Pavan Kumar Chinta

College Park, MD | +1(240)-305-5130 | linkedin.com/in/mr-white-hat | pavankumar.chinta@outlook.com | GitHub

Education

University of Maryland, College Park, MD

Master of Engineering, Cybersecurity Engineering — *Jan 2025 — Dec 2026 (Expected)*

Relevant Graduate Coursework: Penetration Testing, Hacking of C Programs & Unix Binaries, Security Tools for Information Security, Cloud Security, Digital Forensics & Incidence Responses, Secure Operating Systems

Professional Experience

Amadeus Software Labs — Feb 2023 — Apr 2024

Security Engineer — Penetration Tester — *Bengaluru, India*

- Executed **25+ penetration tests** across enterprise web, network, and cloud assets, identifying and prioritizing **high severity vulnerabilities**, and leading technical debriefs with engineering teams to validate and mitigate risks.
- Engineered a Python automation pipeline integrating **Qualys vulnerability scans with Jira workflows**, enabling deduplication and real-time ticket generation; streamlined triage and reduced manual tracking by over **15 hours per week**.
- Detected and reported **3 privilege-escalation vectors** within Telefonica SME's endpoint, email, and web-control agents; coordinated vendor response and achieved full patch deployment within **two weeks**.

Skills

Security Testing & Exploitation: Burp Suite, Metasploit Framework, Nmap, OWASP ZAP, Wireshark, Autopsy, Splunk
Programming & Scripting: Python (automation & exploit PoCs), C (low-level analysis), SQL, Bash
Cloud & DevSecOps: AWS — EC2, IAM, S3, GuardDuty, CloudFormation, Microsoft Azure, Docker, Git/GitHub Actions
Web & API Development: PHP, FastAPI, REST APIs
Certifications: eJPT, OSCP (In progress), Google's Technical Support Fundamentals, HackTheBox Dante Pro Lab

Projects & Research

Cloud Security Automation & Threat Detection — Sept 2025

- Detected **35+ misconfigurations** across AWS IAM roles and S3 buckets that could lead to privilege escalation; built **Lambda-based auto-remediation scripts** to enforce least-privilege access and reduce configuration drift by **40%**.
- Integrated **CloudTrail**, **GuardDuty**, and custom Lambda functions to automate **real-time incident detection**, cutting response latency and improving CSPM metrics by **60%**.
- Implemented **NIST 800-53** and **ISO 27001** controls within the automation pipeline, enhancing compliance posture and increasing SOC audit readiness across cloud operations.

Multi-Layered Network Penetration Test & Privilege Escalation — May 2025

- Simulated **red-team attacks** in a 3-tier hybrid (Linux/Windows) lab using **Nmap, SQLmap, and Metasploit**, uncovering **8 detection blind spots** and improving blue-team alert correlation and patch response.
- Executed **5 exploit chains** to demonstrate lateral movement and privilege escalation paths; collaborated with SOC engineers to strengthen segmentation and endpoint hardening measures.
- Compiled findings with **MITRE ATT&CK mapping** and **CVSS scoring**, reducing mean time to detect (MTTD) and mean time to respond (MTTR) by **25%** through tailored incident response recommendations.

OWASP Top-10 Web Application VAPT — May 2022

- Conducted **10+ vulnerability assessments** on production web applications aligned with the **OWASP Top 10 (2021)** framework using Burp Suite, OWASP ZAP, and manual testing to identify injection, XSS, and authentication bypass issues.
- Developed and validated **proof-of-concept exploits** for each finding, assigned **CVSS 3.1 severity scores**, and collaborated with developers to implement verified mitigations improving application resilience.
- Recorded findings with mapped **CWE references** and remediation steps that led to a **60% reduction** in recurring web vulnerabilities across assessed applications.

Volunteer & Leadership Experience

Next Tech Lab — AP — Aug 2021 — Jun 2023

Board Member — Satoshi Division (Cybersecurity & Blockchain) — *Amaravati, India*

- Hosted **12+ Red-Team CTFs and hackathons**, training **150+ students** in exploitation and vulnerability analysis, and coordinating fixes for **6 critical flaws** in university systems to strengthen campus cybersecurity.

Achievements

- Reported **30+ high-impact vulnerabilities** and earned over **$10,000 in rewards**, receiving acknowledgments from Microsoft, GitHub, Mercedes-Benz, Groww, BigBasket, Hashnode, and India's **NCIIPC**.
- Authored the research chapter *"Optimal Deployment of Multiple IoT Applications on Fog Computing"* published by **CRC Press**, proposing a PSO-based IoT resource-allocation algorithm that improved network lifespan by **15%**. Link
- Spearheaded the development of **Edu-MS**, an SMS-based exam platform for low-connectivity regions; secured **first place** in the Edu-Tech Hackathon, beating 50+ competing teams in the 2020 competition.