Akilesh Kumar

LinkedIn: linkedin.com/in/aki007 **Email:** akihaxor@proton.me

PROFESSIONAL SUMMARY

Cybersecurity specialist with over 4 years of hands-on experience in offensive security, focusing on web application, Android, and API penetration testing. Expertise in vulnerability discovery, reverse engineering, and creating unique exploit chains. Passionate about knowledge sharing, I presented technical workshops and hands-on training sessions at prominent security conferences such as BSides Kerala 2025 and SINCON 2025. Actively participates in the security community through CTFs, bug bounty programs, and internal research efforts. Seeking to use extensive technical knowledge and a solid research background to contribute to cutting-edge security solutions.

SKILLS

- Security Testing: Web App, Android, API
- Scripting/Programming Languages: Bash, Python, PHP, Java, JavaScript, C
- Query/Data Languages: SQL, SQLite
- Tools: Nmap, BurpSuite, Sqlmap, Metasploit, Wireshark, Frida, MobSF, Jadx, GDB, Ida, Ghidra, dnSpy
- Reversing: Binary Exploitation, Reverse Engineering
- Hardware: Raspberry Pi, Arduino, RTL_SDR, Node MCU
- Troubleshooting: Laptop & PC's

ACHIEVEMENTS

- Hall of Fame - Ebay (2019)
- Bounties - Zerocopter (2021 & 2022)

TALKS & WORKSHOPS

- **"Breaking and Securing Android Apps" – BSides Kerala 2025**
  Speaker & Workshop Conductor. Delivered a hands-on session on analyzing and exploiting real-world Vulnerabilities through CTF based challenges, focusing on reversing, Frida, and dynamic attack surfaces.
- **"Unlocking Android Apps: A Deep Dive into Hacking and Security" – Sincon 2025**
  Delivered an in-depth hands-on session on analyzing and exploiting real-world Android vulnerabilities, write an exploit for existing CVE (Dirty Stream Android).

PROFESSIONAL EXPERIENCE

Security Researcher - TRABODA CYBERLABS PVT LTD - 06/2022-Present
Worked on multiple offensive security projects involving deep technical research and assessments across web, Android, and API attack surfaces. Contributed to custom Android challenge creation, vulnerability discovery, and internal security tooling.

- Conducted offensive web application and API testing on real-world client infrastructures with a focus on authentication bypass, business logic flaws, and privilege escalation.
- Designed and developed vulnerable Android applications for internal CTFs and training exercises to simulate real-world exploitation scenarios.

- Performed in-depth reverse engineering and dynamic analysis using tools such as Frida, Jadx, MobSF, and Ghidra for vulnerability research.

- Participated in internal R&D to build custom scripts and automation tooling for reconnaissance and exploitation in web attack surfaces.

- Active participant in CTF competitions covering various categories including Web, Pwn, Reversing, OSINT, MISC, Steganography, and Cryptography.

- Submitted multiple vulnerabilities to coordinated disclosure programs on platforms like BUGCROWD & HACKERONE.

CERTIFICATIONS

- Offensive Bug Bounty Hunter 2.0 - Hackersera
  Certification Code: 26CCCBD89E33B478B4747B0571C4CA1EC3840E89 - Bug Bounty expertise for web and android applications.

- Offensive API Penetration Testing - Hackersera
  Certification Code: A38DFD39F01331FC720AEAC64A0B50B0A9026C11 - Expertise in identifying and securing vulnerabilities in APIs.

- Offensive Thick Client Pentesting - Hackersera
  Certification Code: BE8857C1B953E2F47FCFD47AB646F2E8B0402801 - Expertise in identifying vulnerabilities in desktop applications.

- Offensive Automotive Security Assessment - Hackersera
  Certification Code: 833EC6FC5815121FF000C08E5ADE870BA94E596D - Familiarity with common vulnerabilities in automotive systems.

- SDR Exploitation - Hackersera
  Certification Code: 260A42705B473B7AD9CA3A04213F0AEC69901D1A - Proficiency in Software Defined Radio.