Rohit Mishra

Greater Noida, Uttar Pradesh — +91-8808855884
mrohit.cyber@gmail.com — GitHub: github.com/mrohitmishra
TryHackMe: tryhackme.com/p/mrohitmishra — Portfolio: rohitmishra.co.in

Professional Summary

Ethical cybersecurity practitioner and B.Tech (CSE) student with hands-on experience in web-application security, vulnerability assessment and automation. Daily Solving TryHackMe and Portswigger labs and earned badges. Experienced with reconnaissance, PoC creation, and preparing remediation-focused reports. Seeking a paid internship or entry-level role in VAPT, SOC, or Threat Hunting. All research follows responsible disclosure and lab-authorized testing practices.

Core Skills

Penetration Testing:	Web vulnerabilities (IDOR, SQLi, XSS), auth bypass, access control testing
Tools	Burp Suite, Nmap, Wireshark, OWASP ZAP, sqlmap, Metasploit (basic)
Languages	Python, Bash, SQL, C, Java
Recon & OSINT	Subdomain enumeration, crt.sh, Shodan, passive/active recon workflows
Cloud/Infra	VirtualBox, Docker, Vultr, basic AWS
Other	Automation, Report writing, Responsible disclosure, CI-friendly evidence export

Education

B.Tech — Computer Science and Engineering 2021 – 2025
Dr. A.P.J. Abdul Kalam Technical University (AKTU) CGPA: 8.0/10

Experience

Cybersecurity Intern — Flying Pigeon Solutions / The Trading Fox Sep 2024 – Jan 2025

- Built an automated Telegram fake-channel detection and bulk-reporting tool in Python that reduced manual verification and improved takedown throughput and reporting accuracy.
- Conducted authorized reconnaissance and produced prioritized remediation reports for web vulnerabilities discovered during client engagements.
- Prepared evidence packages and reporting templates suitable for automation and integration with stakeholder workflows.

Selected Projects (High impact)

- **Reconnaissance Toolkit (Python)**
  Subdomain enumeration, crt.sh integration, threaded port scanning wrapper, and structured JSON evidence export for each target. Designed for clean report generation and CI-friendly usage. (Repo: packet_sniffer and Recon repos on GitHub)
- **Telegram Fake-Channel Reporter (Python & Telegram API)**
  Automated detection, verification heuristics, and bulk-reporting workflow with templated takedown reports for brand protection duties.

Certifications

- Google Coursera — Foundations of Cybersecurity
- Microsoft Security Fundamentals
- Forage — Cybersecurity Job Simulation (Mastercard/others)
- Completed multiple vendor and platform micro-credentials (listed in GitHub / portfolio)

Labs & Achievements

- TryHackMe: 9 labs completed, 3 badges.
  Profile: tryhackme.com/p/mrohitmishra
- Performed coordinated, ethical disclosure of IDOR, SQL Injection (SQLi) and Cross-Site Scripting (XSS) findings on multiple government and private websites (PoCs and remediation guidance prepared; testing conducted only within authorized / lab contexts).
- Active GitHub repositories with projects, PoCs (lab-only), and write-ups: github.com/mrohitmishra

Tools & Technologies (quick list)

Burp Suite — Nmap — Wireshark — OWASP ZAP — sqlmap — Scapy — Git — Docker — VirtualBox — Vultr — Linux (Ubuntu)

Availability

Available for paid internships and entry-level roles. Open to relocation and immediate joining. Willing to start on short notice and contribute to hands-on tasks from day one.

Notes for Recruiters

- All security testing described in this resume was performed ethically: on lab environments, with permission, or through responsible disclosure channels. I do not claim to have exploited or exfiltrated private data from production systems.