TRUPTI VIBHUTE

Phone | Email | Portfolio | LinkedIn

SUMMARY

- Cybersecurity Engineer integrating AI into threat detection, log analysis, and security automation workflows.
- Skilled in Python-based data engineering, model training, and deployment using FastAPI, Node.js, and containerized pipelines.
- Working on AI-driven security agents using modular pipelines for log parsing, threat analysis, and automated triage.

EDUCATION

- **Vidyalankar Institute of Technology, Mumbai** **| 2023 - May 2027**
  B.Tech in Computer Science & Electronics — *Honors in Cybersecurity*
  CGPA: 8.5
- **Relevant Coursework:**
  AIML · Network Security · Database Management · SQL · Python · C++ · JavaScript · HTML/CSS

SKILLS

- **Machine Learning & LLM**: Python, Pandas, NumPy, Scikit-learn, PyTorch/TensorFlow, fine-tuning, LLMs, RAG basics
- **Scripting**: Python scripting, Bash, basic SQL
- **Cybersecurity**: Web exploitation, Penetration testing, Burp Suite, Nmap, Wireshark, Metasploit
- **SOC Tools**: SIEM (Splunk/Elastic/Wazuh), IDS (Snort/Suricata), log analysis
- **Backend**: FastAPI, Node.js (Express), REST APIs
- **Cloud/DevOps**: Docker, GitHub Actions (basic CI/CD), Docker Container security and Hardening
- **Automation**: n8n workflows, API integrations (VirusTotal, Shodan)

EXPERIENCE

Web Security & Pentesting (Self-Directed) | May 2025 – June 2025

- Performed hands-on web exploitation including SQLi, XSS, IDOR, SSRF, LFI/RFI, command injection, and authentication bypass.
- Conducted subdomain enumeration, content discovery, and reconnaissance workflows using industry tools.
- Exploited and documented vulnerabilities in OWASP Juice Shop and other lab environments.
- Skilled with Burp Suite for intercepting, fuzzing, and analyzing web traffic.
- Familiar with OWASP Web & API Security standards.
- Technologies: *Burpe Suite, OWASP Top 10, Linux*

Junior Penetration Testing Practice (Homelab) | June 2025 – July 2025

- Executed active and passive reconnaissance using Nmap (basic to advanced scan profiles).
- Used Metasploit for exploitation, session handling, and post-exploitation tasks.
- Deployed bind/reverse shells and performed privilege escalation on Windows & Linux systems.
- Conducted vulnerability research and exploitation in controlled lab setups.
- Technologies: *Metasploit, Nmap, Netcat, JohnTheRipper, msfvenom, ssh, Reverse/Bind Shells*.

SOC & Threat Detection Lab Work (Self-Training) | July 2025 – Nov 2025

- Working with SIEM platforms (*Splunk, Elastic, Wazuh*) for log analysis, alert triage, and threat detection.
- Performed EDR-style monitoring, behavioral analysis, and incident investigation workflows.
- Analyzed network traffic with *Wireshark* and monitored attacks via IDS tools like *Snort/Suricata.*
- Detected web shells, DDoS attempts, brute-force activity, and suspicious process behavior.

PROJECTS

- **Automation & Tooling-** Built n8n automation pipelines for alert enrichment, IOC lookups, and workflow orchestration.
- **Portfolio Website** | Link - Maintained and improved personal cybersecurity portfolio website showcasing projects and writeups.
- **SOC RAG Analyzer**- Generated quick, context-aware explanations of security logs using a local RAG setup built on free, open-source tools.
- **OSINT Recon Automator**- Automated domain intelligence pipeline built in n8n using WHOIS, DNS, CT logs, and a local LLM to generate quick security profiles without paid APIs.
- **PhishGuard** – Email Threat Classifier- Flags suspicious emails using patterns+ NLP + a local LLM model.

CERTIFICATIONS

- **TryHackMe**: Jr Penetration Tester, Web Security Fundamentals, Pre-Security
- **COMPTIA Security+** (Ongoing)
- **Protect** AI: MLSecOps 101 / Foundation
- **Cybrary**: Linux CLI, Linux File System, Network Fundamentals, Nmap, VPN, Wireshark
- **ISC2**: CC (Certified in Cybersecurity)
- **Forage**: Mastercard Cybersecurity Virtual Internship
- **Udemy**: Complete Python Pro Bootcamp