

# AKSHAT PARIKH

akshatparikh.pt@gmail.com | +91 8401685272 | <https://akshatsecurity.com>  
<https://www.linkedin.com/in/akshatparikh-pt/>

## PROFESSIONAL SUMMARY

A Penetration Tester and Security Consultant with over a year of experience specializing in vulnerability identification and risk assessment. I use hands-on testing to uncover a wide range of security weaknesses and provide clear, actionable guidance to help companies reduce their overall security risk.

## TECHNICAL SKILLS

**Domains:** Web Application Penetration Testing (OWASP Top 10), Network Penetration Testing, Vulnerability Assessment

**Cloud & Infrastructure:** AWS Security, Active Directory Penetration Testing

**Security Tools:** Burp Suite, Nmap, Metasploit, Bloodhound, Nessus, OWASP ZAP, Hydra, Splunk

**Scripting Languages:** Python and Bash

## EXPERIENCE

### Freelance Penetration Tester/Security Consultant (Contract)

April 2025 – Present

- **Comprehensive Security Assessments:** Assessed the security posture for 4 companies, identifying and reporting over 13 distinct vulnerabilities across web application and network environments.
- **Critical Vulnerability Remediation:** Uncovered and helped remediate numerous critical-risk vulnerabilities, including Broken Access Control and Security Misconfiguration, leading to immediate and significant security upgrades for clients.
- **Actionable Security Reporting:** Delivered clear and actionable reports detailing findings, business impact, and strategic recommendations that enabled technical teams to quickly patch vulnerabilities.

### Penetration Tester | Opal Omniventures Pvt. Ltd.

July 2024 – March 2025

- **Social Engineering & Awareness Campaigns:** Reduced employee susceptibility to phishing by over 70% by leading targeted phishing campaigns for teams of 50-150, reducing the average click-rate from over 25% down to under 10%
- **Inter-Company Security Engagements:** Served as the sole penetration tester across 3 separate partnered companies, providing detailed vulnerability findings to help improve their security.
- **Web Application Penetration Testing:** Conducted in-depth application assessments, identifying vulnerabilities including SQL injection and a critical file upload flaw that could have led to remote code execution, thereby preventing a major security breach.

### Penetration Tester | MCS Ventures

January 2024 – July 2024

- **Web Application Penetration Testing:** Identified multiple high-impact vulnerabilities, including Cross-Site Scripting (XSS) and SQL Injection, which could have led to the widespread exposure of sensitive customer data.
- **Network Security Hardening:** Strengthened network security by identifying and reporting the use of weak default credentials on a core system, eliminating a key entry point for attackers.
- **Vulnerability Reporting & Remediation Support:** Delivered a series of reports with clear, step-by-step guidance, enabling the development team to consistently patch a wide range of vulnerabilities.

## EDUCATION

L.J.I.E.T. – Bachelor's in Information Communication and Technology Engineering

7.87 CGPA | 2021 – 2024

R.C.T.I. – Diploma in Computer Engineering

7.88 CGPA | 2018 – 2021

## CERTIFICATIONS & CERTIFICATES

- CRTA (Certified Red Team Analyst) • CompTIA Pentest+ (THM) • Jr Pen Tester (THM) • Ethical Hacking (Udemy)

## PROJECTS & ACHIEVEMENTS

**TryHackMe:** Ranked in the top 0.1% of global users by completing over 600 hands-on labs, demonstrating a commitment to continuous skill development with a 400+ day learning streak

**HackTheBox:** Achieved "Pro Hacker" rank and the highest seasonal rank of "HOLO" while actively advancing skills through the Certified Penetration Testing Specialist (CPTS) and Certified Bug Bounty Hunter (CBBH) learning paths.

**Bug Bounty:** Discovered and responsibly disclosed a critical unauthorized account access vulnerability to a private company

**Python Tool Development:** Developed scripts for keylogging, subdomain/directory enumeration, and network scanning to automate security testing