# Executive Summary

**Kosana Ankamma Rao** — kosana.ar@gmail.com
**Project:** Automated Mobile App Hardening + Evidence-driven Pentest (Android)

**Objective:** Build a reproducible pipeline to locate mobile app vulnerabilities, demonstrate actionable proof-of-concept exploit(s), apply automated hardening, and verify remediation with clear evidence.

**Key findings (before):** - Multiple exported components allowing unauthenticated component invocation (DoTransfer, ViewStatement, PostLogin, ChangePassword). - Exported ContentProvider and BroadcastReceiver. - `allowBackup="true"` and `android:debuggable="true"` present — high-risk misconfigurations.

**Actions taken:** - Automated static scan identified exported components and sensitive strings. - PoC demonstrated component hijacking (external intents launched sensitive actions). - Automated patch applied: set `android:exported="false"` where appropriate, set `allowBackup="false"`, removed `debuggable`. - Rebuilt and signed APK, installed patched APK on device.

**Result (after):** - All targeted components deny external access (Permission Denial) when invoked externally. - Backup and debug attack vectors closed. - Artifacts produced: before/after scan logs, PoC logs, rebuilt APK, signed APK.

**Impact:** - Ready-to-run pipeline suitable for CI integration. - Demonstrates offensive + defensive skills and a mature security workflow — ideal portfolio piece for security engineering roles.

**Contact:** kosana.ar@gmail.com