**App Name :** jaylearning

**Package Name : "com.jaylearning.community"**

**Version Code : 28**

**Version Name :** 1.7

**Compile SDK version : 28**

**Build version code : 28**

**Minimum SDK version : 16**

**Target SDK version : 28**

1. This application is being validated for **spyware PHA**
2. Let us understand the definition of spyware again

Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

1. Permissions responsible for spyware :

* android.permission.READ\_CONTACTS
* android.permission.RECEIVE\_SMS
* android.permission.READ\_SMS
* android.permission.READ\_EXTERNAL\_STORAGE
* android.permission.READ\_CALL\_LOG
* android.permission.RECORD\_AUDIO
* android.permission.READ\_CALENDER
* android.permission.ACCESS\_COARSE\_LOCATION
* android.permission.ACCESS\_FINE\_LOCATION
* com.android.browser.permission.READ\_HISTORY\_BOOKMARKS

1. Lets start reversing it.
2. We will check the spyware related permission in this app.

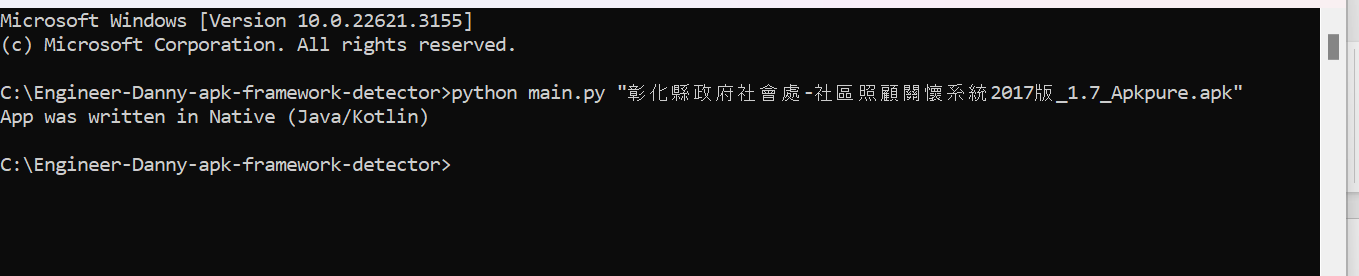
For that we will check androidmanifest.xml



Here we can see list of permissions like RECORD\_AUDIO,CALL\_PHONE, READ\_EXTERNAL\_STORAGE which is related to suspicious activity.

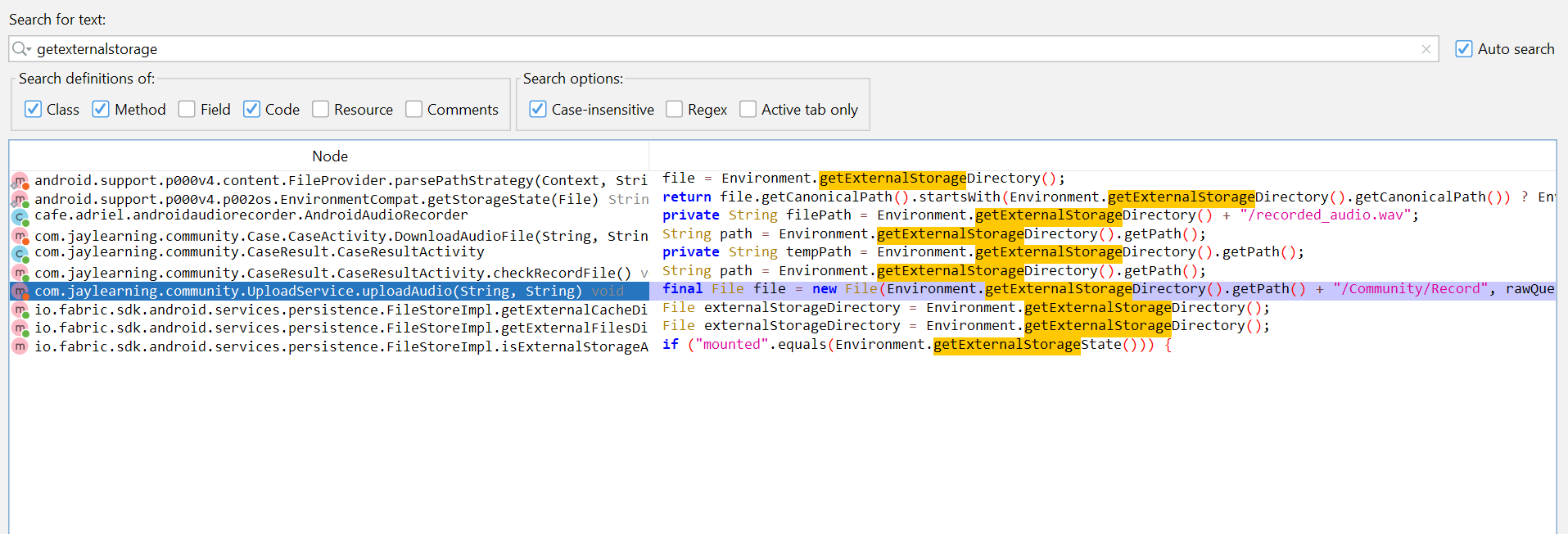
We will start with READ\_EXTERNAL\_STORAGE.

1. Before proceeding further , we will check whether this app is using any framework or not by using engineer danny framework as shown below



Here we can see that this app is built using **java/Kotlin.**

1. Now we will check search getExternalStorageDirectory through lens icon as shown below.



Here we will go with UploadService.uploadAudio package.

1. Double click on the highlighted part as shown above.





Here we can see that file is passed into audioUpload( ) method.

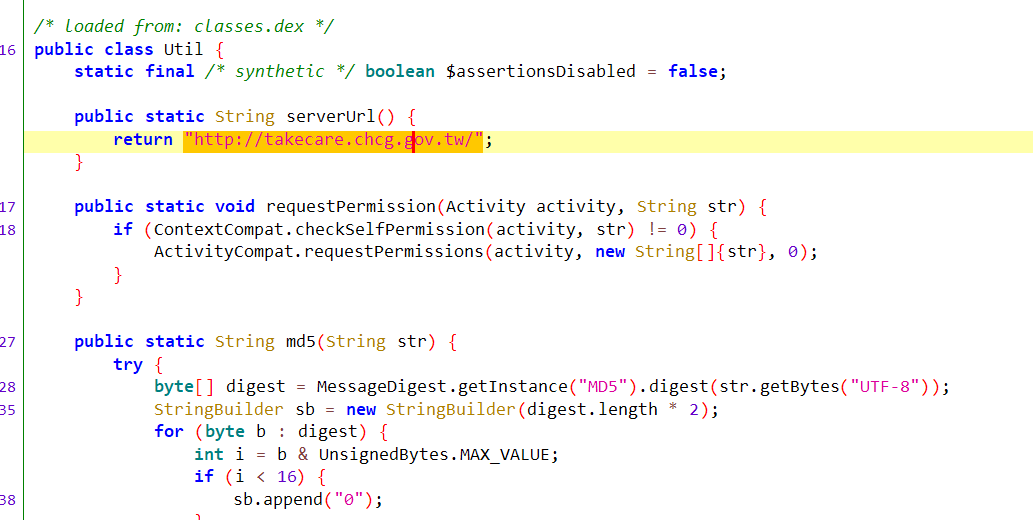
1. Now we will check **declaration** of audioUpload( ) method to know about this method.





Here we can see the **Util**.**serverUrl**( ) method on which http request is made

1. Now we will check the **declatation** of Util.serverUrl( ) method.



Here we can see the base url which is <http://takecare.chcg.gov.tw/> on which audio file is being sent.

1. Now we will check the disclosure part in res/value/string.xml to check whether the app is taking user consent or not.
2. After searching keyword like upload,collect and audio we are not getting any disclosure part.

On the above steps performed we can say that this app is sending data to an url without taking user consent .

So, this app is spyware

**VERDICT - TTP**