

Mokksh A Parekh

Penetration Tester | Mobile (Android & iOS), Web, API & Thick Client Security Testing

Chennai, Tamil Nadu, India · maparekh11@gmail.com · +91 8667504887 · linkedin.com/in/mokksh-parekh · mokksh.netlify.app

SUMMARY

Penetration tester specializing in gray-box and black-box security testing of Android and iOS, web, API, and thick client applications, with hands-on mobile SAST/DAST, reverse engineering, and bypass of SSL pinning and root/jailbreak detection using Frida, objection, and Magisk. Tests against OWASP Top 10, OWASP API Security Top 10, and OWASP MASVS/MASTG. Credited researcher behind 6 published CVEs; LPT (Master), CPENT, and CEH (Master) certified.

EXPERIENCE

Security Analyst

TechDefence Labs Solutions Limited

August 2025 – Present | Ahmedabad, India

- Executed 45+ gray-box and black-box penetration tests across web, mobile (Android and iOS), API, thick client, network, and Active Directory environments, including red team engagements.
- Performed static and dynamic analysis of Android APKs and iOS IPAs using MobSF, jadx, apktool, dex2jar, adb, otool, and plutil, uncovering insecure data storage, hardcoded secrets, insecure configurations, and parameter tampering.
- Reverse engineered mobile binaries and native libraries (.so/.dylib) and bypassed SSL pinning, root/jailbreak detection, obfuscation, and tamper checks using Frida, objection, Magisk, and Xposed.
- Tested web applications, REST APIs, and thick client applications manually with Burp Suite and OWASP ZAP against OWASP Top 10 and OWASP API Security Top 10, scoping each assessment and designing test scenarios.
- Performed SAST/DAST and configuration reviews, identifying 400+ vulnerabilities and documenting each with proof-of-concept evidence and risk-rated remediation guidance for development teams.

Security Analyst Intern

TechDefence Labs Solutions Limited

December 2024 – July 2025 | Ahmedabad, India

- Executed 30+ security assessments across web, API, mobile, network, and Active Directory environments, including VAPT and red team activities.
- Identified 50+ vulnerabilities through SAST/DAST scans and configuration reviews, and validated and documented findings with proof-of-concept evidence across 20+ engagements.

VULNERABILITY RESEARCH & BUG BOUNTY

Credited with 6 CVEs in WordPress and npm software (1 Critical, 3 High, 2 Medium) covering OWASP Top 10 injection and broken access control flaws, coordinated through Patchstack, WPScan, and Snynk.

- **CVE-2026-56070**: Unauthenticated SQL injection in Advance Product Search plugin | CVSS 9.3 Critical
- **CVE-2026-13613**: Authenticated SQL injection via REST API in KiviCare plugin | CVSS 8.8 High
- **CVE-2026-11572**: OS command injection in degit npm package (co-discovered) | CVSS 8.7 High
- **CVE-2026-12877**: Unauthenticated SQL injection in Project Management, Bug and Issue Tracking | CVSS 8.6 High
- **CVE-2026-15153**: Authenticated SQL injection in WP Hotel Booking plugin | CVSS 6.8 Medium
- **CVE-2026-18777**: Unauthenticated broken access control in TrueBooker plugin | CVSS 5.3 Medium

Bug Bounty Hall of Fame: Allcargo Group, Tata Motors, Sai Life Sciences, and Wibmo (Com Olho); KOMOJU (YesWeHack); YesWeHack Dojo challenge hall of fame

EDUCATION

Bachelor of Engineering and Technology, Computer Science and Engineering (Major in Cybersecurity)

Parul University, Gujarat, India | 2021 – 2025 | CGPA 8.22/10.0

CERTIFICATIONS

- **Licensed Penetration Tester (LPT Master)** | EC-Council | 2026
- **Certified Penetration Testing Professional (CPENT)** | EC-Council | 2026
- **Certified Ethical Hacker (CEH v12 Master)** | EC-Council | 2025
- **Certified AppSec Practitioner (CAP)** | The SecOps Group | 2024
- **APIsec Certified Practitioner (ACP)** | APIsec University | 2025
- **Certified Network Security Practitioner (CNSP)** | The SecOps Group | 2025
- **Certified Red Team Analyst (CRTA)** | CyberWarFare Labs | 2025
- **Microsoft Certified: Security, Compliance, and Identity Fundamentals** | Microsoft | 2022

SKILLS

Mobile Security: Android and iOS penetration testing, static and dynamic analysis (SAST/DAST), reverse engineering, runtime hooking, SSL pinning bypass, root/jailbreak detection bypass, OWASP MASVS/MASTG

Application Security: Web, API, and thick client penetration testing, gray-box and black-box testing, manual security testing, security test design, source code review (SAST), OWASP Top 10, OWASP API Security Top 10

Mobile Tools: Frida, objection, Magisk, Xposed, MobSF, jadx, apktool, dex2jar, adb, Xcode, otool, plutil, Cydia, Sileo, Zebra

Web & Network Tools: Burp Suite, OWASP ZAP, Kali Linux, Nmap, Metasploit, BloodHound, ADCS, CrowdStrike EDR

Scripting: Python, Bash