

Rohit Mishra

Greater Noida, Uttar Pradesh, India

mrohit.cyber@gmail.com — +91-8808855884

GitHub: github.com/mrohitmishra — TryHackMe: tryhackme.com/p/mrohitmishra — Portfolio:
rohitmishra.co.in

Professional Summary

Cybersecurity professional and Computer Science graduate with strong hands-on experience in web application security, vulnerability assessment, and security automation. Proven ability to design tools, perform authorized reconnaissance, and deliver remediation-focused reports. Additionally skilled in independent DevOps and cloud infrastructure practices, including containerization and CI/CD. Seeking full-time opportunities in Cybersecurity, DevSecOps, or Cloud Security roles.

Core Skills

Cybersecurity & VAPT: Web vulnerabilities (IDOR, SQLi, XSS), authentication testing, access control reviews, PoC development, remediation reporting

Security Tools: Burp Suite, Nmap, Wireshark, OWASP ZAP, sqlmap, Metasploit (basic), Scapy

Programming & Scripting: Python, Bash, SQL, C, Java

DevOps & Cloud (Independent Experience): Docker, Kubernetes (fundamentals), Jenkins, AWS (EC2, IAM, S3 basics), Vultr Cloud, Linux administration

Other Skills: Automation, Git/GitHub, report writing, responsible disclosure practices

Professional Experience

Cybersecurity Engineer — Trading Fox

Sep 2024 – Aug 2025

Full-Time — Hybrid Model (Office + Work From Home)

- Designed and developed an automated **Telegram fake-channel detection and bulk-reporting system** using Python and Telegram APIs, significantly improving brand-protection response time.
- Conducted authorized reconnaissance and vulnerability assessments on web applications and digital assets.
- Identified security issues and prepared clear, actionable remediation reports aligned with business impact.
- Created reusable reporting templates and evidence packages to streamline internal security workflows.
- Ensured all activities followed ethical testing standards and responsible disclosure policies.

Independent DevOps & Cloud Experience

- Deployed and managed Linux servers on **AWS and Vultr** for personal projects and learning environments.
- Built containerized applications using **Docker** and managed multi-service setups with Docker Compose.
- Practiced **Kubernetes fundamentals** including pod deployment, services, and basic scaling concepts.
- Implemented **CI/CD pipelines using Jenkins** for automated builds and deployments.
- Focused on security-aware configurations, access control, and monitoring basics in cloud environments.

Selected Projects

Reconnaissance & Security Automation Toolkit (Python)

- Modular toolkit for subdomain enumeration, crt.sh integration, threaded scanning, and structured JSON output.
- Designed for CI-friendly workflows and professional report generation.

Telegram Fake-Channel Reporting System (Python, Telegram API)

- Automated impersonation detection using verification heuristics.
- Implemented bulk reporting and templated takedown documentation.

Education

B.Tech — Computer Science and Engineering
Dr. A.P.J. Abdul Kalam Technical University (AKTU)
CGPA: 8.0 / 10

2021 – 2025

Certifications

- Google Coursera — Foundations of Cybersecurity
- Microsoft — Security Fundamentals
- Forage — Cybersecurity Job Simulations (Mastercard and others)

Labs & Achievements

- Active TryHackMe user with continuous hands-on lab practice and earned badges.
- Performed ethical vulnerability research (IDOR, SQLi, XSS) in authorized environments only.
- Maintains active GitHub repositories with tools, lab-based PoCs, and technical documentation.

Availability

Available for full-time roles. Open to relocation and immediate joining.

Note for Recruiters

All security testing described in this resume was conducted ethically, within authorized environments or lab settings, and follows responsible disclosure practices.