##### Description

**Instance 1 - Hook com.uob.mobile.android.profile.ui.passwordandsecurity.ProfilePasswordSecurityActivity**

It was found that the application's activity can be "hooked," allowing for the circumvention of the authentication process. This flaw presents a significant security risk as it enables unauthorized users to bypass established authentication protocols and alter the secure PIN.

**Setup Details**

* Install custom Frida: <https://github.com/hzzheyang/strongR-frida-android>
* Ensure IAmNotADeveloper is enabled in LSPosed

Steps to reproduce:

1. Login to any user with Secure PIN setup. If there were no secure pin being setup, check with UOB developer team.
2. Browse through the application and close the application completely.
3. Run the command to start UOB TMRW ID application with sslpinning disable.

objection -N -h 192.168.137.212 -p 8889 -g com.uob.id.digitalbank.uat explore --startup-command 'android sslpinning disable'

android intent launch\_activity com.uob.mobile.android.profile.ui.passwordandsecurity.ProfilePasswordSecurityActivity

1. Notice that it hooked to the Password and Security Page without authentication.

A screenshot of a computer

Description automatically generated

1. Change the Secure PIN. In this testcase, user PENTESTUNITY07 has the default secure pin set as 100800. Observe that user can change the Secure PIN without logging into the application.

A screenshot of a computer

Description automatically generatedA screenshot of a phone

Description automatically generated

1. To show the evident of the updated Secure Pin, use the normal flow and login to the account. Change the Secure PIN again and observed that it can be changed successfully.

A screenshot of a password

Description automatically generatedA screenshot of a phone

Description automatically generated

**Instance 2 - IAmNotADeveloper (Rooted Android Device)**

When a user uses a Rooted Android device and tries to access the UOB MY Application with USB debugging turned on, user will receive a prompt instructing them to disable USB debugging before they can proceed with using the UOB Application. This can be bypassed by installing IAmNotADeveloper module in LSPosed.

1. Ensure that device is rooted and Shizuku is downloaded in the PlayStore.
2. Install LSPosed from <https://github.com/LSPosed/LSPosed/releases> into the device.
3. Install and enable the LSPosed file into Magisk Modules.
4. Access LSPosed and click on Modules.
5. Search for IAmNotADeveloper and download the module.
6. Enable the module, checked on UOB TMRW ID application.

Screenshot 1: Device is rooted and Shizuku is downloaded and running.

A screenshot of a cell phone

Description automatically generatedA screenshot of a phone

Description automatically generated

Screenshot 2: Install and enable LSPosed in Magisk Modules.

A screenshot of a computer

Description automatically generated

Screenshot 3: Access LSPosed and click on Modules. Search and install IAmNotADeveloper. Enable the module and checked for UOB TMRW ID Application.

A screenshot of a phone

Description automatically generatedA screenshot of a phone

Description automatically generatedA screenshot of a phone

Description automatically generated

Screenshot 4: Access UOB TMRW ID Application

A screenshot of a phone

Description automatically generated