CHIRANJEEVI G

+91 8073761695
chiranjeevi.naidu@proton.me
Bangalore, India
github.com/morpheuslord
Profile Webpage
/in/chiranjeevi-g-naidu
Personal Blogs
ORCID Records

PROFESSIONAL SUMMARY

Professional with more than 2+ years of experience in the cybersecurity, artificial intelligence, and cloud infrastructure domains. Experience in securing systems, networks, and web applications through vulnerability assessments and risk management. Skilled in Python automation and AI integration, developing tools that enhance threat detection and response capabilities. Knowledgeable in deploying secure infrastructure on AWS and Azure cloud platforms. Technical writer with the ability to explain complex concepts in cybersecurity, AI, and cloud technologies to diverse audiences. Continuously learning new technologies and frameworks across multiple domains to deliver effective solutions.

SKILLS

Hard Skills:

- **Programming:** Python, Shell Scripting/Bash, API Development, Python Flask/FastAPI, JavaScript, SQL, Git/GitHub.
- **AI & Machine Learning:** RAG & Agentic AI, LLM Integration (ChatGPT, Claude, Llama2), LangChain/LangGraph, Prompt Engineering, Model Context Protocol (MCP), RAG Ops, Vector Databases, Knowledge Graphs.
- **Cybersecurity & Penetration Testing:** Burp Suite, Nmap, Vulnerability Assessment, Network Security, Wireshark, OWASP, Penetration Testing, MITRE ATT&CK, Wazuh, EDR & XDR, Metasploit, OSINT.
- **Cloud & Infrastructure:** AWS, Linux Administration, Docker/Docker Compose, Terraform, Infrastructure as Code, MongoDB.
- **Research & Documentation:** LaTeX/TexStudio, Technical Documentation, Scientific Writing, Academic Writing, Research Methodology, Jupyter notebooks.
- **Tools & Collaboration:** Project Management, Slack, Jira, VS Code.

Soft Skills:

- **Communication**
- **Project Management**
- **Problem Solving**
- **Teamwork**
- **Adaptability**
- **Critical Thinking**

EDUCATION

4/2021 - 3/2024 **Bachelor of Computer Applications - Jain (Deemed-To-Be-University)** **Undergraduate**
Scored CGPA - 8.6

4/2018 - 3/2021 **PUC(SEBA) - Presidency University** **PUC**
Scored 87.6%

WORK EXPERIENCE

10/2023 - Present **Software Engineer - AI** **Cygne Noir Cyber**

- Developed and implemented Retrieval Augmented Generation (RAG) systems for automated threat intelligence analysis, integrating external knowledge bases with large language models to enhance cybersecurity decision-making
- Designed and deployed Agent Communication Protocol (ACP) frameworks for coordinating multi-agent security operations and automated incident response workflows
- Implemented Model Context Protocol (MCP) solutions to optimize AI model performance in cybersecurity applications, ensuring efficient context management for threat detection and analysis
- Led project teams in developing Python-based security automation tools and managed deployment of cloud security solutions for enterprise clients
- Conducted comprehensive training programs for security analysts on AI-enhanced threat hunting techniques, offensive security methodologies, and Linux exploitation frameworks
- Collaborated with clients to architect secure systems and performed vulnerability assessments, penetration testing, and security compliance audits across diverse organizational environments

3/2024 - 10/2023 **Freelance Programmer and Content Writer** **Worked for clients using Fiverr**

- Automated custom payload generation for Android devices, increasing penetration testing efficiency.
- Developed and deployed a simple C2 server for research and testing.
- Helped clients adhere to Security Compliance standards.
- Wrote 26 blog posts highlighting company services, generating 2,69,169 reads and 1 year 4 months of read time.

7/2023 - 3/2024 **Offensive Security Engineer - Intern** **Avercyber Technologies / Averlon**

- Conducted security assessments and completed prioritization of Azure and AWS infrastructure security tasks, leading to an development of a comprehensive testing suit of configuration related vulnerabilities.
- Developed and deployed several G.O.A.T Projects using Terraform, for product testing and validation.
- Completed comprehensive research on Linux packages, for optimized scanning and a unique vulnerability assessment strategy.
- Evaluated and tested SBOM tools, improving integration efficiency, and built a custom SBOM tool to perform evaluation in accordance to Linux startup research.

5/2023 - 7/2023 **Cybersecurity Engineer - Intern** **Avercyber Technologies / Averlon**

- Completed programming projects, developing automated Red Team tools for black-box analysis, and improving threat detection accuracy.
- Analyzed AWS rules to design security priorities, resulting in an compiled source of compliance standards for testing and improving.
- Performed vulnerability assessments on AWS deployments, identifying and mitigating critical vulnerabilities and testing out custom tools and resources.

PROJECTS

CVE-LLM_Dataset **Github Link**

- AI (Llama and GPT)

- Developed a dataset as a proof of concept for AI training research and the complexities of cybersecurity implementations.

HackBot **Github Link**

- Python
- AI (Llama and GPT3)

- Developed an AI-driven cybersecurity chatbot designed for accurate responses to security-related queries.
- Integrated AI models such as GPT-3 to conduct code analysis and scan analysis.
- Tailored the chatbot to assist security researchers and ethical hackers with automated insights.
- Focused on providing detailed and precise information to enhance cybersecurity efforts.

GPT_Vuln-analyzer **Github Link**

- Python
- AI (Llama2, GPT3, Palm AI, Ollama)
- Vulnerability Analysis

- Developed a proof-of-concept application leveraging AI for precise vulnerability analysis.
- Integrated AI models such as Meta Llama2, Google Palm AI, and Ollama for comprehensive cybersecurity features.
- Enabled functionalities like DNS reconnaissance and subdomain enumeration within the tool.
- Designed the tool to be upgradable and easily integrated with other cybersecurity systems.

Startup-SBOM **Github Link**

- Python
- Linux
- Reverse Engineering

- Reverse-engineered the Linux boot process to extract critical initialization information.
- Analyzed RPM and DPKG entries to identify startup capabilities of Linux OS packages.
- Implemented a function to check startup initialization using chroot for accurate boot process analysis.
- Developed a tool to list potential startup entries with high accuracy.

QuadraInspect **Github Link**

- Python
- Reverse Engineering
- Android Testing

- Developed an Android security analysis framework for comprehensive vulnerability detection.
- Integrated multiple tools within the framework to achieve precise bug hunting for Android devices.
- Focused on accurate detection of vulnerabilities and security assessment of Android applications.
- Enhanced the framework's capability to provide detailed analysis and reporting on security issues.

Brute-Hacking-Framework **Github Link**

- Python
- Batch
- Reverse Engineering
- Custom Framework

- This is a recreation of Pentestbox, this involved reverse engineering the core working of Pentestbox and remaking it from scratch.
- Developed an all-in-one system framework for all the possible tools compatible with Windows with maximum portability.
- This tool focuses on improving the reach and usability of tools. This is achieved by making sure the tools are configured to be accessible and up-gradable.

CERTIFICATIONS

Valid 6-2023 to 6-2027 — **Certified Ethical Hacker - V12** — **EC-Council**
Successfully completed my CEH V12 Certification.

Valid 6-2023 to 6-2027 — **Certified Network Defender** — **EC-Council**
Successfully completed my CND Certification.

PUBLICATIONS

6G & ML — **ML-Driven Secure Communication for Next-Generation 6G Networks** — **Springer Nature Switzerland**
Book chapter exploring machine learning applications for secure communication protocols in 6G networks, focusing on AI-driven security mechanisms and intelligent threat mitigation strategies. Published 2025.

Cybersecurity & AI — **Docker Based Decentralized Vulnerability Assessment with Port Scanning Powered by Artificial Intelligence** — **FMDB**
Research paper presenting a decentralized vulnerability assessment framework using Docker containerization and AI-powered port scanning techniques for enhanced network security analysis. Published December 2024.

AI & Malware — **Using Autoencoder-Driven Machine Learning for Advance Cybersecurity Malware Detection** — **FMDB**
Journal article investigating autoencoder neural networks for advanced malware detection, demonstrating machine learning approaches for identifying sophisticated cyber threats and malicious software patterns. Published December 2024.

AI & Datasets — **cve-llm-training** — **Hugging Face**
Curated dataset for training large language models on Common Vulnerabilities and Exposures (CVE) data, enabling AI models to understand and analyze cybersecurity vulnerabilities for automated threat intelligence. Published 2024.

Cybersecurity — **API Based Network Scanning** — **Computational Sciences and Sustainable Technologies**
Conference paper presenting API-driven network scanning methodologies for improved vulnerability assessment, focusing on scalable and efficient approaches to network security analysis and penetration testing. Published May 2023.

HONORS

Competition — **Certificate of Merit** — **BGS**
Won first place in a research presentation competition hosted by BGS College of Engineering and Technology.

Honor — **Certificate of Appreciation** — **JAIN**
Awarded by Jain(Deemed To Be University) for being the speaker in the IRDCSTEM-2023 post-conference learning.

LANGUAGES

English, **Tamil**, **Kannada**, **Telugu**

DECLARATION

I solemnly declare that the information in this resume is true to the best of my knowledge and belief. All information in this resume is right and truthful. I just wanted to let you know that the information and details shared in this resume are correct and inclusive. I take full liability for the correctness of the information.