Mason Zeng 曾緯淳

Security Research · Generative AI Development · Red-Team Automation · CTF Author

Taipei, Taiwan | ohmygodmason@gmail.com | github.com/masonzeng702550 | masonzeng702550.github.io

SUMMARY

High-school security researcher and generative-AI developer focused on AI/LLM security, web security, penetration testing, and red-team automation. Independently completed a prompt-injection detection study (30,000+ trials, formally published) and built a multi-agent automated offense/defense system that placed in the upper tier of domestic and international CTFs. Inventor on three R.O.C. utility-model patents; trainee of the Ministry of Education AIS3 program; served as red-team operator and security assessor in national cyber offense/defense drills.

SKILLS

- **Languages:** Python, C++
- **Security:** Web security, cryptography, penetration testing, AI/LLM security, CTF
- **AI / Development:** Generative-AI applications, LLM applications, multi-agent systems, web front-end, hardware prototyping
- **Other:** Network administration, project management, cross-disciplinary integration, technical writing & teaching

EXPERIENCE

Red-Team Operator / Security Assessor — National Institute of Cyber Security & Ministry of Education **2025**

- Red-team operator in the Executive Yuan national cyber offense/defense drill; assessor in the education-sector security drill

CTF Challenge Author — FHFCTF, THJCC CTF **2024, 2026**

- Designed web and cryptography challenges for two security competitions, covering scenario design, deployment, and solve validation

Part-time Staff — Emerging-Technology Distance Education Demonstration Program **—**

PROJECTS

Multi-Model Collaborative Detection of Prompt-Injection Attacks (research paper) **2026**

- Proposed an architecture where three heterogeneous commercial LLMs vote to jointly detect attacks, covering the blind spots of any single model
- Reached ~87% detection on long text and ~99.8% on short instructions, outperforming every individual model, over 30,000+ trials
- Solely handled literature review, experiment design, implementation, and analysis; awarded Distinction in the National Senior-High Research-Paper Competition (Information) and presented at an academic symposium

Automated Red-Team Multi-Agent System **2025–2026**

- Orchestrator agent dispatches parallel worker agents by challenge category, with shared memory and self-evolving rules
- Three-tier decision model (hard safety floor / adjustable rules / model reasoning) plus a built-in authorization & ethics policy
- AIS3 Pre-Exam: 14th individually (3,912 pts); UMDCTF: 72nd overall, 22nd in the student division

Industrial Control System (ICS) Security Range — MOE AIS3 **2025**

- Built a low-cost physical ICS range on self-made hardware; analyzed OT protocols and designed a progressive attack/defense workflow

Trashform — Image-Recognition Recycling System (PWA) **—**

– Photograph an item to identify it and get disassembly & sorting guidance per each city's rules; built with the RETHINK NGO

Aircraft Marshaller — Ground-Marshalling Simulator –

– Real-time in-browser gesture recognition with 3D guidance, used as courseware for standard aviation ground-marshalling signals (no image upload)

EDUCATION

– **Taipei Municipal Digital Experimental High School (T-School)** 2023–2026 (expected)

– Nanshan High School — Affiliated Junior High, New Taipei City

AWARDS & HONORS

– 2025 IEYI World Youth Invention Exhibition, Taiwan Selection — Gold (Team Taiwan) / World Final — Silver

– National Senior-High Research-Paper Competition, Information — Distinction (2026)

– 2024 Golden Shield Cybersecurity Skills Award, Finals — Emerging Talent Award

– 2025 CDX Cyber Offense/Defense Exchange — 5th place

– UMDCTF (international) — Open 72/763, Student 22/146

– 2025 MyFirstCTF — 26th; 2024 CGGC Cyber Guardian Challenge — 27th

CERTIFICATIONS & TRAINING

– iPAS Information Security Engineer (MOEA) — Intermediate

– MOE Advanced Cybersecurity Talent Program — AIS3, AIS3 Junior

– TAIWAN HolyHigh Training, 10th cohort — Advanced

– HackTheBox — 7+ Labs completed

TALKS

– Security course instructor (school & external): AI/LLM offense & defense, cryptography, OSINT, Linux/Kali, web security / CTF fundamentals

– MediaTek STEM educators' AI workshop — Teaching Assistant

– COSCUP 2026 ("Hackers In Taiwan") — Speaker

PUBLICATIONS

– W.-C. Zeng, "Multi-Model Collaborative Detection of Prompt-Injection Attacks," 2026 Symposium on AI & Modern Management Theory and Practice — presented.

PATENTS (INVENTOR)

– R.O.C. Utility Model **M669931** — Generative-AI-based intelligent web application firewall system

– R.O.C. Utility Model **M650895** — Intelligent fossil identification system

– R.O.C. Utility Model **M678878** — Smart elevator operation system

LEADERSHIP & COMMUNITY

– T-School InfoSec Club — President; Aviation Club — Vice President

– ISIP inter-school security club "ZeroDay C00kie" — Course Lead; 2026 "Bak3 C00kie" camp — Chief Organizer

– NTUST Information Security Club — Member

– 2025 HITCON Cyber Range — Operations; 2026 SITCON — Operations