JOB DESCRIPTION – SECURITY RESEARCHER- ANDROID

About HackIT

HackIT Technology and Advisory Services is an IT / Cyber Security company, operating since 2009. HackIT is an Indian Computer Emergency Response Team, CERT-IN (www.cert-in.org.in) empaneled provider for IT Security Audit Services. HackIT provides a broad range of security consulting and advisory services to a diverse group of clients, including government organizations, corporations, Military establishments, financial institutions and start-ups, to name a few. Our work spans multiple sectors and industries, including Telecommunications, Defense and Military, ITeS, Financial Services, Aviation, Hospitality, Healthcare and Research. We work end-to-end—from diagnosis to delivery of lasting impact — together generating tangible results that are improving the security posture of organizations worldwide.

Job Title	• Security Researcher- Android
Location	• Delhi

Job Overview

We are seeking a detail-oriented Security Researcher- Android to support our mobile security research, red teaming, and penetration testing initiatives. The role involves analyzing Android applications and malware, performing reverse engineering, identifying vulnerabilities and developing proof-of-concepts for security weaknesses. The ideal candidate should have strong Android development fundamentals combined with deep interest in mobile security and low-level analysis.

Job Responsibilities

- Perform Android application security assessments, including static and dynamic analysis.
- Conduct reverse engineering of Android applications and mobile malware.
- Analyze malicious Android applications to identify behavior, persistence and impact.
- Identify, validate, and exploit mobile security vulnerabilities.
- Develop proof-of-concepts (PoCs) for discovered vulnerabilities and research findings.
- Build or customize tools and scripts to support mobile security testing and research.
- Support red teaming and penetration testing engagements involving mobile platforms.
- Stay updated with emerging mobile threats, vulnerabilities and attack techniques.
- Prepare detailed technical reports and present findings to internal teams and clients.
- Assist in delivering capacity-building and knowledge-sharing sessions when required.

Technical Skillsets (Mandatory)

- Strong experience in Android application development and reverse engineering.
- Hands-on expertise in Android malware analysis.

- Good understanding of low-level concepts and assembly language (ARM preferred).
- Solid knowledge of mobile security concepts, Android OS internals and application sandboxing.
- Familiarity with OWASP Mobile Top 10 vulnerabilities.
- Working knowledge of Linux environments and command-line tools.
- Android Application Modification (APK / KPK Patching)

Technical Skillsets (Preferred)

- Experience with tools such as JADX, APK Tool, Frida, Drozer, Burp Suite, Ghidra, IDA or similar.
- Knowledge of cryptography concepts and secure mobile communication.
- Understanding of network protocols and mobile traffic analysis.
- Exposure to penetration testing methodologies and security frameworks.
- Experience in scripting using Python, Bash or similar languages.

Non-Technical Skillsets

- Strong analytical and problem-solving skills.
- Good technical documentation and report-writing abilities.
- Ability to work independently and as part of a team.
- High level of integrity and discretion while handling sensitive information.

Education and Certifications

- Bachelor’s degree in Computer Science, Information Technology, or a related field.
- Relevant security certifications are a plus.

Experience

1–2 years of experience in Android application development or a related information security field.

Send your updated profiles to **careers@hackit.co**