SHAKTHI VEL

GRADUATE STUDENT

My Contact

vshakthi@hotmail.com

Vancouver, BC

https://shakthiv.netlify.app/

https://memegamer138.github.io/
(HTB Writeups)

Skills

- **Offensive Security & Testing:** Penetration Testing, Vulnerability Assessment, Web Application Security, Cloud Security Testing (AWS), Business Logic Testing, OWASP Top 10, Red Teaming Fundamentals, Adversarial Thinking
- **Tools & Exploitation:** Burp Suite, Metasploit, Nmap, Wireshark, Kali Linux, Nessus, SQLmap, John the Ripper, Hashcat, ghidra
- **Programming:** Python, Bash, Go (Familiar), Git, Scripting for Exploit Development
- **Core Competencies:** Exploit Research, Technical Documentation, Root Cause Analysis, Cross-functional Collaboration, Analytical Problem-Solving

Certifications and Awards

- Google CyberSecurity Certificate
- Foundation of Machine Learning & Secure Interaction - Birla Institute of Technology and Science Pilani, Dubai.
- Ethical Hacking and Cybersecurity Masterclass course
- Website Hacking / Penetration Testing & Bug Bounty Hunting
- Certificate of Distinction in Canadian Computing Contest , University of Waterloo, Canada.
- Certificate of Distinction in Euclid Contest, University of Waterloo, Canada.

Professional Summary

Cybersecurity graduate student maintaining a GPA of 3.56/4 and with deep experience in analyzing LLM behavior, prompt injection risks, and system misuse cases. Combine structured security methodology (OWASP, threat modeling) with hands-on AI project work to identify, classify, and mitigate emerging AI security threats. Precise, analytical, and curious about how systems fail and how to make them safer.

Education Background

- **SIMON FRASER UNIVERSITY**
  Masters in Cybersecurity
  2025-2027
- **UNIVERSITY OF BRITISH COLUMBIA**
  Bachelors in Computer Science
  2021-2025

Projects and Experience

VimiLabs Research Platform — Security Vulnerability Assessment

- **Conducted a comprehensive security assessment** of a cloud-based platform, employing a structured methodology to identify critical gaps in AWS IAM, authentication, and data flows.
- **Analyzed business logic and system interactions** to uncover vulnerabilities impacting data integrity and access, demonstrating risk analysis and holistic system evaluation.
- **Delivered a detailed analysis report** with prioritized recommendations, showcasing the ability to **investigate technical solutions and communicate findings** for strategic improvement.

AI-Powered Social Engineering Detection

- **Leading the development of AI agent workflows** to automate the analysis and interpretation of security threats in electronic messages.
- **Building and optimizing Python APIs** (FastAPI) to deliver real-time security assessments to browser and email plugins developed through JavaScript.
- **Engineering prompt strategies to improve AI accuracy** in identifying phishing tactics, working towards a 90% success rate for actionable user advice.
- **Technologies:** Python, FastAPI, AWS, LLM/Prompt Engineering, Agno, JS

ReXeN ReconSentry – AI-Powered Reconnaissance Orchestrator

- Engineering a **reconnaissance tool to automate and enhance** the initial phase of penetration tests by orchestrating 30+ security tools
- Implementing **intelligent post-processing to analyze and categorize** discovered endpoints to prioritize high-value targets.
- Designed a **compliance-first architecture** with scope validation to adhere to legal and programmatic testing boundaries.
- Built to solve the practical problem of **reducing analyst noise** and focusing effort, demonstrating a process-improvement mindset.

Threat Intelligence Dashboard

- Developing Python-based dashboard **aggregating real-time threat data** from VirusTotal, Google OSV, Alienvault OTX APIs
- Correlated malware, IOCs, and vulnerability data to **identify attack patterns** and prioritize threats
- Gained hands-on threat intelligence and **security monitoring experience**