Manjunath T S

Bangalore, India
☎ +91-8884987355 ✉ crimsonsec11@gmail.com in Manjunath T S Portfolio

Education

Sri Sairam College of Engineering, Bangalore, India
Bachelor of Engineering (Information Science & Engineering), CGPA: 8.4/10 2022–2026

Krupanidhi PU College, Bangalore, India
Pre-University Education, Percentage: 90.16% 2020–2022

Sri Venkateshwara Public School, Bangalore, India
SSLC, Percentage: 93.28% 2019–2020

Experience

Cybersecurity Intern – Cybersapiens
Feb 2025 – May 2025

- Conducted penetration testing on web targets, identifying and documenting security issues.
- Wrote detailed reports about various cybersecurity tools and their effectiveness in real-world engagements.

CTF Player – TryHackMe (Online)
Feb 2024–Present

- Competed in advanced CTF challenges focusing on Active Directory exploitation, privilege escalation, and web application attacks.
- Consistently ranked among the **Top 1% globally on TryHackMe**, solving high-difficulty scenarios under time constraints.

Skills

Offensive Security: Web Application Pentesting, Active Directory Pentesting, Privilege Escalation (Windows/Linux), Network Penetration Testing, Post-Exploitation Techniques

Security Tools: Burp Suite, Nmap, Metasploit, BloodHound, LinPEAS, WinPEAS Wireshark, Nessus, Nikto, Nuclei, SQLmap, XSStrike.

Additional: Vulnerability Assessment, OSINT, Phishing Simulation, Security Reporting.

Certifications

- Certified Red Team Professional (CRTP) – Altered Security
- Practical Junior Penetration Tester (PJPT) – TCM Security
- External Pentest Playbook – TCM Security
- OSINT Fundamentals – TCM Security
- Jr Penetration Tester – TryHackMe
- Google Cybersecurity Professional Certificate – Coursera

Achievements

- **Top 1% on TryHackMe**: Solved 150+ advanced scenarios including Active Directory attacks, privilege escalation, and real-world exploitation labs.
- **Bug Bounty Findings**: Identified 7 verified security vulnerabilities through responsible disclosure:
  - Shopify: 2 Medium Severity (Privilege Escalation)
  - Huntflow: 1 High Severity (Stored XSS), 1 Medium Severity (HTML Injection)
  - Figma: Double Clickjacking
  - Reddit: Double Clickjacking
  - Additional: IDOR vulnerability allowing unauthorized deletion of user blog posts

Projects

ZBOT – AI-Powered Vulnerability Analysis Platform: Developed ZBOT, an intelligent security assistant that consolidates multiple scanning tools (Nmap, OpenVAS, Nessus, Nikto, Nuclei) into one interface. Built ML models to predict attack paths from vulnerability data and automated threat intelligence correlation with NVD, ExploitDB, and Rapid7. Integrated a RAG-based chatbot for natural language queries on vulnerabilities, delivering exploit steps and remediation guidance in real-time. System generates structured reports with CVE IDs, CVSS scores, and actionable security insights.
Tech: Python, RAG/NLP, Nmap, OpenVAS, Nessus, Nikto, Nuclei, Threat Intelligence APIs

HTTP Attack Detection System using ML: Built an ML-based system to detect URL-based cyber attacks in HTTP traffic by analyzing IPDR data. Generated large-scale simulated attack dataset using SQLmap, Burp Suite, XSStrike, and Commix. Trained models to identify 10+ attack types including SQLi, XSS, directory traversal, command injection, SSRF, LFI/RFI, credential stuffing, and web shell uploads. Developed web GUI for attack visualization with PCAP ingestion for real-time threat detection.
Tech: Python, ML/Deep Learning, Wireshark/PCAP Analysis, SQLmap, Burp Suite, XSStrike, Flask/React

Languages

- English: Fluent
- Kannada: Fluent
- Hindi: Intermediate