Mohammad Kaif

Bachelor of Technology
Computer Science and Engineering
Dr. A. P. J. Abdul Kalam Technical University,
Lucknow

+91 (966)390-8353
kaif2k17@gmail.com
mohammad-kaif-security
https://hackerone.com/kaif0x01
kaif0x01
Medium Blogs

Education

Dr. A. P. J. Abdul Kalam Technical University, Lucknow **2022 – 2026**
Bachelor of Technology in Computer Science and Engineering

Technical Skills and Interests

Languages: Python, Javascript, Bash
Tools and Technologies: Git, Linux, Jadx, Burp suite, WireShark
Interests: Android Security, API Security,Web APP Security,AI Security, Bug Bounty, Web Pen-testing

Experience

Independent Security Researcher @ Apple **2025 – Present**
Apple Security Bounty Program

- Performed responsible vulnerability research on Apple core apps (App Store, Music (iTunes) etc.). A critical **Account Takeover via App Store** issue was responsibly disclosed to **Apple Security Team** with exploit code and POC.
- The issue was fixed in a single day and asked for retest,I found a unique bypass and reported it to the team. Again quickly fixed by Apple Security Team and rewarded with ***$15,000 USD*** bounty for my responsible disclosure.
- Responsibly disclosed **2 unique CSRFs** affecting App Store and iTunes (Music) exploited via **itmss://** scheme. Affecting **Billing Information of Users' Apple Account** and rewarded with ***$5,000 USD*** bounty each from Apple Security Team.
- Found and exploited an issue affecting iTunes (Music) macOS app which allows any website to be loaded into **iTunes(Music) internal webview** and got access to **iTunes** javascript bridge method. Getting access to crucial account information of users' Apple Account such as ***dsId, email, guid, User first Name, last Name, Machine ID etc.***
- **Exposure**:Working of Apple's custom url schemes, Exploit development, Co-ordination , iOS and macOs security research.

Independent Security Researcher @ Tecno Mobile **2021 – 2025**
Tecno Security Response Center

- Performed security research on Tecno Mobile's critical business apps: **TECNO SPOT** *(500 Millions+ Downloads)*, **Boomplay** *(100 Millions+ Downloads)*, **Tecno ID**, **Tecno Cloud** *(Pre-Installed App)*, and other pre-installed apps.
- Reverse Engineered android apps using **JADX** and **apktool** and exploited API vulnerabilities using Burp Suite, resulting in significant security vulnerabilities in the target apps: **PIIs leakage, Account Takeovers, IDORs** in primary functionalities
- Exploited a **critical API** vulnerability affecting pre-installed **device configuration app** [**com.hoffnung**]. It fetched device config values from API and used in various device ops, exploited the API to **modify all the config values**.
- Responsibly disclosed total of **120 vulnerabilities** of which **74** reports are accepted and rewarded. Severity wise, **Critical Vulnerabilities: 14 , High Vulnerabilities: 29, Medium Vulnerabilities: 23** and **Low Vulnerabilities: 8**
- **Exposure**: Java, JADX, Reverse Engineering, Android security, API Security

Independent Security Researcher @ HackerOne
kaif0x01

- Worked on bug bounty programs hosted on HackerOne, some of them are **Xiaomi, Zomato (Eternal), Private Program**.
- Responsibly disclosed 6 vulnerabilities to **Xiaomi** (**4 accepted**), **1 valid** in **Zomato**, and **7 valid** in a **Private Program**.
- Stats: **7.00 Signal**, 94th Percentile, **24.69 Impact**, **607** Reputation.

Independent Security Researcher @ OPPO **2019 – 2021**
OPPO Security Response Center

- Performed security research on OPPO's web and mobile assets including **OPPO Store, ColorOS Community, Realme Paysa, Realme Community** and other business-critical apps.
- Discovered **Stored XSS** in **ColorOS Community**, **IDOR** in **Realme Community** enabling **deletion of all user posts**, and **CORS misconfiguration** in **OPPO Store** leaking **users' sensitive information**.
- Found multiple vulnerabilities in **Realme Paysa** (financial services app) including **Source Code leakage** via **insecure Docker Registry API** and **Account Takeover** by forging JWT tokens using **none algorithm** to impersonate users.
- Secured **OPPO's internal source code** from leakage due to **misconfigured Harbor Registry** with public read access, exposing **100+ Docker images** containing proprietary application code.
- **Exposure**: Docker Registry, Harbor, Android Security, Jadx, Android Reversing, API Security

Honors and Achievements

- Received my highest individual bug bounty of *15,000 USD* by the Apple Security Team.
- Got **acknowledged** by **Apple Security** Team in security content of **iOS 26.4 and iPadOS 26.4** for reporting a security vulnerability in the **Music** app which was fixed in the update. *https://support.apple.com/en-in/126792*
- Listed on **Apple's Hall of Fame** page **2 times** in **2026** (in February and January 2026) and **2 times** in **2025** (September and January 2025). *https://support.apple.com/en-us/102774*
- Listed on **Apple's Hall of Fame** page in **July 2023**. *https://support.apple.com/en-us/122162*
- **Top 1** Ranked **Security researcher** of **TECNO** Security Response Center in **2024,2023,2021** *leaderboards(mkahmad)*
- **Top 2** Ranked **Security researcher** of **TECNO** Security Response Center in **2022**.*leaderboards (mkahmad)*
- **Top 1** Ranked **Security researcher** of **OPPO** Security Response Center in **2021**. *leaderboards (mkahmad)*
- **Top 1** Ranked **Security researcher** of **OPPO** Security Response Center in **2020**. *leaderboards (mkahmad)*
- **Top 2** Ranked **Security researcher** of **OPPO** Security Response Center in **2019**. *leaderboards (mkahmad)*