LAKSHMIKANTHAN K

Security Research Engineer | *Vulnerability Research & AI/LLM Security*

Tamil Nadu, India | lakshmikanthank2006@gmail.com | LinkedIn | GitHub | Portfolio

SUMMARY

Security Research Engineer with **24 published CVEs** (6 Critical, up to **CVSS 9.9**) across production systems including **MariaDB**, **Ghost CMS**, and **AI-agent frameworks**. **11 GitHub Security Advisory** credits, **50+ responsible disclosures**, and **10 published PyPI** security tools.

SECURITY RESEARCH & CVE DISCLOSURES

- **24 CVEs** disclosed across **10+ open-source projects**, including **6 Critical** findings (**CVSS 9.1–9.9**), resulting in vendor-issued patches.
- **MariaDB Server**: Critical RCE via unsafe wsrep_notify_cmd handling (**CVE-2026-49261**, **CVSS 9.9**), plus a related command-injection flaw (**CVE-2026-48165**).
- **PraisonAI**: led a **6-CVE** exploit chain — template injection RCE, sandbox bypass, unsafe workflow execution (**CVE-2026-40088, -40154, -40156, -40158, -40159, -40288**; up to **CVSS 9.8**).
- **Ghost CMS**: 3 SSRF vulnerabilities via IPv4-mapped IPv6 bypass and DNS rebinding (**CVE-2026-53944, -53945, -37666**).
- **compliance-trestle**: recursive SSTI → RCE, SSRF, and path-traversal file write (**CVE-2026-46439, -46380, -46345**).
- Additional CVEs in **Apache Airflow**, **Apache ECharts**, **Oracle OCI CLI**, **Flarum**, **pyload**, **WordPress GamiPress**.
- **Top 1%** ranked on TryHackMe; multiple vendor **Hall of Fame** recognitions.
- Publish technical vulnerability write-ups and CVE analysis on Medium (**@letchupkt**).

TECHNICAL SKILLS

Offensive Security: Vulnerability Research, Exploit Development, Burp Suite, Metasploit, Nmap, Wireshark, OWASP Top 10

Application & Product Security: Secure Code Review, SAST/DAST, RCE/SSRF/SSTI/IDOR/SQLi Analysis, Supply-Chain Security

AI / LLM Security: AI-Agent Auditing, Prompt Injection, Sandbox Escape Analysis

Languages & Cloud: Python, C, C++, JavaScript, SQL | Linux (Kali), Docker, Git, AWS, GCP

PROFESSIONAL EXPERIENCE

Security Researcher & Bug Bounty Hunter | Independent *2024 – Present | Remote*

- Independent vulnerability research yielding **24 CVEs** and **50+ disclosures** over **2 years**.
- Coordinated disclosure end-to-end — report, triage, patch verification — via **GitHub Security Advisories**.
- Built and open-sourced **6 security tools** (PluginHunter, DepRaptor, BugPilot CLI, AppXploit, OriginX, Kali MCP).

AI & ML Developer Intern | genzi.ai *Jun 2025 – Feb 2026 | Singapore (Remote)*

- De facto technical lead for a **4-person team** building a production AI real estate platform for Singapore agents, driving architecture with the Tech Manager.
- Designed the **PostgreSQL** schema and backend architecture; integrated **LLM** features into production.
- Defined security architecture and deployment for the platform, applying secure coding to LLM-facing interfaces.

Open Source Contributor | Open Source Connect *Sep 2025 – Present | Remote*

- Contributed code, fixes, and documentation across multiple open-source projects.

OPEN SOURCE

- **10 PyPI** security tools spanning web, mobile, WiFi, hardware, and AI-inference security.
- **37 repositories**, **49 stars**, **25 followers**; GitHub Pull Shark & Starstruck achievements.
- **11 GitHub Security Advisory** credits across major open-source projects.
- Authored **Bug Bounty Roadmap 2025**, an open-source learning path for security researchers.

SELECTED OPEN SOURCE SECURITY PROJECTS

PluginHunter — *Python, WordPress Security* (5 stars, PyPI)

- AI-powered scanner with **48 detection rules**; full **OWASP Top 10** coverage.

AppXploit — *Python, Android Security* (PyPI)

- APK security analysis tool for bug bounty hunters; automates static mobile-vuln analysis.

DepRaptor — *Python, Supply-Chain Security* (PyPI)

- Dependency-confusion vulnerability scanner and PoC generator for public registries.

OriginX — *Python, Network Recon* (PyPI)

- WAF origin-IP discovery tool for bypassing CDN/WAF protection in recon workflows.

BugPilot CLI — *Python, AI, Offensive Security* (PyPI)

- Autonomous pentesting assistant integrating **50+ tools** and multiple LLM providers.

Kali MCP — *Python, MCP, Linux*

- API bridge connecting MCP clients to Kali Linux for AI-driven offensive workflows.

EDUCATION

B.Tech, Artificial Intelligence and Data Science *2023 – 2027 | CGPA: 8.00/10.0*
Sri Ramakrishna College of Engineering, Perambalur

CERTIFICATIONS

- **CRTOM** (Certified Red Team Operations Management) — Red Team Leaders, 2026
- **CTIGA** (Certified Threat Intelligence & Governance Analyst) — Red Team Leaders, 2026
- **CBTP** (Certified Blue Team Practitioner) — The SecOps Group, 2026
- **CSEDP** (Certified Social Engineering Defense Practitioner) — The SecOps Group, 2026
- **CRTA** (Certified Red Team Analyst) — CyberWarFare Labs, 2025
- **CCEP** (Certified Cybersecurity Educator Professional) — Red Team Leaders, 2025
- **CNSP** (Certified Network Security Practitioner) — The SecOps Group, 2025
- **CORE** (Certified Cybersecurity Foundations) — Hackviser, 2026
- ISC2 Candidate — ISC2, 2025 | OPSWAT ICIP, 2025 | LFS101 — The Linux Foundation, 2025