BÁO CÁO BÀI TẬP

Môn học: Bảo mật web và ứng dụng

GVHD: Nghi Hoàng Khoa

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O22.ATCL.1- Nhóm 3

STT	Họ và tên	MSSV	Email
1	Nguyễn Ngọc Trà My	21520353	21520353@gm.uit.edu.vn
2	Bùi Hoàng Trúc Anh	21521817	21521817@gm.uit.edu.vn
3	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
4	Huỳnh Minh Tân Tiến	21521520	21521520@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**

STT	Công việc	Kết quả tự đánh giá
1	**Bài tập 1**	100%
2	**Bài tập 2**	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

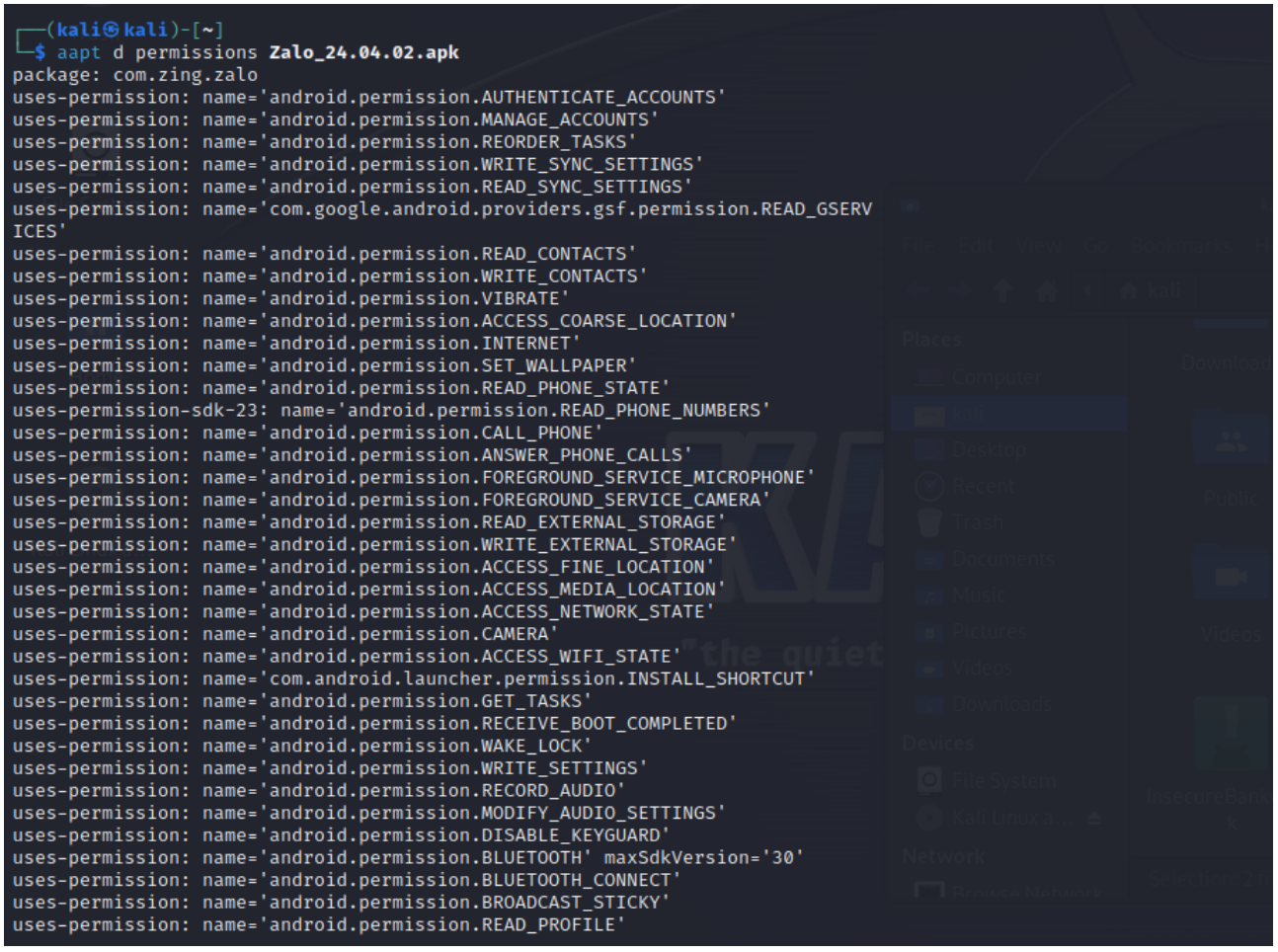
BÁO CÁO CHI TIẾT

Bài tập 1

2 ứng dụng nhóm dùng để kiểm tra và phân tích là: Zalo_24.04.02.apk và Zavi_22.01.01.apk

Dùng appt để kiểm tra quyền của các tập apk

Các quyền Zalo yêu cầu



```
┌──(kali㉿kali)-[~]
└─$ aapt d permissions Zalo_24.04.02.apk
package: com.zing.zalo
uses-permission: name='android.permission.AUTHENTICATE_ACCOUNTS'
uses-permission: name='android.permission.MANAGE_ACCOUNTS'
uses-permission: name='android.permission.REORDER_TASKS'
uses-permission: name='android.permission.WRITE_SYNC_SETTINGS'
uses-permission: name='android.permission.READ_SYNC_SETTINGS'
uses-permission: name='com.google.android.providers.gsf.permission.READ_GSERV
ICES'
uses-permission: name='android.permission.READ_CONTACTS'
uses-permission: name='android.permission.WRITE_CONTACTS'
uses-permission: name='android.permission.VIBRATE'
uses-permission: name='android.permission.ACCESS_COARSE_LOCATION'
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.SET_WALLPAPER'
uses-permission: name='android.permission.READ_PHONE_STATE'
uses-permission-sdk-23: name='android.permission.READ_PHONE_NUMBERS'
uses-permission: name='android.permission.CALL_PHONE'
uses-permission: name='android.permission.ANSWER_PHONE_CALLS'
uses-permission: name='android.permission.FOREGROUND_SERVICE_MICROPHONE'
uses-permission: name='android.permission.FOREGROUND_SERVICE_CAMERA'
uses-permission: name='android.permission.READ_EXTERNAL_STORAGE'
uses-permission: name='android.permission.WRITE_EXTERNAL_STORAGE'
uses-permission: name='android.permission.ACCESS_FINE_LOCATION'
uses-permission: name='android.permission.ACCESS_MEDIA_LOCATION'
uses-permission: name='android.permission.ACCESS_NETWORK_STATE'
uses-permission: name='android.permission.CAMERA'
uses-permission: name='android.permission.ACCESS_WIFI_STATE'
uses-permission: name='com.android.launcher.permission.INSTALL_SHORTCUT'
uses-permission: name='android.permission.GET_TASKS'
uses-permission: name='android.permission.RECEIVE_BOOT_COMPLETED'
uses-permission: name='android.permission.WAKE_LOCK'
uses-permission: name='android.permission.WRITE_SETTINGS'
uses-permission: name='android.permission.RECORD_AUDIO'
uses-permission: name='android.permission.MODIFY_AUDIO_SETTINGS'
uses-permission: name='android.permission.DISABLE_KEYGUARD'
uses-permission: name='android.permission.BLUETOOTH' maxSdkVersion='30'
uses-permission: name='android.permission.BLUETOOTH_CONNECT'
uses-permission: name='android.permission.BROADCAST_STICKY'
uses-permission: name='android.permission.READ_PROFILE'
```

```
uses-permission: name='android.permission.BROADCAST_STICKY'
uses-permission: name='android.permission.READ_PROFILE'
uses-permission: name='com.zing.zalo.permission.BIND_ZALO_SERVICE'
uses-permission: name='zing.zalo.permission.ZALO_SERVICE'
uses-permission: name='android.permission.GET_ACCOUNTS'
uses-permission: name='android.permission.FLASHLIGHT'
uses-permission-sdk-23: name='android.permission.USE_FINGERPRINT'
uses-permission: name='android.permission.SYSTEM_ALERT_WINDOW'
uses-permission-sdk-23: name='android.permission.READ_CALL_LOG'
uses-permission: name='com.android.vending.BILLING'
uses-permission: name='com.huawei.android.launcher.permission.CHANGE_BADGE'
uses-permission: name='com.sonymobile.home.permission.PROVIDER_INSERT_BADGE'
uses-permission: name='com.anddoes.launcher.permission.UPDATE_COUNT'
uses-permission: name='com.majeur.launcher.permission.UPDATE_BADGE'
uses-permission: name='android.permission.READ_APP_BADGE'
uses-permission: name='android.permission.USE_FULL_SCREEN_INTENT'
uses-permission: name='android.permission.USE_BIOMETRIC'
uses-permission: name='android.permission.USE_FINGERPRINT'
uses-permission: name='android.permission.SCHEDULE_EXACT_ALARM'
uses-permission: name='android.permission.CHANGE_WIFI_STATE'
uses-permission: name='android.permission.POST_NOTIFICATIONS'
uses-permission: name='android.permission.READ_MEDIA_IMAGES'
uses-permission: name='android.permission.READ_MEDIA_VIDEO'
uses-permission: name='android.permission.READ_MEDIA_VISUAL_USER_SELECTED'
uses-permission: name='com.google.android.gms.permission.AD_ID'
uses-permission: name='android.permission.FOREGROUND_SERVICE_LOCATION'
uses-permission: name='android.permission.FOREGROUND_SERVICE_DATA_SYNC'
uses-permission: name='android.permission.FOREGROUND_SERVICE_SPECIAL_USE'
uses-permission: name='android.permission.FOREGROUND_SERVICE'
permission: zing.zalo.permission.ZALO_SERVICE
permission: com.zing.zalo.permission.BIND_ZALO_SERVICE
uses-permission: name='com.zing.zalo.permission.BROADCAST_FROM_VIDEO_PROCESSI
NG'
permission: com.zing.zalo.permission.BROADCAST_FROM_VIDEO_PROCESSING
permission: com.zing.zalo.permission.C2D_MESSAGE
uses-permission: name='com.zing.zalo.permission.C2D_MESSAGE'
```

Quyền hạn cơ bản:

android.permission.AUTHENTICATE_ACCOUNTS: Cho phép ứng dụng truy cập thông tin tài khoản Google của bạn.

android.permission.MANAGE_ACCOUNTS: Cho phép ứng dụng thêm, xóa và sửa đổi tài khoản Google của bạn.

android.permission.REORDER_TASKS: Cho phép ứng dụng sắp xếp lại các ứng dụng đã mở gần đây.

android.permission.WRITE_SYNC_SETTINGS: Cho phép ứng dụng thay đổi cài đặt đồng bộ hóa của bạn.

android.permission.READ_SYNC_SETTINGS: Cho phép ứng dụng đọc cài đặt đồng bộ hóa của bạn.

com.google.android.providers.gsf.permission.READ_GSERVICES: Cho phép ứng dụng truy cập các dịch vụ của Google.

android.permission.READ_CONTACTS: Cho phép ứng dụng đọc danh bạ của bạn.

android.permission.WRITE_CONTACTS: Cho phép ứng dụng ghi vào danh bạ của bạn.

android.permission.VIBRATE: Cho phép ứng dụng rung điện thoại của bạn.

android.permission.ACCESS_COARSE_LOCATION: Cho phép ứng dụng truy cập vị trí gần đúng của bạn.

android.permission.INTERNET: Cho phép ứng dụng truy cập internet.

Quyền hạn nâng cao:

android.permission.SET_WALLPAPER: Cho phép ứng dụng đặt hình nền cho bạn.

android.permission.READ_PHONE_STATE: Cho phép ứng dụng truy cập thông tin trạng thái điện thoại của bạn, bao gồm số IMEI và số điện thoại.

android.permission.READ_PHONE_NUMBERS: Cho phép ứng dụng đọc các số điện thoại được lưu trữ trên điện thoại của bạn.

android.permission.CALL_PHONE: Cho phép ứng dụng thực hiện cuộc gọi điện thoại.

android.permission.ANSWER_PHONE_CALLS: Cho phép ứng dụng trả lời cuộc gọi điện thoại.

android.permission.FOREGROUND_SERVICE_MICROPHONE: Cho phép ứng dụng sử dụng micrô khi chạy như dịch vụ nền.

android.permission.FOREGROUND_SERVICE_CAMERA: Cho phép ứng dụng sử dụng camera khi chạy như dịch vụ nền.

android.permission.READ_EXTERNAL_STORAGE: Cho phép ứng dụng đọc dữ liệu từ bộ nhớ ngoài của bạn.

android.permission.WRITE_EXTERNAL_STORAGE: Cho phép ứng dụng ghi dữ liệu vào bộ nhớ ngoài của bạn.

android.permission.ACCESS_FINE_LOCATION: Cho phép ứng dụng truy cập vị trí chính xác của bạn.

android.permission.ACCESS_MEDIA_LOCATION: Cho phép ứng dụng truy cập vị trí của các tệp phương tiện của bạn.

android.permission.ACCESS_NETWORK_STATE: Cho phép ứng dụng truy cập trạng thái mạng của bạn.

android.permission.CAMERA: Cho phép ứng dụng sử dụng camera của bạn.

android.permission.ACCESS_WIFI_STATE: Cho phép ứng dụng truy cập trạng thái wifi của bạn.

com.android.launcher.permission.INSTALL_SHORTCUT: Cho phép ứng dụng tạo lối tắt trên màn hình chính của bạn.

android.permission.GET_TASKS: Cho phép ứng dụng truy cập danh sách các ứng dụng đã mở gần đây.

android.permission.RECEIVE_BOOT_COMPLETED: Cho phép ứng dụng tự động khởi chạy khi điện thoại của bạn khởi động lại.

android.permission.WAKE_LOCK: Cho phép ứng dụng ngăn điện thoại của bạn ngủ.

android.permission.WRITE_SETTINGS: Cho phép ứng dụng thay đổi cài đặt hệ thống của bạn.

android.permission.RECORD_AUDIO: Cho phép ứng dụng ghi âm thanh của bạn.

android.permission.MODIFY_AUDIO_SETTINGS: Cho phép ứng dụng thay đổi cài đặt âm thanh của bạn.

android.permission.DISABLE_KEYGUARD: Cho phép ứng dụng tắt màn hình khóa của bạn.

android.permission.BLUETOOTH: Cho phép ứng dụng sử dụng Bluetooth.

android.permission.BLUETOOTH_CONNECT: Cho phép ứng dụng kết nối với các thiết bị Bluetooth.

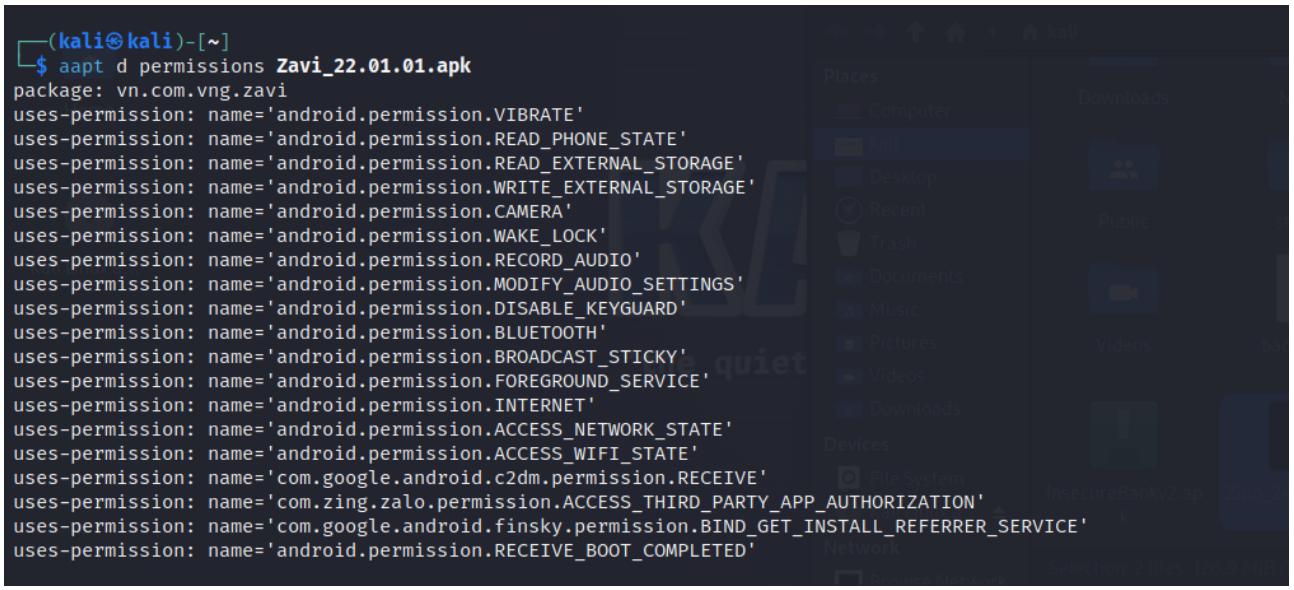
android.permission.BROADCAST_STICKY: Cho phép ứng dụng gửi tin nhắn phát sóng dính.

android.permission.READ_PROFILE: Cho phép ứng dụng đọc thông tin hồ sơ của bạn.

Quyền hạn tùy chỉnh:

Ngoài các quyền hạn cơ bản và nâng cao được liệt kê ở trên

Các quyền Zavi yêu cầu



"Zavi" đã được cấp một số quyền hạn sau:

Truy cập vào internet: Quyền hạn này cho phép ứng dụng kết nối với internet để tải xuống dữ liệu, hiển thị quảng cáo và thực hiện các chức năng khác.

Truy cập vào bộ nhớ ngoài: Quyền hạn này cho phép ứng dụng đọc và ghi dữ liệu vào bộ nhớ ngoài của thiết bị, chẳng hạn như thẻ SD.

Truy cập vào camera: Quyền hạn này cho phép ứng dụng chụp ảnh và quay video.

Ghi âm: Quyền hạn này cho phép ứng dụng ghi âm thanh.

Truy cập vào vị trí: Quyền hạn này cho phép ứng dụng truy cập vào vị trí hiện tại của thiết bị.

Gửi thông báo: Quyền hạn này cho phép ứng dụng gửi thông báo cho người dùng.

Truy cập vào danh bạ: Quyền hạn này cho phép ứng dụng truy cập vào danh bạ của người dùng.

Truy cập vào lịch: Quyền hạn này cho phép ứng dụng truy cập vào lịch của người dùng.

Quản lý cuộc gọi: Quyền hạn này cho phép ứng dụng thực hiện và nhận cuộc gọi.

Truy cập vào tin nhắn SMS: Quyền hạn này cho phép ứng dụng đọc và gửi tin nhắn SMS.

Truy cập vào Bluetooth: Quyền hạn này cho phép ứng dụng kết nối với thiết bị Bluetooth.

Truy cập vào cài đặt Wi-Fi: Quyền hạn này cho phép ứng dụng truy cập vào cài đặt Wi-Fi của thiết bị.

Truy cập vào cài đặt mạng di động: Quyền hạn này cho phép ứng dụng truy cập vào cài đặt mạng di động của thiết bị.

Truy cập vào tài khoản Google: Quyền hạn này cho phép ứng dụng truy cập vào tài khoản Google của người dùng.

Cài đặt ứng dụng: Quyền hạn này cho phép ứng dụng cài đặt các ứng dụng khác.

Phân tích quyền hạn tùy chỉnh trên các thành phần của ứng dụng

Hình ảnh không cung cấp đủ thông tin để phân tích quyền hạn tùy chỉnh trên các thành phần của ứng dụng. Để thực hiện việc này, cần phải có thêm thông tin về ứng dụng, chẳng hạn như mã nguồn hoặc tệp cấu hình.

Tuy nhiên, có thể suy đoán rằng một số quyền hạn được cấp cho ứng dụng có thể được sử dụng cho các mục đích sau:

Truy cập vào camera và micro để thực hiện cuộc gọi video hoặc ghi âm: Ứng dụng có thể sử dụng camera và micro để thực hiện cuộc gọi video hoặc ghi âm cuộc trò chuyện.

Truy cập vào vị trí để cung cấp các dịch vụ dựa trên vị trí: Ứng dụng có thể sử dụng vị trí của người dùng để cung cấp các dịch vụ dựa trên vị trí, chẳng hạn như bản đồ hoặc dự báo thời tiết.

Gửi thông báo để thông báo cho người dùng về các sự kiện hoặc cập nhật: Ứng dụng có thể gửi thông báo cho người dùng để thông báo cho họ về các sự kiện hoặc cập nhật quan trọng.

Truy cập vào danh bạ để tìm kiếm bạn bè hoặc chia sẻ thông tin: Ứng dụng có thể sử dụng danh bạ của người dùng để tìm kiếm bạn bè hoặc chia sẻ thông tin với họ.

Truy cập vào lịch để lên lịch các sự kiện hoặc nhắc nhở: Ứng dụng có thể sử dụng lịch của người dùng để lên lịch các sự kiện hoặc nhắc nhở họ về các cuộc hẹn sắp tới.

Quản lý cuộc gọi để thực hiện hoặc nhận cuộc gọi: Ứng dụng có thể quản lý cuộc gọi của người dùng, chẳng hạn như thực hiện hoặc nhận cuộc gọi, ghi âm cuộc gọi hoặc chặn các số không mong muốn.

Truy cập vào tin nhắn SMS để gửi hoặc nhận tin nhắn: Ứng dụng có thể gửi hoặc nhận tin nhắn SMS cho người dùng.

Truy cập vào Bluetooth để kết nối với các thiết bị khác: Ứng dụng có thể sử dụng Bluetooth để kết nối với các thiết bị khác, chẳng hạn như tai nghe hoặc loa.

Truy cập vào cài đặt Wi-Fi và mạng di động để quản lý kết nối internet: Ứng dụng có thể quản lý kết nối internet của người dùng, chẳng hạn như kết nối với mạng Wi-Fi hoặc mạng di động.

Truy cập vào tài khoản Google để đồng bộ hóa dữ liệu hoặc sử dụng các dịch vụ của Google: Ứng dụng có thể sử dụng tài khoản Google của người dùng để đồng bộ hóa dữ liệu hoặc sử dụng các dịch vụ của Google, chẳng hạn

Chữ ký : dùng apksigner check

Zalo

```
┌──(kali㉿kali)-[~]
└─$ apksigner verify --print-certs Zalo_24.04.02.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Signer #1 certificate DN: CN=zingtalk
Signer #1 certificate SHA-256 digest: d86efe151e09bf4ca8440cb3bfa0a81be2544f70c78587daf0266dfca2fa25df
Signer #1 certificate SHA-1 digest: 9487ba76b32e9e36785fb4c3540021f85af8d7b7
Signer #1 certificate MD5 digest: 34db1f467711ec53309269 2edb49847d
Source Stamp Signer certificate DN: CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US
Source Stamp Signer certificate SHA-256 digest: 3257d599a49d2c961a471ca9843f59d341a405884583fc087df4237b733bbd6d
Source Stamp Signer certificate SHA-1 digest: b1af3a0bf998aeede1a8716a539e5a59da1d86d6
Source Stamp Signer certificate MD5 digest: 577b8a9fbc7e308321aec6411169d2fb
```

Zavi

```
┌──(kali㉿kali)-[~]
└─$ apksigner verify --print-certs Zavi_22.01.01.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Signer #1 certificate DN: O=Zalo Group
Signer #1 certificate SHA-256 digest: 9b788b57660aa8eb5b0b25a465031dab69bbbe51f81c6ac8a479a5616bcd0826
Signer #1 certificate SHA-1 digest: 9f5ae1cb52c4d5f344870bae6633d2325552a584
Signer #1 certificate MD5 digest: f0029b45e1dc6cf5b7a93afcf56b506e
Source Stamp Signer certificate DN: CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=California, C=US
Source Stamp Signer certificate SHA-256 digest: 3257d599a49d2c961a471ca9843f59d341a405884583fc087df4237b733bbd6d
Source Stamp Signer certificate SHA-1 digest: b1af3a0bf998aeede1a8716a539e5a59da1d86d6
Source Stamp Signer certificate MD5 digest: 577b8a9fbc7e308321aec6411169d2fb
WARNING: META-INF/NativeUtil_release.kotlin_module not protected by signature. Unauthorized modifications to this JAR entry will no
de of META-INF/.
```

Bài tập 2:

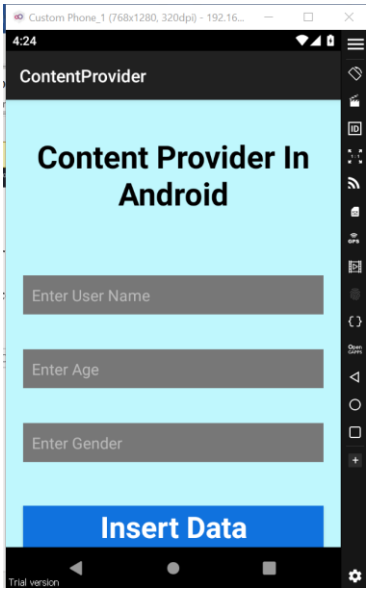
Ở đây ta sử dụng Content Provider để cho phép ứng dụng khác quyền truy cập và lấy thông tin.

Ứng dụng ContentProvider là ứng dụng lưu trữ thông tin. Ứng dụng AccessContent là ứng dụng để lấy thông tin từ ContentProvider và hiện ra màn hình

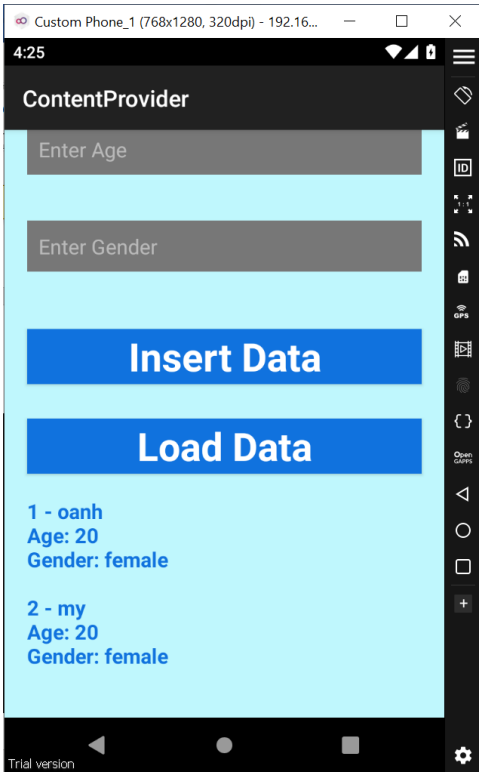
Lưu ý: Khi build apk cho cả 2 ứng dụng để chạy thử thì cần ký cùng 1 chữ ký.

ContentProvider: https://github.com/lhoanh123/ContentProvider

Khi nhấn Insert thì thông tin sẽ đi vô database

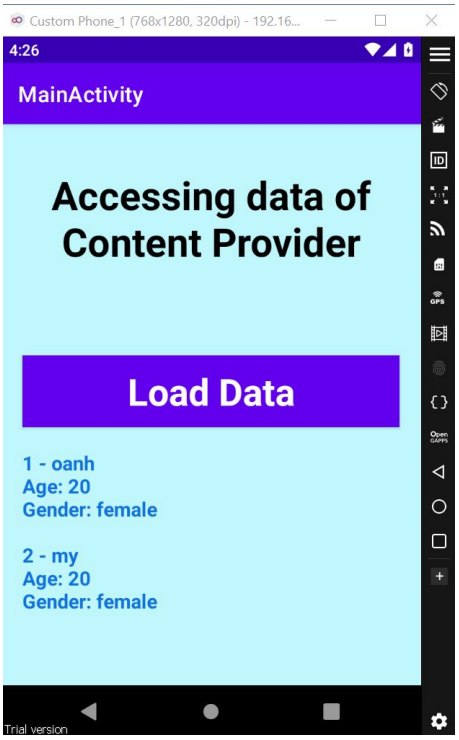


Khi nhấn Load Data thì thông tin được lưu trữ sẽ hiện ra màn hình



AccessContent: https://github.com/lhoanh123/AccessContent

Khi nhấn Load Data thì AccessContent sẽ lấy dữ liệu được lưu trữ trong ContentProvider để hiện ra màn hình


Custom Phone_1 (768x1280, 320dpi) - 192.16...
4:26
MainActivity
Accessing data of Content Provider
Load Data
1 - oanh
Age: 20
Gender: female
2 - my
Age: 20
Gender: female
Trial version