




MOHAMMED AFROZE

Junior Penetration Tester

 [LinkedIn](#)

 Hyderabad, India •  +91 8978072164 •  mohammedaffroze.h3@gmail.com

PROFESSIONAL SUMMARY

Detail-oriented Junior Penetration Tester with a year of experience specializing in web application security testing, vulnerability management, and threat analysis. Skilled in identifying OWASP Top 10 security risks, delivering CVSS analysis-based security reports, and executing full VAPT cycles. Proficient in manual testing, automation tools, and remediation tracking. Eager to enhance secure SDLC practices within a dynamic, security-focused setting.

TECHNICAL SKILLS

Pentesting Tools: Burp Suite expertise, Skilled in using OWASP ZAP, Nmap, Nikto, sqlmap, XSSStrike, FFUF, Postman, openVas, Nessus, Qualys

Cloud & Container Security: Familiar with AWS S3 misconfigurations, IAM roles, Azure App Services, Docker environments

Languages: Python, JavaScript, HTML, CSS

Operating Systems: Windows, Linux, Kali, Ubuntu

Concepts: Knowledge of OWASP Top 10 security risks, Red Teaming, Vulnerability Reporting, Vulnerability Assessment and Exploitation, CVSS Analysis

Others: Git, Wireshark, TryHackMe, PortSwigger Labs

PROJECTS

1. Web Application Pentest (Confidential)

- Conducted VAPT on enterprise-level web applications using manual and automated tools.
- Identified 15+ XSS and SQLi flaws; rated 5 as critical (CVSS \geq 8).
- Delivered detailed technical reports with PoC links, risk summaries, and mitigation steps.
- Tools used: Burp Suite, sqlmap, dev tools, OWASP ZAP.

2. Secure Login Portal Testing (Confidential)

- Tested login and session flows, discovered IDORs and session fixation flaws.
- Detected improper cookie security and forced browsing issues.
- Documented findings in CVSS v3 format with risk impact.

3. Miscellaneous VAPT Projects (50+ apps)

- Audited diverse stacks: PHP, Node.js, Django-based web apps.
 - Discovered misconfigurations like directory listing and verbose error leaks.
 - Helped teams close 80% of reported bugs before go-live.
-

EXPERIENCE

Junior Penetration Tester

KIIS (Subsidiary of Kleep Technologies) • Jan 2024 – Present

- Executed 50+ web app pentests, focusing on OWASP Top 10 security risks and business logic flaws.
 - Created CVSS analysis-based technical and executive reports with actionable mitigation.
 - Simulated real-world attack scenarios and supported secure patching efforts.
 - Improved coverage in bug bounty targets through fuzzing and manual parameter tampering.
-

EDUCATION

Computer Science Engineering

Jawaharlal Nehru Technological University (JNTU), Hyderabad • 2021 - 2024

CERTIFICATIONS

- KLEAP Certified Penetration Tester
 - Cisco Networking: Introduction to Cybersecurity
 - Web Application Security Fundamentals (PortSwigger)
-

VULNERABILITY COVERAGE

- SQL Injection (Boolean, Error, Time-based)
 - Cross-Site Scripting (Reflected, Stored, DOM-Based)
 - CSRF (Token bypass, Cookie-based)
 - IDOR (Horizontal and Vertical Privilege Escalation)
 - CORS Misconfigurations
 - Broken Authentication & Session Management
 - Security Misconfigurations
 - Open Redirects, Insecure File Uploads, Unvalidated Input Fields
-

ACHIEVEMENTS & ACTIVITIES

- Winner – KLEAP Cybersecurity Hackathon (Bug bounty track)
 - Disclosed 20+ bugs in private programs with proof-of-concepts
 - Built PoCs for CSRF, XSS, and logic bypass and shared internally for training
 - Practiced daily on TryHackMe, Burp Academy, and internal testbeds
 - Created automation scripts using Python and Burp extensions for repeat tasks
-

SOFT SKILLS

Attention to Detail • Problem Solving • Technical Documentation • Communication • Team Collaboration