CHIRANJEEVI G

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

PROFESSIONAL SUMMARY

I am a proactive and hands-on Cybersecurity Engineer with over a year of practical experience securing systems, networks, cloud infrastructure, and web applications. I work extensively on vulnerability assessment, threat analysis, and risk mitigation, with a strong focus on building automation-first security solutions. I am proficient in Python, security tooling, and AI-driven integrations, and I actively develop custom tools and agent-based workflows to improve detection, response, and operational efficiency. I have worked on infrastructure security projects across AWS and Azure, improving deployment reliability and security posture. Alongside engineering, I have strong technical writing and research experience, enabling me to clearly communicate complex security concepts to both technical and non-technical audiences. I am a continuous learner and problem solver, consistently pushing myself to stay ahead of evolving threats and emerging security technologies.

SKILLS

Hard Skills:

- **Programming & Scripting:** Python (automation, security tooling, agent workflows), Bash/Shell scripting, basic JavaScript for web testing and tooling.
- **Red Teaming & Offensive Security:** Web application penetration testing, system exploitation, privilege escalation, vulnerability assessment, attack surface analysis, proof-of-concept development.
- **Network VAPT:** Network enumeration, service fingerprinting, vulnerability analysis, lateral movement analysis, network penetration testing.
- **Cloud Security & DevSecOps:** AWS and Azure security fundamentals, Infrastructure as Code (Terraform), container security (Docker, Docker Compose), CI/CD security concepts, misconfiguration analysis, cloud threat modeling.
- **Linux & Systems:** Linux system administration, package management, process and service management, shell scripting, security hardening, debugging and performance analysis.
- **AI & Security Automation:** AI-assisted security workflows, integration with LLMs (OpenAI GPT, Meta Llama), agent-based automation, threat analysis augmentation, intelligent parsing and classification systems.
- **Security Tooling:** SBOM and supply-chain security tools (Trivy, Syft), vulnerability scanners, container scanning tools, static analysis concepts, custom tool development.
- **Research & Technical Writing:** Writing research papers, conference papers, and technical documentation; long-form security blogs with 100,000+ cumulative reads; LaTeX for academic and professional documentation.
- **Databases & Data Handling:** SQLite3, JSON-based data modeling, structured logging, dataset preprocessing for security and ML pipelines.
- **APIs & Backend Systems:** REST API design, authentication concepts, secure API development, integration of security and AI services.

Soft Skills:

- **Technical Communication**
- **Problem Solving**
- **Project Ownership**

Team Collaboration
Critical Thinking
Adaptability

EDUCATION

4/2021 - 3/2024 **Bachelor of Computer Applications - Jain (Deemed-To-Be-University)** **Undergraduate**
Scored CGPA - 8.7

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

WORK EXPERIENCE

10/2024 – Present **Cybersecurity Engineer** **Cygne Noir Cyber**

- Develop Python-based backend systems, APIs, and automation tooling across multiple product verticals, with cybersecurity as the primary focus.
- Performing design development sessions with clients to understand and find key development bottlenecks and improve development workflows.
- Design and implement agentic AI workflows and modular control pipelines to support security automation, threat analysis, and research-driven use cases.
- Contribute to architectural design and system structuring for MVP-level projects, ensuring scalability, maintainability, and clear technical boundaries.
- Work hands-on on client-facing and internal demo-ready projects, translating research concepts into production-grade prototypes.
- Support application security testing efforts and contribute to team coordination, documentation, and internal knowledge sharing.
- Actively adapt to new domains beyond cybersecurity, contributing to cross-domain research and automation initiatives.
- Actively involved in intern training and employee training sessions and represented my firm in university talks.
- Involved in guiding the development team to achieve a faster product development life-cycle.
- Implemented Sprint management and advocated for active project management along with performing said product management for a considerable time period.

03/2024 – 10/2024 **Freelance Researcher & Developer** **Independent**

- Designed proof-of-concept implementations for security research, automation workflows, and experimental tooling.
- Developed custom automation scripts for testing, monitoring, and data processing use cases.
- Provided technical writing and review support for research papers, reports, and documentation.

07/2023 – 03/2024 **Offensive Security Engineer Intern** **Avercyber Technologies**

- Performed cloud security assessments across AWS and Azure environments, focusing on misconfigurations and exposure risks.
- Conducted vulnerability research and penetration testing on infrastructure and application components.
- Built and deployed security-focused Infrastructure-as-Code environments using Terraform for testing and research.
- Researched Linux initialization processes, system hardening techniques, and supply-chain security tooling (SBOM).

05/2023 – 07/2023 **Cybersecurity Engineer Intern** **Avercyber Technologies**

- Developed Python-based red team and security automation tools to support assessment workflows.
- Assisted with vulnerability assessments, reporting, and remediation validation.
- Conducted research on AWS security rules and early-stage AI applications in cybersecurity.

PROJECTS

GPT-Vuln-Analyzer **Github Link**

- Python
- AI / LLMs
- Security Analysis

- Built an AI-assisted proof-of-concept for vulnerability analysis using large language models.
- Integrated multiple LLM backends including Llama2, GPT, PaLM, and Ollama for comparative analysis.
- Implemented features such as DNS reconnaissance, subdomain enumeration, and structured vulnerability reasoning.
- Designed the system to be modular and extensible for integration into larger security pipelines.

Startup-SBOM

Github Link

- Python
- Linux
- SBOM

- Reverse-engineered the Linux boot and initialization process to extract startup behavior of system packages.
- Analyzed RPM and DPKG package metadata to identify service initialization and startup persistence.
- Implemented chroot-based inspection to accurately evaluate boot-time behavior without full system execution.
- Produced a structured SBOM-style output highlighting potential startup and persistence vectors.

QuadraInspect

Github Link

- Python
- Mobile Security
- Reverse Engineering

- Developed an automated Android (APK) security analysis framework for vulnerability detection.
- Integrated multiple analysis techniques to inspect permissions, components, and application behavior.
- Focused on scalable analysis and structured reporting for mobile security assessments.
- Designed the framework to support extensibility for future analysis modules.

Brute Framework

Github Link

- Python
- Windows
- Security Framework

- Recreated the core concepts of PentestBox by reverse-engineering its architecture and rebuilding it from scratch.
- Developed an all-in-one Windows-based security testing framework focused on portability and ease of use.
- Implemented centralized tool management with upgrade-friendly and accessible configurations.

Nmap-API

Github Link

- Python
- API Development
- Network Security

- Built a RESTful API wrapper around Nmap as part of a graduation project.
- Enabled programmatic network scanning and result retrieval via structured endpoints.
- Focused on usability, extensibility, and integration with external systems.

HackBot

Github Link

- Python
- AI / LLMs
- Assistant Systems

- Developed an LLM-powered assistant for security-related analysis and information gathering.
- Integrated GPT-based models to assist with code inspection and scan result interpretation.
- Designed the system to support researchers and ethical hackers during analysis workflows.

CVE-LLM-Dataset

Github Link

- Dataset
- LLM Research
- CVE Analysis

- Created a structured dataset as a proof-of-concept for training and evaluating LLMs on CVE-related data.
- Focused on dataset design challenges specific to cybersecurity and vulnerability intelligence.

C2C-Server

Github Link

- Python
- C2
- Red Team

- Developed a command-and-control (C2) server to demonstrate real-world attack and communication patterns.
- Used the project for controlled red-team experimentation and learning scenarios.

WinFiHack

Github Link

- Python
- WiFi
- Windows Internals

- Implemented WiFi brute-force experimentation using native Windows networking libraries.
- Focused on understanding Windows wireless stack behavior and automation constraints.

Komo.do-Hub **Github Link**

- Android
- Containers
- Full-Stack

- Developed a mobile application interface for the Komodo container management platform.
- Worked across frontend and backend components using Java, Node.js, React Native, and React.
- Focused on usability and operational visibility for containerized environments.

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

Cybersecurity & ML

API-Based Network Scanning **Paper Link**
This paper presents an API-driven approach to network vulnerability scanning, based on the implementation and findings of the Nmap-API project. The work focuses on improving stability, usability, and scalability of network scanning systems through structured resource management and virtualized client interactions.

Cybersecurity & ML

AI-Based Enumeration and Exploit Suggester **JETIR**
This research proposes the integration of artificial intelligence into cybersecurity workflows to automate reconnaissance, vulnerability enumeration, and exploit suggestion. The paper explores the feasibility of using AI models to assist in identifying potential attack vectors and prioritizing vulnerabilities.

Cybersecurity & ML

AI in Action: Exploiting the Nexus of Cybersecurity **Paper Link**
This paper examines the role of artificial intelligence in modern cybersecurity environments, with a focus on integrating AI-driven analysis into CI/CD pipelines to enhance security automation, threat detection, and response workflows.

Cybersecurity & ML

Using Autoencoders for Malware Detection **FMDB**
This study investigates the application of autoencoder-based machine learning models for malware detection. The work analyzes how unsupervised learning techniques can be used to identify anomalous behavior in executable and network data.

Cybersecurity & Cloud Computing

Docker-Based Decentralized Vulnerability Assessment **FMDB**
This paper explores a decentralized vulnerability assessment framework built using Docker-based containerization. The approach focuses on distributed scanning, scalability, and the integration of AI-assisted techniques for port scanning and vulnerability analysis.

Network Security & ML

ML-Driven Secure Communication for 6G Networks **Springer**
This work presents a machine learning-driven approach to secure communication in next-generation 6G networks. The paper discusses how ML techniques can enhance security, reliability, and adaptability in emerging high-speed network infrastructures.

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.

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.