Vimalatithyan S.

Penetration Tester · Bug Bounty Hunter · Offensive Security Intern · Aspiring SOC Analyst

Chennai, India
Email: vimalatidhyan@gmail.com — Phone: +91 93455 18356
Portfolio: vimalatidhyan.vercel.app — LinkedIn: linkedin.com/in/vimalatithyan — GitHub: github.com/Vimalatidhyan

Summary

Second-year BE student with 2+ years of hands-on experience in penetration testing, vulnerability assessment, ethical hacking, and bug bounty hunting. Recognized by NASA, Google, Microsoft, Amazon, and 3 other global organizations for responsible vulnerability disclosures. Currently interning at TECHNIEUM in offensive security, contributing to Attack Surface Management (ASM), LLM security testing, SAST/DAST tool development, and AI-powered automated penetration testing research. Skilled in Python, Bash scripting, Burp Suite, Nuclei, and end-to-end recon automation. Targeting SOC Analyst or Junior Penetration Tester roles.

Education

Bachelor of Engineering — Electronics and Communication Engineering
Saveetha School of Engineering, Chennai *2024 – 2028 (2nd Year)*

Higher Secondary Education (Class XII)
Jaya Jaya Sankara International School, Nazarathpet, Chennai *2023*

Internship Experience

Offensive Security Intern — TECHNIEUM Chennai, India
February 2026 – Present

- Contributing to the development of an **Attack Surface Management (ASM)** platform to automate asset discovery, subdomain enumeration, and exposure monitoring across large attack surfaces.
- Involved in research and development of an **LLM Security Suite** — testing and identifying security vulnerabilities in large language model deployments including prompt injection, data leakage, and model abuse vectors.
- Participating in **SAST and DAST tool development** — building static and dynamic analysis pipelines to detect vulnerabilities in source code and running web applications.
- Contributing to **AI-powered automated penetration testing** research — exploring how AI/ML can automate recon, vulnerability detection, and exploit chaining workflows.
- Conducting web application penetration testing and vulnerability assessment on real-world client targets under supervised offensive security engagements.
- Writing professional penetration testing reports with CVSS scoring, PoC evidence, and remediation guidance.

Security Hall of Fame & Responsible Disclosures

Vulnerabilities responsibly disclosed to and acknowledged by the following global organizations:

- **NASA** — Hall of Fame Recognition (vulnerability responsibly disclosed and acknowledged)
- **Microsoft** — MSRC (Microsoft Security Response Center) acknowledgment
- **Google** — Vulnerability Reward Program (VRP) submission acknowledged

- **Amazon** — VRP submission for security issue in web infrastructure acknowledged
- **Audinate** — Security team acknowledgment for responsible disclosure
- **TrekMail** — Valid security vulnerability disclosure acknowledged
- **Shippit** — Valid security disclosure acknowledged

Security Experience

Bug Bounty Researcher — HackerOne — Bugcrowd — Intigriti — YesWeHack *2023 – Present*

- Identified 15+ valid vulnerabilities across 4 platforms including authentication flaws, IDOR, OAuth misconfiguration, information disclosure, and API security issues.
- Developed custom recon pipelines combining subfinder, httpx, gau, nuclei, and ffuf — reducing manual recon effort by ˜70% for large-scope targets.
- Validated and triaged findings with detailed exploitation steps, CVSS scoring, and professional disclosure reports.
- Recognized by 7 global organizations including NASA, Microsoft, Google, and Amazon for responsible vulnerability disclosures.

Core Team Lead — Cybersecurity, GDG SIMATS Chennai, India *2024 – Present*

- Organized and led 5+ cybersecurity workshops, CTF events, and security awareness sessions reaching 100+ students.
- Delivered hands-on sessions covering OWASP Top 10, ethical hacking methodology, bug bounty workflows, and web application attack techniques.
- Promoted security-first mindset and responsible disclosure culture within the student developer community.

Projects & Tools

VScanAI — AI-Powered Vulnerability Scanner *2024 – Present*

- Building an AI-based vulnerability scanner integrating Wappalyzer fingerprinting, OCR, and CVE mapping using Python.
- Automates full pipeline: technology detection → CVE lookup → vulnerability validation, reducing manual analysis time significantly.

BBRM — Bug Bounty Recon Master *2024 – Present*

- Developing an all-in-one Python recon automation tool covering subdomain discovery, URL crawling, JS file analysis, and vulnerability scanning.
- Integrates subfinder, httpx, gau, nuclei, and ffuf into a single automated workflow with structured reporting output.

Bash Recon Automation Framework *2024*

- Designed end-to-end Bash scripting pipeline: subdomain enumeration → live host detection → vulnerability scanning → result aggregation.
- Reduced full reconnaissance time by ˜70% compared to manual workflow for large-scope bug bounty targets.

Certifications & Training

Certified Red Team Operations Management (CRTOM) *2024*
Certified Cybersecurity Educator Professional (CCEP) *2024*
Google Cloud Skill Badges — Google *2024*
Network Fundamentals — LetsDefend *2024*
Digital Forensics Training — Crypto Eagle Forensics *2024*

- Hands-on exposure to data, memory, email, web, and basic network forensics.

AI-Powered Full Stack Training — Hifi11 Technologies *2024*

Skills

Offensive Security: Penetration Testing, Ethical Hacking, Web Application Security, VAPT, Vulnerability Assessment, Bug Bounty Hunting, Reconnaissance, OAuth Testing, API Security Testing, OWASP Top 10, OSINT, Exploit Research, Security Auditing, Information Security
Security Research: LLM Security Testing, SAST, DAST, Attack Surface Management, AI-Powered Pentest Automation, CVE Analysis, Vulnerability Research, Threat Intelligence
Defensive Security: SOC Fundamentals, Network Security, Log Analysis, Alert Triage, Incident Response, Network Fundamentals, Security Monitoring
Tools: Burp Suite, Nuclei, FFUF, Subfinder, Assetfinder, httpx, Katana, GAU, Wayback Machine, Nmap, Kali Linux, Git, Linux
Programming & Scripting: Python, Bash Scripting, Security Automation, Recon Automation
Platforms: HackerOne, Bugcrowd, Intigriti, YesWeHack
Other: Technical Report Writing, Responsible Disclosure, CVSS Scoring, Penetration Test Reporting, Security Documentation, Vulnerability Triage