Vimalatithyan S

Chennai, Tamil Nadu, India | Vimalatidhyan@gmail.com | +91 9345518356
LinkedIn | Portfolio | GitHub

Professional Summary

Cybersecurity practitioner focused on Vulnerability Assessment and Penetration Testing (VAPT), Application Security, and AI/LLM Security. Experience includes web application and network security testing, attack surface discovery, security workflow automation, and responsible vulnerability disclosure. Hands-on exposure to prompt-injection testing, AI red teaming, SAST/DAST integration, and reconnaissance tooling. Interested in entry-level VAPT, Application Security, Product Security, and AI Security opportunities.

Technical Skills

VAPT and Offensive Security: Penetration Testing, Vulnerability Assessment, Web Application Security Testing, Network Security Testing, Exploitation Validation, Reconnaissance, Bug Bounty

Application and API Security: OWASP Top 10, API Security, SAST, DAST, Software Composition Analysis (SCA), Threat Modeling, Authentication and Access-Control Testing, Vulnerability Triage

AI and LLM Security: LLM Security Testing, Prompt Injection, AI Red Teaming, Model Extraction Risks, Training-Data Poisoning Detection

Vulnerability Research: Proof-of-Concept (PoC) Development, CVSS Scoring, Responsible Disclosure, Security Reporting, STRIDE

Tools: Burp Suite, Nmap, Nuclei, Subfinder, httpx, Kali Linux, Wireshark

Programming and Scripting: Python, Bash (Basic)

Cloud: AWS, Microsoft Azure, Google Cloud Platform (GCP) (Basic)

Professional Experience

TECHNIEUM Feb 2026 – Aug 2026
Offensive Security Consultant Intern *Chennai, India*

- Contributed to an Attack Surface Management (ASM) platform supporting external asset discovery, exposure monitoring, and security assessment.
- Performed network and web application penetration testing to identify, validate, and document security vulnerabilities.
- Conducted LLM security assessments focused on prompt injection, AI application weaknesses, and AI red-teaming techniques.
- Worked on SAST and DAST integrations to support application security testing and vulnerability identification.

Education

Saveetha School of Engineering 2024 – 2028
Bachelor of Engineering (B.E.), Electronics and Communication Engineering *CGPA: 7.50/10*

Selected Security Projects

CVE-2026-91751 – Path Traversal in Flextype CMS *Security Research*

- Discovered and responsibly disclosed a path traversal vulnerability in Flextype CMS; prepared a proof of concept, impact analysis, and remediation details for the CVE record.

Reconnaissance Automation Tool *Personal Project*

- Built an end-to-end reconnaissance pipeline using Python, Bash, Subfinder, httpx, and Nuclei to automate subdomain enumeration, live-host identification, and vulnerability scanning.
- Recorded an 80% reduction in manual reconnaissance time through workflow automation.

Web Application VAPT Case Studies *Security Assessments*

- Assessed 20+ web applications and investigated issues including broken authentication, insecure direct object references (IDOR), OAuth token leakage, and exposed API keys.
- Documented findings with proof of concept, impact, severity, and remediation recommendations.

Attack Surface Management (ASM) Platform *Platform Development*

- Contributed to continuous asset discovery, shadow IT identification, and external exposure monitoring workflows.
- Developed workflows to map an organization's external digital footprint and flag potentially exposed or unauthorized assets.

Selected Security Projects (Continued)

LLM Security Testing Suite *AI Security*
- Developed security-testing workflows for LLM applications covering prompt injection, model-extraction risks, training-data-poisoning detection, and AI red teaming.
- Evaluated weaknesses in AI application workflows and the effectiveness of security controls.

SAST and DAST Integration Platform *Application Security*
- Worked on integrating static source-code analysis and dynamic application testing to support application security assessments.
- Designed workflows to identify code-level weaknesses and runtime vulnerabilities across application components.

AI-Assisted Automated Penetration Testing *Security Automation*
- Designed an AI-assisted penetration-testing framework to map attack surfaces, identify potential vulnerability chains, and generate actionable security reports.
- Explored automation of reconnaissance, vulnerability validation, and reporting with human oversight.

Independent Security Research *Ongoing*
- Conduct independent vulnerability research across web applications, enterprise software, and cloud infrastructure.
- Investigate attack vectors, validate security impact, and follow responsible disclosure practices.

AI Security Automation Platform *Security Automation*
- Designed an AI-agent-based security workflow platform for alert triage, contextual enrichment, security automation, and reporting.
- Explored orchestration of security workflows to improve assessment efficiency and reduce repetitive manual tasks.

Security Research and Recognition

- Reported security vulnerabilities through responsible disclosure programs involving Beamery, Shippit, Crossmint, LG, and Artsy.
- Received NASA Hall of Fame recognition for security research.
- Research interests include web application vulnerabilities, API security, authentication weaknesses, and attack surface research.

Practical Security Training

- **PortSwigger Web Security Academy:** Hands-on labs covering authentication, access control, file upload, path traversal, JWT, API testing, and race conditions.
- **Security Labs:** Practical reconnaissance, vulnerability validation, penetration testing, and web security assessment.

Leadership and Activities

- **Google Developer Groups (GDG), SIMATS – Core Team Member, Cybersecurity Team Lead:** Contributed to technical activities and community events.