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 Sniffed Username, PIN

Impact Description:

A malicious app with accessibility permission on a user's device can sniff private data such as Phone number(Username) & Login PIN. The can be leaked if the user clicks on the "Show" button. We create the app with accessilbity permission enabled. The app also has the ability to send/receive/read SMS so that it can intercept SMS messages and forward it.

- **Steps to reproduce:**
  - Install & Start PhonePe app
  - User sets up her account by entering the phone number, name and PIN. Then log out and then try to login using the phone number and PIN.
  - When entering PIN, the user clicks on "Show" button to confirm the pin she has entered

Below is the screenshot of Login activity: