MOHAMMED ABDUL KAREEM

✉ *MohammedAbdulKareem247@Gmail.com | ✆ +1(773) 800-4273| 💻 https://linkedin.com/in/1337iMAK*
https://github.com/0xiMAK | Portfolio: *https://0ximak.github.io*

Application Security Engineer and Offensive Security Specialist with over 6 years of hands-on experience in web, mobile, network, and Wi-Fi penetration testing across diverse industries. Skilled in conducting black-box, grey-box, and authenticated assessments, identifying complex vulnerabilities, and simulating real-world attack scenarios.

Experienced in driving product security efforts—performing threat modelling, design/code reviews, secure architecture assessments, and integrating SAST, DAST, and SCA into CI/CD pipelines. Strong contributor to internal and external bug bounty programs, with a proven record of identifying critical issues in production and clou d-native environments.

Also passionate about cybersecurity education—leading CTFs, hands-on labs, and secure coding trainings. Known for effectively bridging engineering, security, and leadership teams through clear communication and actionable security guidance. Currently pursuing a Master's in Computer Science and Engineering (2023–2025).

SKILLS & EXPERTISE

- Web Application Security
- Mobile App Security (iOS & Android)
- Secure Code Review
- GenAI & LLM Security
- Secure SDLC & DevSecOps
- Network Pentesting & VAPT
- Threat Modeling & Risk Assessment
- CI/CD Security (SAST/DAST)
- Red Teaming & Bug Bounty
- AWS Cloud Security

PROFESSIONAL EXPERIENCE

Product Security Engine *Dec 2021–June 2023*
Loyalty Juggernaut

- Led end-to-end security reviews across the SDLC, covering architecture, design, source code, and deployed systems for web, mobile, API, and cloud applications.
- Partnered with DevOps to integrate automated security tools (SAST, DAST, SCA) into CI/CD pipelines, enabling scalable and continuous vulnerability detection.
- Conducted monthly AWS security audits and Docker/ECR container assessments, reducing cloud and container vulnerabilities through mitigation strategies.
- Performed DAST analysis and penetration testing for web, mobile, and API applications; conducted risk analysis using CVSS scoring and recommended remediation aligned with OWASP and SANS best practices.
- Reviewed SCA results (GitHub, AWS ECR, Snyk), created tickets, and coordinated with engineers to ensure timely resolution in compliance with ISMS policies.
- Prepared threat profiles, test plans, and comprehensive assessment reports with actionable remediation strategies.
- Delivered security training, mentorship, and secure design guidance to engineering teams, strengthening a security-first culture and improving secure coding maturity.
- Supported compliance initiatives including ISO 27001 and PCI DSS; contributed to RFPs and partner security questionnaires.
- Developed educational PoC videos and reports to raise organizational security awareness; facilitated quarterly security reviews to assess posture and address engineering concerns.
- Led and completed third-party vulnerability assessments (VAPT) to validate and strengthen overall security posture.
- Implemented processes and controls to eliminate entire classes of vulnerabilities, driving continuous improvement in product resilience.

Penetration Tester, *Sep 2018–Dec 2021*
TrekShield

- Performed comprehensive penetration testing of web applications, APIs, mobile apps (Android & iOS), internal/external networks, wireless environments, and thick client applications.
- Led vulnerability assessments and security testing engagements for 100+ clients across BFSI, healthcare, telecom, retail, and education sectors.
- Executed black-box, grey-box, and authenticated security assessments using both manual techniques and tools like Burp Suite, Nmap, Metasploit, Wireshark, Nessus, and MobSF.
- Developed test plans, defined engagement scope, and created threat profiles to guide business logic testing and infrastructure assessments.
- Conducted risk analysis using CVSS scoring and provided cost-effective remediation aligned with OWASP and SANS best practices.
- Delivered high-quality security reports with detailed findings, proof-of-concept exploits, and prioritized risk mitigation strategies.
- Engaged directly with clients for scoping, progress updates, remediation support, and final security walkthroughs.
- Led internal team of analysts, ensured project quality, and managed timelines for multi-phase testing projects.
- Conducted regular internal network audits and supported secure design and architecture reviews.
- Contributed to responsible disclosure and 0day reporting on public platforms, and won multiple CTF competitions at security conferences.

EDUCATION

Campbellsville University *2023 – 2025*
Master of Science – MS, Computer Science

TRAININGS & CERTIFICATIONS

- OWASP Top 10 Mastery Badge – TryHackMe
- Completed All Learning Paths – PortSwigger Web Security Academy
- iOS & Android Penetration Testing – MobileHackingLabs

HONORS & AWARDS

- Winner – CTFs at AppSecVillage (1st Place, Golden Coin), NULLCON 2020 (Top 10), and n|u Hyderabad 100th Meetup (1st Place).
- Recognized in Telangana’s 1st Live Hacking Event for reporting critical flaws in government web/mobile apps.
- Credited with 0day CVEs: ***CVE-2018-19914 & CVE-2018-19915***.
- Acknowledged by 50+ global organizations (e.g., NASA, Microsoft, Intel, SAP, Sony) for vulnerability disclosures via bug bounty & VDPs.
- Active contributor to OWASP and Null communities through CTFs, workshops, and public engagements.