Satvik Vemulapalli

linkedin.com/in/satvik-vemulapalli contact@satvik.live +91 7993703484 www.satvik.live

Professional Summary

Offensive Security Analyst specializing in web application and network security, vulnerability research, and automated attack workflows. Reported **8–10 validated vulnerabilities** including SQLi, authentication bypass, XSS, IDOR, and payment bypass across real-world applications on Bugcrowd and private programs. Hands-on experience in **Active Directory attacks, AI-assisted exploit automation, recon engineering**, and **C2-driven attack chains**. Founder and technical lead of cybersecurity communities with **600+ members**.

Skills Summary

- **Languages**: Java, Bash, PowerShell, SQL
- **Offensive Tools**: Burp Suite, Nmap, ffuf, gobuster, SQLMap, nuclei, CrackMapExec, Hydra, Hashcat, subfinder, Wireshark
- **Frameworks**: Metasploit, MITRE ATT&CK, MITRE D3FEND, PTES, OWASP Top 10, C2 Frameworks
- **Platforms**: Linux, Windows Server, AWS
- **Core Security**: Active Directory Attacks, Web Pentesting, Red Teaming, Recon Engineering, Detection Evasion Concepts, EDR/XDR Awareness

Experience

- **Bug Hunter – Freelance Security Researcher** *Feb 2025 – Present*
  Bugcrowd, Web Application Security
  - Identified and responsibly disclosed **8–10 confirmed vulnerabilities** across public and private programs.
  - Demonstrated real-world impact including **unauthorized access, account takeover vectors, and sensitive data exposure**.
  - Executed the complete offensive lifecycle from **reconnaissance through exploitation and disclosure**.
- **Cybersecurity Intern – Srida IT Consulting & Services** *May 2025 – June 2025*
  Sysmon, Wazuh SIEM, MITRE ATT&CK
  - Analyzed **1,000+ endpoint events** to identify credential dumping, persistence, privilege escalation, and lateral movement behaviors.
  - Developed **5 custom Wazuh detection rules**, improving signal-to-noise ratio.
  - Correlated defensive telemetry with offensive **TTPs** to understand detection gaps and evasion techniques.

Projects

- **Intelligent Attack Surface & Risk Correlation Platform** *In Progress*
  Risk Mapping, n8n, MITRE ATT&CK, Threat Intelligence
  - Developing an automated pipeline to discover vulnerabilities, assess exploitability, and map findings to MITRE ATT&CK for threat-driven risk scoring.
  - Implementing threat-intelligence enrichment to determine APT relevance, exposure severity, and business impact.
  - Designing executive-ready reports translating technical findings into clear risk narratives for stakeholders.
- **DorkDog – OSINT & Recon Automation** *May 2024 – July 2024*
  Google Dorking
  - Developed an OSINT and reconnaissance automation engine generating **300+ intelligence records per target**.
  - Integrated Nmap, theHarvester, and modular scraping components for attack surface mapping.
- **Custom CTF Hosting Platform (CTFd Alternative)** *Jan 2025 - Feb 2025*
  Full-Stack Platform, PostgreSQL, Automation
  - Designed and developed a custom full-stack platform to host Capture The Flag competitions without relying on third-party solutions.
  - Implemented challenge management, user registration, submissions, scoring, and admin-controlled workflows using a centralized PostgreSQL backend.
  - Enabled flexible, self-hosted CTF operations with improved control compared to off-the-shelf platforms.

Certifications

- **eJPT – INE**: Junior Penetration Tester (Hands-on) - Aug 2025
- **ICCA – INE**: Cloud security, IAM, and network security - Aug 2025

Education

- **Bachelor of Technology (B.Tech) – Computer Science (Cybersecurity)** *2022 – Present*
  GITAM University, Hyderabad *CGPA: 7.64*

Leadership & Community

- **Founder & President – HackOps GITAM**: Founded and led a **200+ member** cybersecurity club; organized workshops and CTFs.
- **President / Secretary / Tech Lead – CySec GITAM**: Managed **400+ members** and delivered hands-on security bootcamps.
- **Technical Author**: Published **50+ cybersecurity write-ups** on HTB, THM, exploitation, and recon.