

Utkarsh Barethiya

Dublin, IE | P: +353 089XXXX77 | utkarshXbarXXXXXX@gmail.com | [LinkedIn](#) | [Github](#) | [Portfolio](#)

PROFESSIONAL SUMMARY

Information Security Engineer / Offensive Security Engineer with 2.5+ years of experience in **penetration testing, vulnerability assessment, API security testing, and Active Directory penetration testing** across enterprise and financial environments. Proven ability in **network security testing, internal network penetration testing, risk assessment, and security reporting**, aligned with **MITRE ATT&CK** and **OWASP Top 10**. Certified CRTP, CEH, eJPT, with CTO in progress, focused on improving organizational security posture and supporting compliance and remediation initiatives.

EXPERIENCE

Anzen Technologies Pvt Ltd. – India, Navi Mumbai

Security Consultant / Penetration Tester

Aug 2022 - Dec 2024

- Led **penetration testing** and **vulnerability assessment** engagements for a top stock exchange client, performing **web application, API, network, and Active Directory penetration testing** across enterprise environments.
- Conducted **API security testing** and **internal network penetration testing**, identifying authentication flaws, authorization bypasses, Kerberoasting, privilege escalation, and lateral movement aligned with **MITRE ATT&CK**.
- Assessed **large-scale environments (1,000+ internal and external IPs)** for a leading banking client, delivering detailed risk-based remediation recommendations based on SAST and DAST.
- Collaborated with **SOC and Blue Team** members during **purple team exercises and cyber drills** to improve detection, response, and alerting capabilities.
- Identified, validated, and documented **30+ high and medium-risk vulnerabilities** across **20+ enterprise applications and infrastructure assets**, reducing remediation turnaround time by **20%**.
- Developed **proof-of-concept exploits and attack paths**, clearly demonstrating technical and business impact to stakeholders.
- Supported **CERT-In-empanelled security assessments**, ensuring compliance with national cybersecurity standards.

BUG BOUNTY & RESPONSIBLE DISCLOSURE:

- Identified and responsibly disclosed security vulnerabilities in production systems of organizations including **Dell, Swiggy, BigBasket**, and others.
- Received multiple **Hall of Fame recognitions** for responsible disclosure contributions.

TECHNICAL SKILLS

- Offensive Security:** Penetration Testing, Vulnerability Assessment (VAPT), Red Teaming, Adversary Simulation, Purple Teaming.
- Web & API Security:** OWASP Top 10, Authentication & Authorization Testing, Business Logic Flaws.
- Network & AD Security:** Active Directory Exploitation, Privilege Escalation, Lateral Movement.
- Frameworks:** MITRE ATT&CK.

TOOLS & TECHNOLOGIES

BurpSuite, Metasploit, Nmap, Nessus, Tenable, Mimikatz, BloodHound, SharpHound, Wireshark, SQLMap, etc.

EDUCATION

MSc in Cyber Security (Pursuing)
Dublin Business School, Dublin, Ireland

04/2025 – Present (Expected Completion: Apr 2026)

CERTIFICATIONS

- **Certified Red Team Operator (CRTO)** – Zero-Point Security | **In Progress**
- **Certified Red Team Professional (CRTP)** – Altered Security
- **Junior Penetration Tester (eJPT)** – eLearnSecurity
- **Certified Ethical Hacker (CEH v11)** – EC-Council