VRUJAHI SUWARE

VAPT ANALYST | PENETRATION TESTER | BUG BOUNTY RESEARCHER

Navi Mumbai, MH 400706 | +91 85919 66521 | vrusuw@gmail.com | Portfolio
LinkedIn: /in/vrujahi-suware | GitHub: /vrusuware

PROFILE SUMMARY

Cybersecurity Analyst specializing in vulnerability assessment and penetration testing (VAPT) across web, network, and cloud environments. Skilled in identifying and exploiting OWASP Top 10 and business-logic vulnerabilities, and producing client-ready reports with clear risk ratings, proof-of-concept, and remediation guidance. Active independent security researcher on HackerOne and Intigriti, with disclosed findings spanning authentication, authorization, and injection classes. Proficient with Burp Suite, Nmap, Nessus/Nemasis, Metasploit, and Wireshark.

EXPERIENCE

VAPT Analyst (CyberSecurity Executive) — *Everence Technologies Pvt. Ltd.* Dec 2025 – Present

- Perform end-to-end vulnerability assessments and penetration tests across client web applications, networks, and infrastructure as part of a professional security consultancy.
- Scan and enumerate enterprise environments to map open ports, running services, and attack surface ahead of manual exploitation.
- Identify and exploit vulnerabilities including OWASP Top 10 issues (injection, broken auth, IDOR, SSRF), business-logic flaws, and misconfigurations across multi-client engagements.
- Author detailed VAPT and forensic-readiness reports with CVSS-based risk ratings, proof-of-concept evidence, and prioritized remediation strategies for client stakeholders.

Cybersecurity Intern — *NIIT Foundation* Jul 2025 – Aug 2025

- Conducted threat detection and vulnerability assessment exercises in guided lab environments.
- Completed hands-on virtual labs and simulations covering core offensive security fundamentals.

INDEPENDENT SECURITY RESEARCH

- Active bug bounty researcher on HackerOne and Intigriti, testing production and private-program targets across fintech, travel, and enterprise networking sectors.
- Disclosed and reported findings spanning authorization bypass, hardcoded/leaked JWTs with elevated claims, SSTI/template-expression injection, and API-level access-control flaws.
- Tested vendor infrastructure APIs (e.g. Citrix NetScaler NITRO) for authorization weaknesses, and web login flows for template-injection and enumeration issues.

SKILLS

Languages: Python, C, JavaScript, HTML, CSS

Tools: Burp Suite, Nemasis DA/VA, Wireshark, Metasploit, sqlmap, Nuclei, Gobuster, FFUF, Uniscan, MobSF

Networking: TCP/IP, DNS, HTTP/HTTPS, Packet Analysis, Port Scanning & Enumeration

Platforms: TryHackMe, Hack The Box, PortSwigger Web Security Academy, DVWA, HackerOne, Intigriti

PROJECTS

- **SIEM / Log Monitoring Tool —** Built a Python-based log monitoring tool for centralized event collection and basic anomaly flagging.
- **Keylogger Tool —** Developed a Python-based keylogger to study input-capture techniques for red-team/awareness training use cases.
- **MAC Changer Tool —** Wrote a Python script to automate MAC address modification for network-identity testing scenarios.

EDUCATION

- **NetTech India —** Post Graduate Diploma in Cybersecurity & Ethical Hacking (Completed, June 2026)
- **University of the People —** Associate Degree in Computer Science (Pursuing)
- **Bhavan's College —** B.Sc IT, 2025 (GPA: 8.78)

ACHIEVEMENTS

- 2nd Runner-Up — Trustoryx Scam Awareness CTF-OSINT Challenge (1st Edition), organized by TrustoryX.
- Ranked #29 — Xsec CTF Season 1.