RAGHAVA N

raghavtwenty@gmail.com | Portfolio | www.linkedin.com/in/raghavtwenty/ | GitHub

EDUCATION

Integrated Masters in Artificial Intelligence & Machine Learning July 2021 - May 2026
Coimbatore Institute of Technology, Coimbatore CGPA 8.7/10 as of 6th sem

EXPERIENCE

MALWARE ANALYST (Research Internship) July 2024 - November 2024
Defence Institute of Advanced Technology Pune, Maharastra

- Researched the generation and analysis of polymorphic and metamorphic malware using Large Language Models (LLMs), configured a custom malware analysis lab using FlareVM and Remnux, and performed static and dynamic malware analysis on 50+ malware samples in a sandboxed environment, delivering comprehensive reports on findings.
- Utilized AI agents and LangChain to demonstrate the effectiveness of different prompt types (Direct, Indirect, Adversarial) in generating malware with LLaMA 3.1 70B, achieving the highest success rates with adversarial prompts, generating 51 compiled and 35 executable code samples, showcasing advanced malware creation techniques.

INDEPENDENT SECURITY RESEARCHER August 2023 - June 2024
NCIIPC (A unit of NTRO) Remote

- Performed penetration testing and vulnerability assessments on Indian government websites and public organizations, identifying and reporting over 10+ critical security vulnerabilities (CVSS 9+), including XSS, OTP bypass, account takeover, and SQL injection attacks, earning recognition and appreciation from the Indian government and ISRO.

PROJECTS

PROTECTION ONLINE Source Code

- Developed a Chrome extension with a four-layered security approach (SSL certification, Google Safe Browsing, crowd sourced data, obfuscated JavaScript), achieving 89% accuracy in detecting malicious sites through deep learning methods. Utilized Generative AI and RAG to check regulatory compliance (DPDPA 2023, IT Act 2000) and to summarize E-commerce privacy policies with regional language translation, reducing reading time by 93%.

GENZ HIRING Source Code

- Engineered a resume analysis tool using LLM, LangChain, and ChatGPT 3.5 to provide tailored suggestions for aligning with career goals, streamlining the applicant experience by leveraging SerpAPI and web scraping techniques for personalized job suggestions, reducing time spent on job searches by 50%, and creating customized resumes to enhance success in specific job applications, making it an essential tool for students, professionals, and job seekers.

INTRUSION DETECTION PREDICTION Source Code

- Developed and deployed a cybersecurity solution using machine learning to predict cyber attacks based on network packet data, employing preprocessing (EDA, cleaning, sampling, scaling, visualization) to reduce data redundancy by 39%. Utilized Naive Bayes, Random Forest, and XGBoost models for classification, with hyperparameter tuning and cross-validation, achieving an average accuracy of 94% with the XGBoost model, outperforming other models.

CERTIFICATIONS

- Red Teaming LLM applications, DeepLearning.AI August 2024
- Ethical Hacking Essentials (EHE), EC Council July 2024
- Google Cybersecurity Professional Certification, Coursera April 2024
- Introduction to Cyber Intelligence, U.S. Department of Homeland Security November 2023

ACHIEVEMENTS

- CTF Player, Top 150 in National level CTF Time Ranking August 2024
- First place in the Byte Sized Brainstrom Hackathon (The DoughVinci Code) hosted by Cookr April 2024
- Secured 15th position out of 870+ teams in the National-level Dark Patterns Hackathon at IIT Varanasi January 2024
- Achieved second place in Googleathon 2.0 organized by the Google Developers Student Club, SNS November 2023

TECHNICAL SKILLS

Languages:	Python, SQL, C, HTML, CSS, JavaScript, Java, R, React JS
Frameworks:	LangChain, CrewAI, TensorFlow, Pandas, Scikit learn, TKinter, Flask, FastAPI
Tools:	Git & GitHub, Virtual Machines, Docker, Figma, Cisco Packet Tracer, MacOS, Linux
Machine Learning Concepts:	Supervised and Ensemble Learning, Artificial Neural Networks, Deep Learning, LLM
VAPT Tools & Techniques:	OSINT, Reconnaissance, Floss, CFF Explorer, Burp Suite, Nikto, Nmap, Wireshark