Joshua Hung

909-760-8177 | rjhung8949@gmail.com | linkedin.com/in/jrhung | github.com/JoshRJHung

Competitions

Cyberforce September 2025 - November 2025

U.S Department of Energy *Tinley Park, IL*

- Recommended cost-effective mitigations using OPNsense, Velociraptor, and Ansible AWX—reducing potential response costs by **over $3 million** compared to average ICS incident impact.
- Designed and maintained a 6-machine AWS environment, hosting critical services (SSH, Mail, Web, SMB, NFS) across Ubuntu 22.04.5 and OpenSUSE 15.7, achieving **100% service uptime** during competition
- Conducted a comprehensive vulnerability assessment, identifying and documenting **100+** security flaws with prioritized remediation recommendations.

Experience

Competitions Developer August 2025 - Present

Cal Poly Pomona SWIFT *Pomona, CA*

- Built CTF/Purple Team environments simulating Linux attack chains (privilege escalation, persistence, service exploitation)
- Developed realistic vulnerabilities (SUID abuse, SSH misconfigurations, bind shells, PostgreSQL defaults) for training scenarios
- Delivered cybersecurity labs and workshops on system hardening and access control

Projects

Hardening Linux Presentation & Workshop March 2026

- Delivered a technical presentation on Linux threat hunting, privilege escalation, and persistence techniques to 15 participants
- Led a hands-on workshop using a Kali vs Ubuntu lab to simulate end-to-end attack and remediation workflows
- Demonstrated privilege escalation vectors and applied hardening controls (iptables, least privilege) to reduce system attack surface

Web Application Security Lab (Competition Environment) March 2026

- Remediated critical web vulnerabilities including SQL injection and server-side template injection (SSTI) in a Python Flask application
- Secured PostgreSQL integration by enforcing proper input handling, parameterization, and access controls
- Implemented SSL/TLS to protect data in transit and reduce exposure to interception and injection attacks
- Operated in a timed, adversarial environment requiring rapid identification and mitigation of active exploits

MITRE eCTF Defensive Team January 2026 - March 2026

- Solved embedded security challenges involving reverse engineering, cryptographic analysis, and system exploitation
- Analyzed vulnerabilities in C-based firmware and contributed to identifying weaknesses in authentication and communication mechanisms
- Used Docker and Git to work within a shared, reproducible development and testing environment

Certificates

- *Google Cybersecurity Certificate*
- *CompTIA Security+ (SY0-701)*

Technical Skills

Languages: C, Python, SQL, Bash

Developer Tools: Cisco Packet Tracer, Github, Git, Docker, Microsoft Office 365, VS Code, Google Workspace, Slack

Education

California State Polytechnic University , Pomona Pomona, CA

Bachelor of Science: Business Administration in Computer Information Systems *Aug. 2024 – Present*

Expected Graduation: December 2027 — Current GPA : 3.98