PhonePe Vulnerability Report- User Impersonation Attack

PhonePe is a UPI based App to provide a cashless and a seamless payment experience.

- Version: 3.0.6 - 3.3.26
- Package name: com.PhonePe.app
- Vulnerabilities found:
- Exposure of Private Information
- Authentication Bypass
- Improper verification of the source

1. User Impersonation Attack

Impact Description:

For this attack, the user does not need an account of PhonePe. A malicious app is running on the victim device that can intercept SMS messages and forward it to an attacker. An attacker can setup a PhonePe account on behalf of a user on his device. This account can be used to carry out fraudulent activities, which could implicate the victim.

- **Steps to reproduce:**
  - Attacker Installs PhonePe. She sets up her account by entering the victims phone number.
  - PhonePe server sends OTP to victim which the malicious app forwards to attacker.
  - Attacker enters the OTP to login to the app and sets a PIN for the user . At this point, user account is setup completely.