

# CHIRANJEEVI G

-  +91 8073761695
-  Bangalore, India
-  Profile Webpage
-  Personal Blogs
-  [chiranjeevi.naidu@proton.me](mailto:chiranjeevi.naidu@proton.me)
-  [github.com/morpheuslord](https://github.com/morpheuslord)
-  [/in/chiranjeevi-g-naidu](https://in/chiranjeevi-g-naidu)

## PROFESSIONAL SUMMARY

Dedicated and detail-oriented cybersecurity engineer with over two years of hands-on experience in system, network, and web application security. Proven track record in reducing security breaches by 20% through comprehensive vulnerability assessments and strategic risk management. Proficient in Python, automation, and AI integration, focusing on developing innovative tools that enhance cybersecurity measures. Demonstrated ability to improve deployment efficiency by 30% through infrastructure security projects on AWS and Azure. Skilled in technical writing with a broad reach, aiding in the dissemination of complex security concepts to a diverse audience. A proactive learner and problem solver, consistently seeking to stay ahead of the latest security trends and technologies to deliver robust and salable solutions.

## SKILLS

### Hard Skills:

- **Programming:** Python for automation, Red Team tool development, shell scripting.
- **Red Teaming:** Web application penetration testing, system exploitation, vulnerability assessments.
- **Network VAPT:** Network enumeration, network exploitation, vulnerability analysis and penetration testing.
- **Cloud Security (AWS):** Infrastructure as Code (Terraform), containerization (Docker, Docker-Compose), G.O.A.T project development, security automation.
- **Linux:** System administration, package management, shell scripting, security hardening.
- **Technical Writing:** Writing technical papers, blog content creation (100,000+ reads on personal blogs).
- **Artificial Intelligence:** Integration with AI models (OpenAI GPT-3, Meta Llama), AI-driven security automation.
- **Security Tools:** SBOM tools (Trivy, Syft), Latex for documentation.

### Soft Skills:

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

## EDUCATION

4/2021 - 3/2024	<b>Bachelor of Computer Applications - Jain (Deemed-To-Be-University)</b> Scored CGPA - 8.7	Undergraduate
4/2018 - 3/2021	<b>PUC(SEBA) - Presidency University</b> Scored 87.6%	PUC

## WORK EXPERIENCE

7/2023 - 3/2024	<b>Offensive Security Engineer</b>	Avercyber Technologies	<ul style="list-style-type: none"><li>• Conducted security assessments and completed prioritization of Azure and AWS infrastructure security tasks, leading to a 25% increase in overall security posture.</li><li>• Developed and deployed 5 G.O.A.T Projects using Terraform, reducing deployment time by 30%.</li><li>• Completed comprehensive research on Linux packages, optimizing initialization processes.</li><li>• Evaluated and tested SBOM tools, improving integration efficiency.</li></ul>
5/2023 - 7/2023	<b>Cybersecurity Engineer</b>	Avercyber Technologies	<ul style="list-style-type: none"><li>• Completed programming projects, developing automated Red Team tools for black-box analysis, and improving threat detection accuracy.</li><li>• Analyzed AWS rules to design security priorities, resulting in a 30% reduction in security incidents.</li><li>• Performed vulnerability assessments on 10 deployments, identifying and mitigating 50 critical vulnerabilities.</li></ul>
2023 - 2023	<b>Freelance Programmer and Content Writer</b>	Worked for clients using Fiverr	<ul style="list-style-type: none"><li>• Automated custom payload generation for Android devices, increasing penetration testing efficiency.</li><li>• Developed and deployed a simple C2 server, reducing setup time by 40%.</li><li>• Wrote 23 blog posts highlighting company services, generating 153,125 reads and 1 year of view time.</li></ul>

## PROJECTS

	<b>Startup-SBOM</b>	<a href="#">Github Link</a>
<ul style="list-style-type: none"><li>• Python</li><li>• Linux</li><li>• Reverse Engineering</li></ul>	<ul style="list-style-type: none"><li>• Reverse-engineered the Linux boot process to extract critical initialization information.</li><li>• Analyzed RPM and DPKG entries to identify startup capabilities of Linux OS packages.</li><li>• Implemented a function to check startup initialization using chroot for accurate boot process analysis.</li><li>• Developed a tool to list potential startup entries with high accuracy.</li></ul>	
	<b>GPT_Vuln-analyzer</b>	<a href="#">Github Link</a>
<ul style="list-style-type: none"><li>• Python</li><li>• AI ( Llama2, GPT3, Palm AI, Ollama )</li><li>• Vulnerability Analysis</li></ul>	<ul style="list-style-type: none"><li>• Developed a proof-of-concept application leveraging AI for precise vulnerability analysis.</li><li>• Integrated AI models such as Meta Llama2, Google Palm AI, and Ollama for comprehensive cybersecurity features.</li><li>• Enabled functionalities like DNS reconnaissance and subdomain enumeration within the tool.</li><li>• Designed the tool to be upgradable and easily integrated with other cybersecurity systems.</li></ul>	
	<b>QuadraInspect</b>	<a href="#">Github Link</a>
<ul style="list-style-type: none"><li>• Python</li><li>• Reverse Engineering</li><li>• Android Testing</li></ul>	<ul style="list-style-type: none"><li>• Developed an Android security analysis framework for comprehensive vulnerability detection.</li><li>• Integrated multiple tools within the framework to achieve precise bug hunting for Android devices.</li><li>• Focused on accurate detection of vulnerabilities and security assessment of Android applications.</li><li>• Enhanced the framework's capability to provide detailed analysis and reporting on security issues.</li></ul>	
	<b>Brute-Hacking-Framework</b>	<a href="#">Github Link</a>
<ul style="list-style-type: none"><li>• Python</li><li>• Batch</li><li>• Reverse Engineering</li><li>• Custom Framework</li></ul>	<ul style="list-style-type: none"><li>• This is a recreation of Pentestbox, this involved reverse engineering the core working of Pentestbox and remaking it from scratch.</li><li>• Developed an all-in-one system framework for all the possible tools compatible with Windows with maximum portability.</li><li>• 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.</li></ul>	
	<b>CVE-LLM_Dataset</b>	<a href="#">Github Link</a>
<ul style="list-style-type: none"><li>• AI ( Llama and GPT)</li></ul>	<ul style="list-style-type: none"><li>• Developed a dataset as a proof of concept for AI training research and the complexities of cybersecurity implementations.</li></ul>	

## CERTIFICATIONS

Valid 6-2023 to 6-2027	<b>Certified Ethical Hacker - V12</b> Successfully completed my CEH V12 Certification.	<a href="#">EC-Council</a>
---------------------------	---	----------------------------

## PUBLICATIONS

Cybersecurity	<b>AI-BASED ENUMERATION AND EXPLOIT SUGGESTER</b> This research is intended to implement Artificial Intelligence with Cyber Security. Our main goal of this research is to make an AI that can gather information and search for the best possible exploits and all the vulnerabilities.	<a href="#">JETIR</a>
Cybersecurity	<b>API Based Network Scanning</b> This paper is written on improving the stability and overall usability of a system involving network vulnerability scanning. This paper involves a resource managing utility over a virtual client to achieve this goal.	<a href="#">MAPANA</a>

## 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.