PhonePe Vulnerability Report- Authentication Bypass

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. Authentication Bypass using Forgot Password Mechanism

Impact Description:

We assume that 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 and use the "Forgot Password" feature to reset a victims password and compromise her account. The reset password feature is protected only by an OTP.

- **Steps to reproduce:**
    - Attacker Installs PhonePe and sets up her account.
    - Attacker initiates a password reset and enters victim phone number. The Phonepe server sends an OTP to the victim device. The malicious app intercepts the OTP and forwards to attacker.
    - Attacker keys in the OTP and sets a new PIN number. Since only a PIN is required for login, the account is compromised at this point. At this point the attacker can setup an SBI Buddy account of the victim

Forgot Password Activity and sample of how information can be exposed