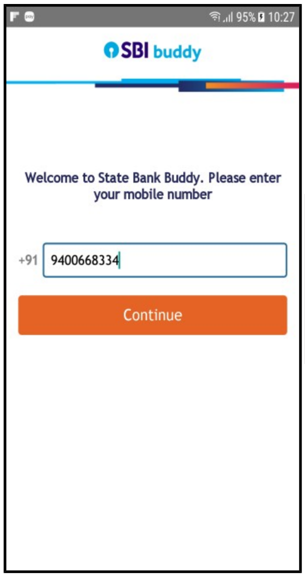
SBI Buddy Vulnerability Reporting

SBI Buddy is a wallet application

- Version: 1.41
- Current version: 1.42
- Package Name: com.sbi.erupee
- Vulnerabilities found:
    - Information exposure (**Both app versions**)
    - Authentication bypass using an alternate path or channel
    - Exposure of private information (**Both app versions**)

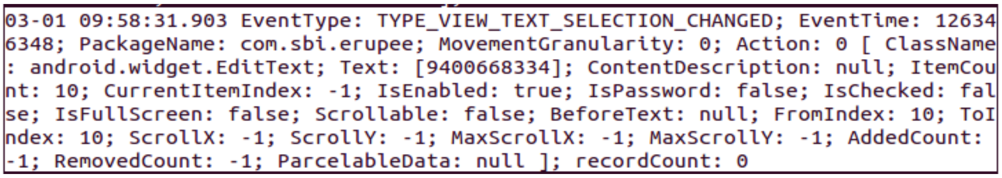
1. **Authentication bypass using an alternate path or channel**
    - **Impact description:** When the user configures the app for the first time, she sets a security question. This security question is required to reset password. The answer to the security question can be leaked.
    - **Steps to reproduce:**
        - Install SBI Buddy app.
        - Victim: When the user sets up the app for the first time, she enters the user name. The user name can be sniffed and when user sets up her account and forwards it to the attacker.
        - Attacker: Attacker receives username and waits for the victim to set the optional security question.
        - Victim: She sets the security question after OTP verification. \textit{Mally} intercepts the response and forwards it to the attacker.
        - Attacker: Attacker now uses the user name and security question to to initiate a password reset. Attacker waits for temporary PIN.
        - Victim: Malicious app forwards PIN to attacker.
        - Attacker: Enters PIN to set a new password. Since only a PIN is required for login, the account is compromised at this point.
    - **Screenshots:**



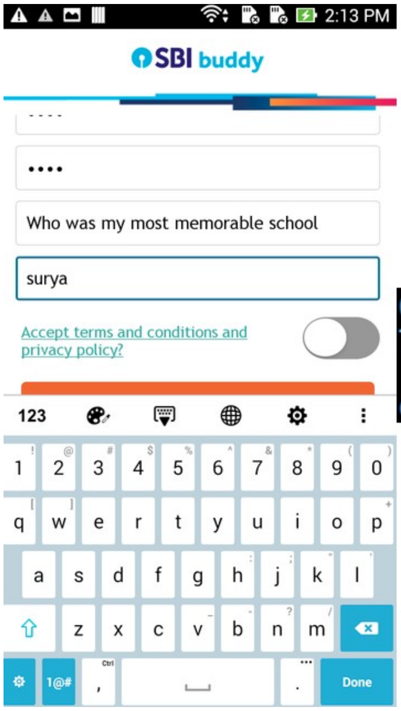
Welcome to State Bank Buddy. Please enter your mobile number

+91 9400668334

Continue



```
03-01 09:58:31.903 EventType: TYPE_VIEW_TEXT_SELECTION_CHANGED; EventTime: 12634
6348; PackageName: com.sbi.erupee; MovementGranularity: 0; Action: 0 [ ClassName
: android.widget.EditText; Text: [9400668334]; ContentDescription: null; ItemCou
nt: 10; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: fal
se; IsFullScreen: false; Scrollable: false; BeforeText: null; FromIndex: 10; ToI
ndex: 10; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount:
-1; RemovedCount: -1; ParcelableData: null ]; recordCount: 0
```

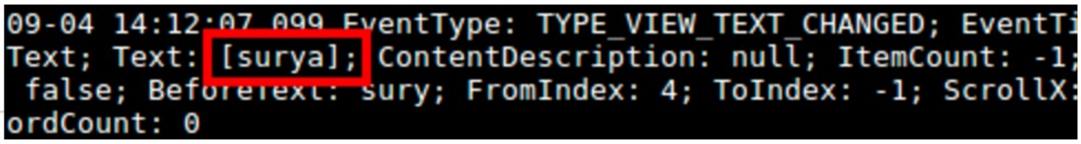


••••

Who was my most memorable school

surya

Accept terms and conditions and privacy policy?



```
09-04 14:12:07.099 EventType: TYPE_VIEW_TEXT_CHANGED; EventTi
Text; Text: [surya]; ContentDescription: null; ItemCount: -1;
 false; BeforeText: sury; FromIndex: 4; ToIndex: -1; ScrollX:
ordCount: 0
```