# Aenosh Rajora

Lucknow, India • +91 8808109748 • rajora.aenosh.0x01@gmail.com • LinkedIn • Github • Website

## Professional Summary

Passionate about ethical hacking, red teaming, and simulating real-world attack scenarios. I build offensive security tools, publish security research, and solve high-difficulty labs on TryHackMe and HTB. Recognized for Strong Collaboration, adaptability, and a fast learning curve, with 20+ CTF writeups and real-world projects. Seeking to contribute to dynamic security teams that value technical depth and creativity are initiative.

## Work Experience

JAN 2024 – PRESENT
**Offensive Security Researcher | Independent**

- Designed and deployed 7+ custom labs replicating real-world attacks (AD, RCE, privilege escalation).
- Built tools for phishing simulation and recon automation; open-sourced on GitHub with active community use.
- Reverse-engineered malware using PyCrypto and sandboxing to extract behavior signatures and flag infection indicators.

FEB 2025 – MAY 2025
**Cyber Security Intern | Hack Secure**

- Conducted reconnaissance, exploited web app flaws (XSS, SQLi, SSRF), and bypassed WAF and authentication mechanisms.
- Developed Python/Bash payloads for privilege escalation and lateral movement in simulated AD environments.
- Documented red team kills chains, evasion techniques, and post-exploitation persistence.

## Projects

- **Ghost Phish:** Engineered a bash-powered phishing simulator with credential harvesting and dynamic tracking.
- **PhantomMist**: Built a stealthy password spraying tool supporting multiple protocols and evasion tactics for red team simulations.
- **Shadow Recon:** Developed an automation tool to streamline subdomain enumeration, OSINT, and asset discovery.
- **VulneraX:** Developed a high-performance rust based scanner to detect and exploit XSS vulnerabilities in web apps.

- **Web Honeypot:** Designed a vulnerable web app to simulate OWASP Top 10 flaws for hands-on attacker behavior analysis.
- **Virus Voyager:** Analyzed and sandboxed malware samples to study behavior, persistence, and detection evasion.

## Technical Skills

- **Languages:** Python, Bash, Rust, JavaScript, SQL
- **Red Team Tools:** Burp Suite, OWASP ZAP, Metasploit, SQLMap, Hydra, Nmap, CrackMapExec, Gobuster, Sublist3r.
- **Security Techniques:** Phishing Simulation, Privilege Escalation, OSINT, Threat Modeling, Web Exploitation (OWASP Top 10), Malware Analysis, Active Directory Attacks.
- **Environments:** Kali Linux, Parrot OS, Windows, Docker, VirtualBox, Git, GitHub
- **Soft Skills:** Communication, Collaboration, Critical Thinking, Fast Learner, Self-Motivated, Problem Solving.

## Education

OCT 2022 – PRESENT (EXPECTED - AUG 2026)

**Bachelor of Technology (B.Tech) | Dr. A.P.J. Abdul Kalam Technical University | Lucknow, Uttar Pradesh, India**

- **GPA**: 7.8
- **Coursework:** Cybersecurity, Data Structures, Algorithm Design, System Programming, Computer Security, UI Design, Database System, Data Analytics, Machine Learning, Web Programming.

## Certification

- CPTS (Certified Penetration Testing Specialist) | HackTheBox| In Progress – Est. Sep 2025
- Google Cybersecurity Professional Certificate – Google/Coursera

## Achievements

- Published 20+ detailed cybersecurity write-ups on with 3k+ views on Medium.
- Achieved **rank** 348 at TryHackMe and **rank 842** on HackTheBox.
- Consistently participated in national and international Capture The Flag (CTF) events.
- Develop security tools such as automating red recon, phishing simulation.