名；2024 CGGC 網路守護者挑戰賽 第 27 名

## 證照與培訓

---

- iPAS 經濟部 資訊安全工程師能力鑑定 中級
- 教育部先進資通安全實務人才培育計畫 AIS3、AIS3 Junior
- TAIWAN HolyHigh Training 第十屆 高階學員
- HackTheBox 完成 7+ Labs

## 演講

---

- 校內外資安課程講師：AI / LLM 攻防、密碼學、OSINT、Linux / Kali、網頁安全 / CTF 入門
- 聯發科 STEM 造課師研習 AI 工作坊 助教 / 分享
- 2026 COSCUP「Hackers In Taiwan」議程發表者

## 論文發表

---

- 曾緯淳，〈多模型協同偵測提示注入攻擊〉，2026 前瞻會計與財務專刊暨人工智慧與現代管理理論與實務研討會，正式發表。

## 專利（發明人）

---

- 中華民國新型 **M669931** — 基於生成式 AI 的智能網頁應用程式防火牆系統
- 中華民國新型 **M650895** — 智能化石辨識系統
- 中華民國新型 **M678878** — 智慧電梯運作系統

## 社團與幹部

---

- 數位實驗高中 資訊研究社 社長；航空研究社 副社長
- ISIP 跨校資安社團 零日餅乾社 課程組長；2026 寒訓「Bak3 C00kie」總召
- 國立臺灣科技大學 資訊安全研究社 社員
- 2025 HITCON Cyber Range 場務組；2026 SITCON 場務組