Mahir Asif

Security Automation Engineer

asifmahir907@gmail.com
+60133329115
Kuala Lumpur, Malaysia
https://www.linkedin.com/in/mahir907
https://github.com/mahirhacks
https://mahirhacks.github.io/MHACKS/

PROFESSIONAL SUMMARY

Security Automation Engineer combining hands-on web and API penetration testing with automated security tooling and AI-driven risk estimation. Built VULNERA, a C/C++ vulnerability triage and research pipeline using GraphCodeBERT embeddings and tree-based ensemble models, exposed through a FastAPI backend for function-level risk review. Performed web application and API security assessments for Australian enterprise and Malaysian government clients as Junior Penetration Tester at FSeC, reviewing AWS security configurations and documenting findings with CVSS-based severity ratings. Focused on automating offensive security workflows, vulnerability triage pipelines, and structured VAPT reporting.

CORE SKILLS

Automation & Cloud: Python, Bash, FastAPI, AWS, Azure

Offensive Security: Penetration Testing, Web & API Security, Burp Suite, Metasploit, Nmap, Privilege Escalation

AI & Machine Learning: GraphCodeBERT, PyTorch, LLM Engineering, AI Agents

Security Research & Reporting: VAPT Reporting, OSINT, Networking

Development & Tooling: CI/CD, Linux, Git, C/C++, JavaScript, React

PROFESSIONAL EXPERIENCE

Junior Penetration Tester Oct 2025 - Jan 2026
FSeC @ APU / APIIT

- Conducted web application and API penetration testing for Australian enterprise and Malaysian government clients.
- Reviewed security configurations across AWS and Azure environments for enterprise and government clients.
- Documented vulnerabilities using CVSS-based severity ratings and translated findings into practical remediation guidance.

Graphic Designer Dec 2022 - Dec 2022
MD Infotech

- Created an animated technical explainer for a future company project, translating technical requirements into a concise visual narrative.
- Developed the supporting concept, motion direction, and graphics for the explainer.

SELECTED PROJECTS

VULNERA - Function-Level Vulnerability Risk Estimation Jan 2025 - Jun 2026

Built a C/C++ vulnerability triage and research pipeline using GraphCodeBERT embeddings, tree-based ensemble models, calibration, signature corroboration and optional explainability. Designed temporal train/validation/test evaluation for forward-era generalization and exposed the analysis pipeline through a FastAPI backend and React interface for function-level risk review.

Xekute Jan 2026 - Present

Built a local-first workspace for authorized security assessments that connects scope and rules of engagement, intercepted HTTP traffic, evidence, findings, security tooling, behavior mapping and policy-controlled AI assistance. Designed human-in-the-loop authority controls and persistent assessment artifacts to keep automated actions bounded by operator-defined scope.

LeadBondhu AI Jan 2025 - Present

Built and deployed a production AI-powered lead-capture platform for Bangladeshi small and medium businesses with Bangla, Banglish and English language support. Integrated Meta messaging channels (Messenger and Instagram), the Gemini API, Supabase, Resend and Cloudflare-based serverless infrastructure. Built with React, TypeScript, Node.js and Tailwind CSS.

Joblicator Jan 2024 - Present

Developed a local-first job application workspace that stores structured career data and job postings in JSON. It uses a multi-stage local LLM pipeline, built with Python and Ollama, to generate tailored resumes and cover letters through reviewable generation stages. Visual templates with local HTML/PDF export complete the workflow, with a React/Vite frontend and REST APIs.

Mentora Jan 2026 - Present

Voice-first visual AI tutoring prototype in which an LLM plans short teaching turns, deterministic board tools construct and verify the visual state, and a realtime voice layer performs the validated explanation. Added strict script validation, session persistence, turn cancellation, state verification and regression tests for reliable multimodal orchestration.

Jarvis Voice Assistant Jan 2026 - Present

Engineered a local Windows voice assistant using wake-word detection, speech recognition, layered intent routing, deterministic tool execution, and a local LLM fallback for ambiguous commands. Designed the routing path so common actions execute without requiring an LLM, keeping routine commands fast and deterministic. Built with Python, faster-whisper, openWakeWord, and Ollama.

EDUCATION

Asia Pacific University of Technology & Innovation (APU / APIIT) Jan 2022 - Jun 2026

Bachelor of Science (Honours), Computing / Cybersecurity

CGPA: 3.38

Relevant Coursework: Programming and Systems: C, C++, Python, Java, x86 Assembly, Linux and Windows administration. Networking and Cloud: Cisco networking, OSPF, VLANs, ACLs, AWS and cloud architecture. Cybersecurity: web and API security, vulnerability assessment and penetration testing, OWASP, STRIDE and secure systems. AI/ML: deep learning, transformer models, dataset pipelines, fine-tuning, LoRA and QLoRA.

CERTIFICATIONS

eJPT - Junior Penetration Tester - INE Security Mar 2026

AWS Certified Solutions Architect - Associate - Amazon Web Services Jan 2026

AWS Certified AI Practitioner - Amazon Web Services Jan 2026

AWS Certified Cloud Practitioner - Amazon Web Services Jan 2026

RH134 - Red Hat System Administration II - Red Hat Dec 2025

ACHIEVEMENTS

Google Capture the Flag 2025 Participant Oct 2025

Participated in Google Capture the Flag (CTF) 2025.

Junior Penetration Tester - FSeC @ APU / APIIT Oct 2025

Completed hands-on penetration-testing work involving enterprise and government-facing web, API and cloud-security assessments.

Production SaaS Deployment Jan 2025

Designed and shipped LeadBondhu AI as a production multilingual AI lead-capture application.

ADDITIONAL INFORMATION

Languages: English (Fluent), Bengali (Native)