VENKATA RAMA KRISHNA DULAM

8019133994 | ramakrishnadulam10@gmail.com | linkedin.com/in/venkata-rama-krishnadulam-302637378 | github.com/Ru0k3

PROFILE

AI-focused Computer Science and Engineering student building agentic systems and RAG pipelines, with seven months of Android penetration-testing experience at bi0s, Amrita Amritapuri.

EDUCATION

Amrita Vishwa Vidyapeetham, Amrita School of Computing, Amritapuri Campus **2025-2029**
Bachelor of Technology in Computer Science and Engineering, Artificial Intelligence

Prathibha Junior College, Rajahmundry, Andhra Pradesh
Intermediate (+1, +2) *945/1000*

Prathibha Educare, Rajahmundry, Andhra Pradesh
SSC (10th Grade) *545/600*

PROJECTS

SentinelOps — Safety-Gated DevOps Agent |*Python, LangGraph, LangChain, FastMCP*

- Built an incident-response workflow that correlates alerts with logs and recent commits, prepares candidate patches, runs sandbox tests, evaluates confidence and blast radius, and escalates sensitive changes instead of modifying production.

MailDM — Privacy-Focused AI Email Briefing |*TypeScript, Discord, Gmail OAuth, Scheduled workflows*

- Developed a multi-user application that creates timezone-aware AI summaries from read-only Gmail access and delivers them through Discord direct messages without sending, deleting, archiving, or marking mail as read.

Provider-Neutral Agent Launch — Enterprise AI Architecture |*Python, FastAPI, Redis, Prometheus, CI/CD*

- Designed a provider-independent agent architecture spanning model providers, runtime, storage, authentication, rate limiting, streaming, testing, monitoring, and deployment.

Open-Source AI Contributions |*Cognee, Headroom, NitroStack*

- Contributed provider-aware NVIDIA NIM embedding support and tests to Cognee; hardened fork-safe CI workflows; fixed uv-installed Headroom binary detection; and added a Zerogravity MCP sample app to NitroStack.

bi0s Security Writeups and DexProbe |*Ghidra, GDB, ltrace, JADX, Frida, Python — Sep 2025 - Mar 2026*

- Completed a 7-month Android penetration-testing engagement at bi0s, Amrita Amritapuri, where the tools and techniques below were learned and applied.
- Conducted Android application security analysis, APK inspection, and Flutter reverse engineering through hands-on research and technical writeups.
- Used JADX, Frida, Objection, Reflutter, Ghidra, GDB, ltrace, and Python to inspect application logic, authentication behavior, data flow, and binary transformations.
- Documented reverse-engineering challenges involving XOR, ROT13, obfuscation, memcmp analysis, Android APK inspection, SSH, Nmap, Netcat, OpenSSL, and setuid.
- Practiced CTF reverse engineering, Linux security, x86-64 assembly, stack and memory inspection, breakpoint analysis, and binary patching.

TRAINING AND ACHIEVEMENTS

- Google Cohort 3 / Hack2Skill: completed three Google Cloud hands-on labs involving AI agents, RAG, MCP, BigQuery, and human-in-the-loop workflows; scored 10/10 on all three associated quizzes.
- Summer Analytics 2026: Certificate of Excellence (Top 10%), Certificate of Merit (Top 25%), and capstone completion recognition; focus areas included data science, machine learning, AI, hackathons, Celonis, and process mining.

SKILLS

Cybersecurity: Android penetration testing, APK analysis, Flutter reverse engineering, dynamic analysis, binary analysis, binary patching, CTFs, Linux security, GDB, x86-64 assembly

Security Tools: JADX, Frida, Objection, Reflutter, Ghidra, GDB, ltrace, Nmap, Netcat, OpenSSL, pwntools, Kali Linux, Ubuntu

AI and Agent Systems: LangGraph, LangChain, Langfuse, Google ADK, RAG, MCP tools, agent orchestration, evaluation and tracing, human-in-the-loop workflows, NLP, machine learning, data science

Programming and Infrastructure: Python, C, C++, Java, JavaScript, FastAPI, Streamlit, Redis, REST APIs, Git/GitHub, CI/CD, Prometheus, Linux

Portfolio: github.com/Ru0k3/portfolio | Public work and writeups available on GitHub