Facebook

Basic Details

Website for Bug Bounty : https://www.facebook.com/whitehat
Package: com.facebook.katana
Application Label: Facebook
Process Name: com.facebook.katana
Version: 174.0.0.54.96
Data Directory: /data/data/com.facebook.katana
APK Path: /data/app/com.facebook.katana-2.apk
UID: 10121
GID: [1028, 1015, 3003]
Shared Libraries: [/system/framework/com.google.android.maps.jar]Website for Bug Bounty : https://www.facebook.com/whitehat
Shared User ID: null
Uses Permissions:

- android.permission.ACCESS_COARSE_LOCATION
- android.permission.WAKE_LOCK
- android.permission.VIBRATE
- android.permission.READ_CONTACTS
- android.permission.WRITE_CONTACTS
- android.permission.GET_ACCOUNTS
- android.permission.MANAGE_ACCOUNTS
- android.permission.AUTHENTICATE_ACCOUNTS
- android.permission.READ_SYNC_SETTINGS
- android.permission.WRITE_SYNC_SETTINGS
- android.permission.ACCESS_FINE_LOCATION
- android.permission.BROADCAST_STICKY
- com.facebook.katana.provider.ACCESS
- com.facebook.orca.provider.ACCESS
- com.facebook.mlite.provider.ACCESS
- com.facebook.pages.app.provider.ACCESS
- android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
- android.permission.CAMERA
- android.permission.RECORD_AUDIO
- com.google.android.gms.permission.ACTIVITY_RECOGNITION
- android.permission.WRITE_EXTERNAL_STORAGE
- com.facebook.permission.prod.FB_APP_COMMUNICATION
- android.permission.READ_PHONE_STATE
- android.permission.READ_CALENDAR

- android.permission.WRITE_CALENDAR
- android.permission.MODIFY_AUDIO_SETTINGS
- android.permission.READ_PROFILE
- android.permission.READ_SMS
- android.permission.CHANGE_NETWORK_STATE
- android.permission.CHANGE_WIFI_STATE
- android.permission.SYSTEM_ALERT_WINDOW
- com.google.android.providers.gsf.permission.READ_GSERVICES
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.GET_TASKS
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.ACCESS_NETWORK_STATE
- android.permission.REQUEST_INSTALL_PACKAGES
- com.facebook.katana.permission.CROSS_PROCESS_BROADCAST_MANAGER
- android.permission.BATTERY_STATS
- android.permission.ACCESS_WIFI_STATE
- android.permission.INTERNET
- com.android.launcher.permission.INSTALL_SHORTCUT
- com.facebook.receiver.permission.ACCESS
- com.sec.android.provider.badge.permission.READ
- com.sec.android.provider.badge.permission.WRITE
- com.htc.launcher.permission.READ_SETTINGS
- com.htc.launcher.permission.UPDATE_SHORTCUT
- com.sonyericsson.home.permission.BROADCAST_BADGE
- com.facebook.katana.permission.RECEIVE_ADM_MESSAGE
- com.amazon.device.messaging.permission.RECEIVE
- com.google.android.c2dm.permission.RECEIVE
- com.facebook.katana.permission.C2D_MESSAGE
- com.nokia.pushnotifications.permission.RECEIVE

Defines Permissions:

- com.facebook.katana.provider.ACCESS
- com.facebook.permission.prod.FB_APP_COMMUNICATION
- com.facebook.katana.permission.CROSS_PROCESS_BROADCAST_MANAGER
- com.facebook.receiver.permission.ACCESS
- com.facebook.katana.permission.RECEIVE_ADM_MESSAGE
- com.facebook.katana.permission.C2D_MESSAGE

Setup & Assumptions

The attack involves a victim device and an attacker device, both device has the legitimate version of Facebook app installed. At some point the device has been compromised resulting in a Trojan running in the background. The Trojan has some basic features such as:

1. Sniff and log user name,password, a file.
2. Forward username password to attacker.

Vulnerability Details

- CWE 200- Information Exposure

Description :

An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information.

Facebook app has username and password in the input textbox. For username attribute on the input textbox of the keypad is categorized as “not password” thus allowing it to be sniffable through accessibility service. In password field user have a show/hide option which user can toggle attribute as “password” and “not password”. If user clicks the show password then attribute changes to “not password” thus allowing trojan to sniff using accessibility service.

Exploit:

1. Create a Trojan app that has permission to use accessibility service.
2. The accessibility service intercepts all events and data (sensitive or not) from facebook app.

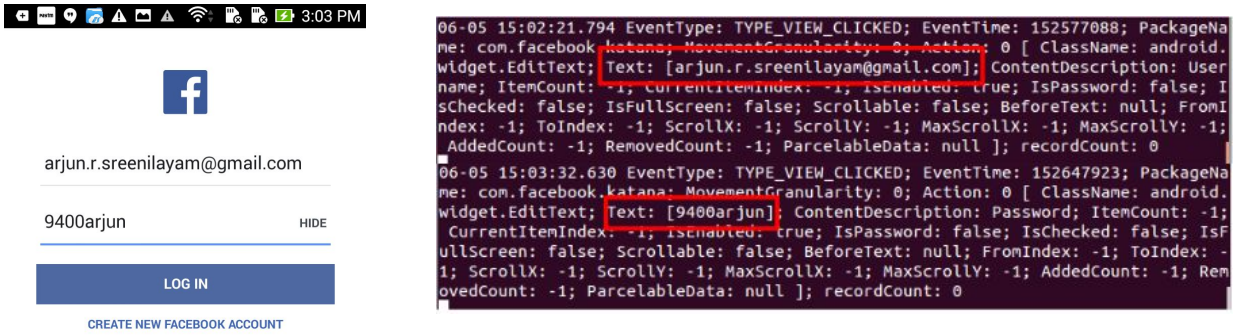


Fig: Screenshot of Facebook app and UI Automator

Remediation:
Removal of Show/Hide button in password field

- CWE-359: Exposure of Private Information ('Privacy Violation')

Description :

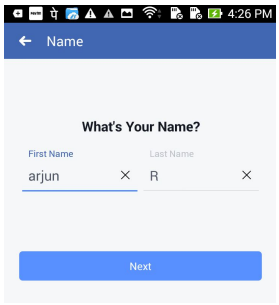
The software does not properly prevent private data (such as credit card numbers) from being accessed by actors who either (1) are not explicitly authorized to access the data or (2) do not have the implicit consent of the people to which the data is related.

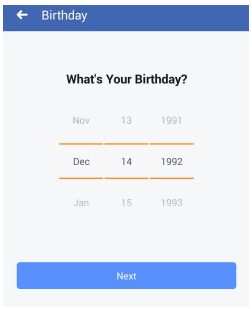
Exploit:
Same as above

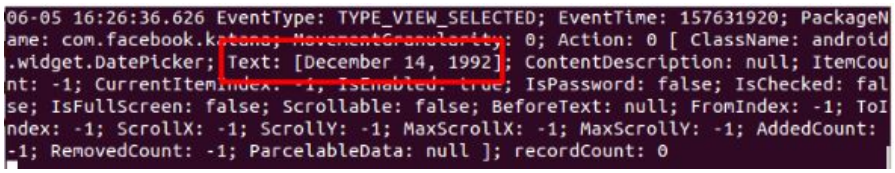
When a user is creating new facebook account using facebook application,
For all the personal details attribute on the input textbox of the keypad is categorized as “not password” thus allowing it to be sniffable through accessibility service.

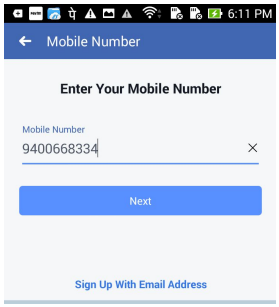
Sniffable Data

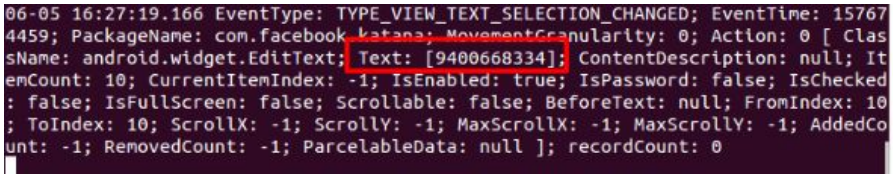
- Username
- Phone Number
- Email id
- DOB
- Password

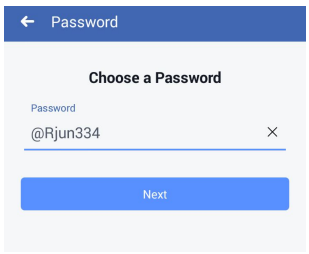












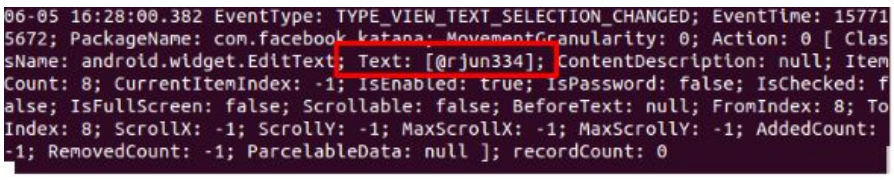


Fig: Screenshot of Facebook app and UI Automator

Remediation:

Sensitive data should be hidden from other apps.