SBI Buddy Vulnerability Reporting

SBI Buddy is a wallet application

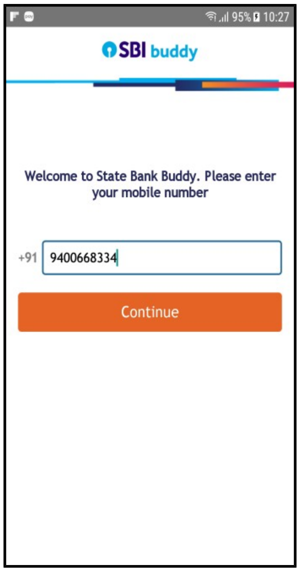
- Version: 1.41
- Current version: 1.42
- Package Name: com.sbi.erupee
- Vulnerabilities found:
  - Information exposure (**Both app versions**)
  - Authentication bypass using an alternate path or channel
  - Exposure of private information (**Both app versions**)

Vulnerabilities

1. **Confidential Information Exposure:**
   - **Impact description:** Phone number, which is used as the login username, can be sniffed from the login page by a malicious app which has accessibility permission. The leakage of username is a serious threat to the account
   - **Steps to reproduce:**
     - Install SBI Buddy app.
     - The device has a malicious app with accessibility permission and the ability to intercept accessibility events. The text from GUI is saved into a file by the app.
     - Start SBI Buddy and enter the credentials (username).
     - The malicious app intercepts all accessibility events and stores the password into a file.
   - **Screens shot:**

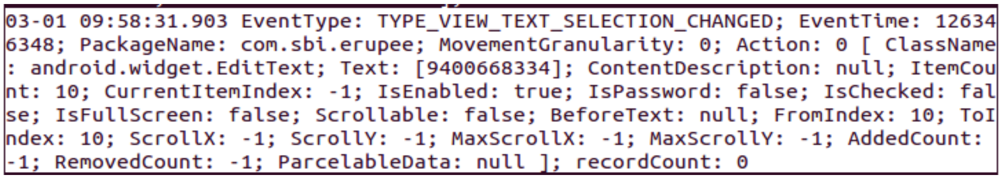
     Figure 1 : User name
     Figure 2: PAN Card (Government ID)
     Figure 3: Date of Birth

Figure 1



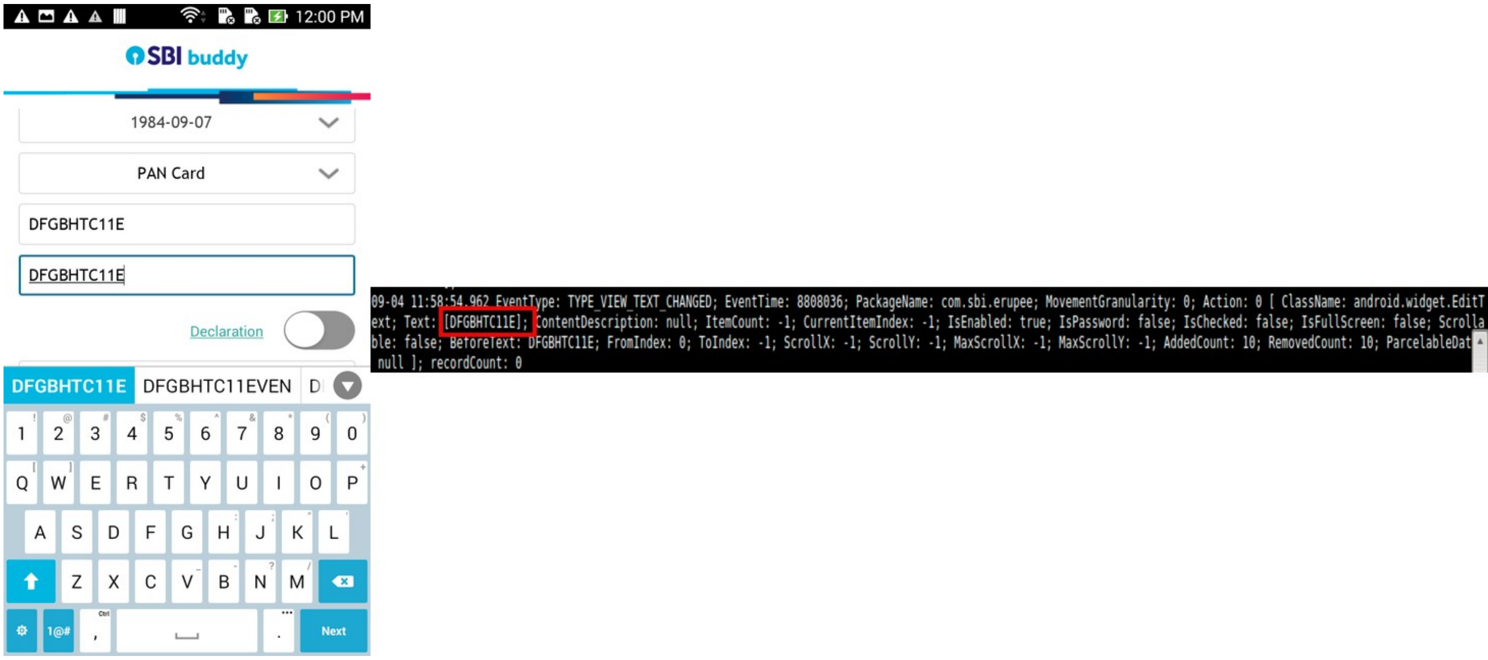
Welcome to State Bank Buddy. Please enter your mobile number

+91 9400668334



```
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
```

Figure 2



1984-09-07

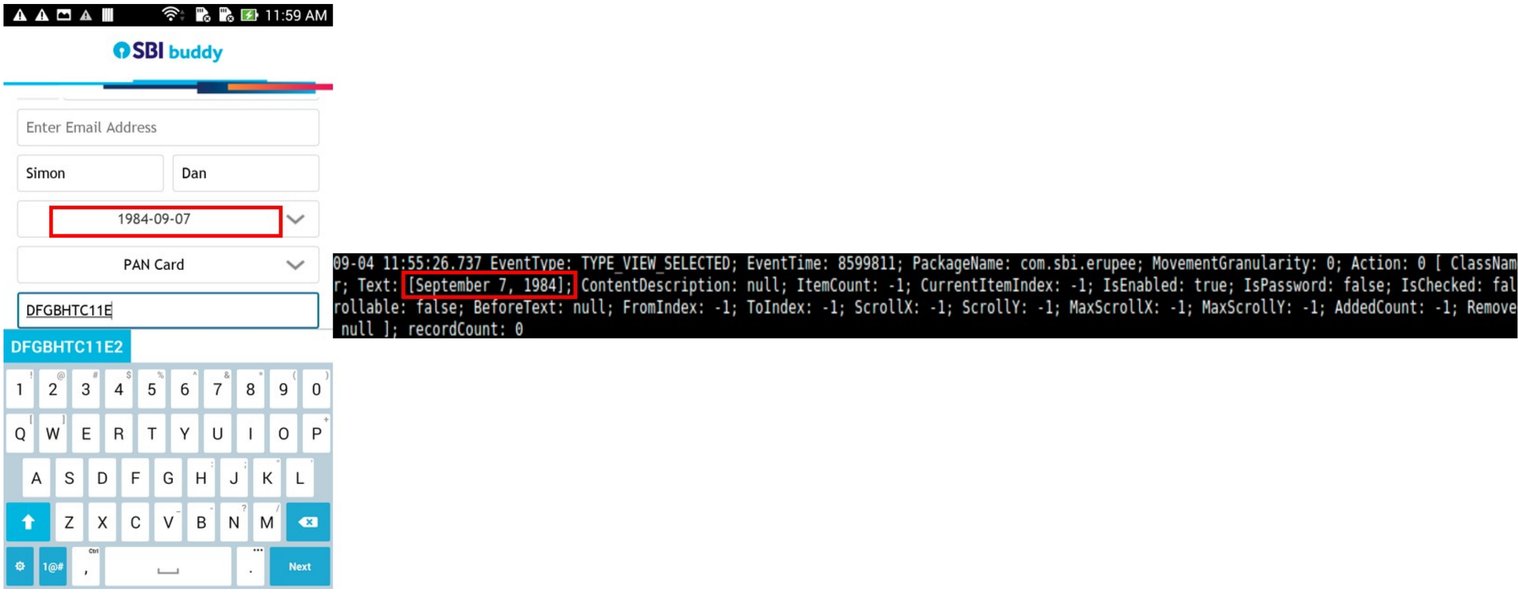
PAN Card

DFGBHTC11E

DFGBHTC11E

```
09-04 11:58:54.962 EventType: TYPE_VIEW_TEXT_CHANGED; EventTime: 8808036; PackageName: com.sbi.erupee; MovementGranularity: 0; Action: 0 [ ClassName: android.widget.EditT
ext; Text: [DFGBHTC11E]; ContentDescription: null; ItemCount: -1; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: false; IsFullScreen: false; Scrolla
ble: false; BeforeText: DFGBHTC11E; FromIndex: 0; ToIndex: -1; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount: 10; RemovedCount: 10; ParcelableDat
 null ]; recordCount: 0
```

Figure 3



Enter Email Address

Simon

Dan

1984-09-07

PAN Card

DFGBHTC11E

```
09-04 11:55:26.737 EventType: TYPE_VIEW_SELECTED; EventTime: 8599811; PackageName: com.sbi.erupee; MovementGranularity: 0; Action: 0 [ ClassNam
r; Text: [September 7, 1984]; ContentDescription: null; ItemCount: -1; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: fal
rollable: false; BeforeText: null; FromIndex: -1; ToIndex: -1; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount: -1; Remove
 null ]; recordCount: 0
```