**App Name :** Cash mama personal loan app

**Package Name :** in.cashmama.app

**Version Code :** 111

**Version Name :** 2.8.0

**Compile SDK version : 29**

**Build version code : 10**

**Minimum SDK version : 19**

**Target SDK version : 28**

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

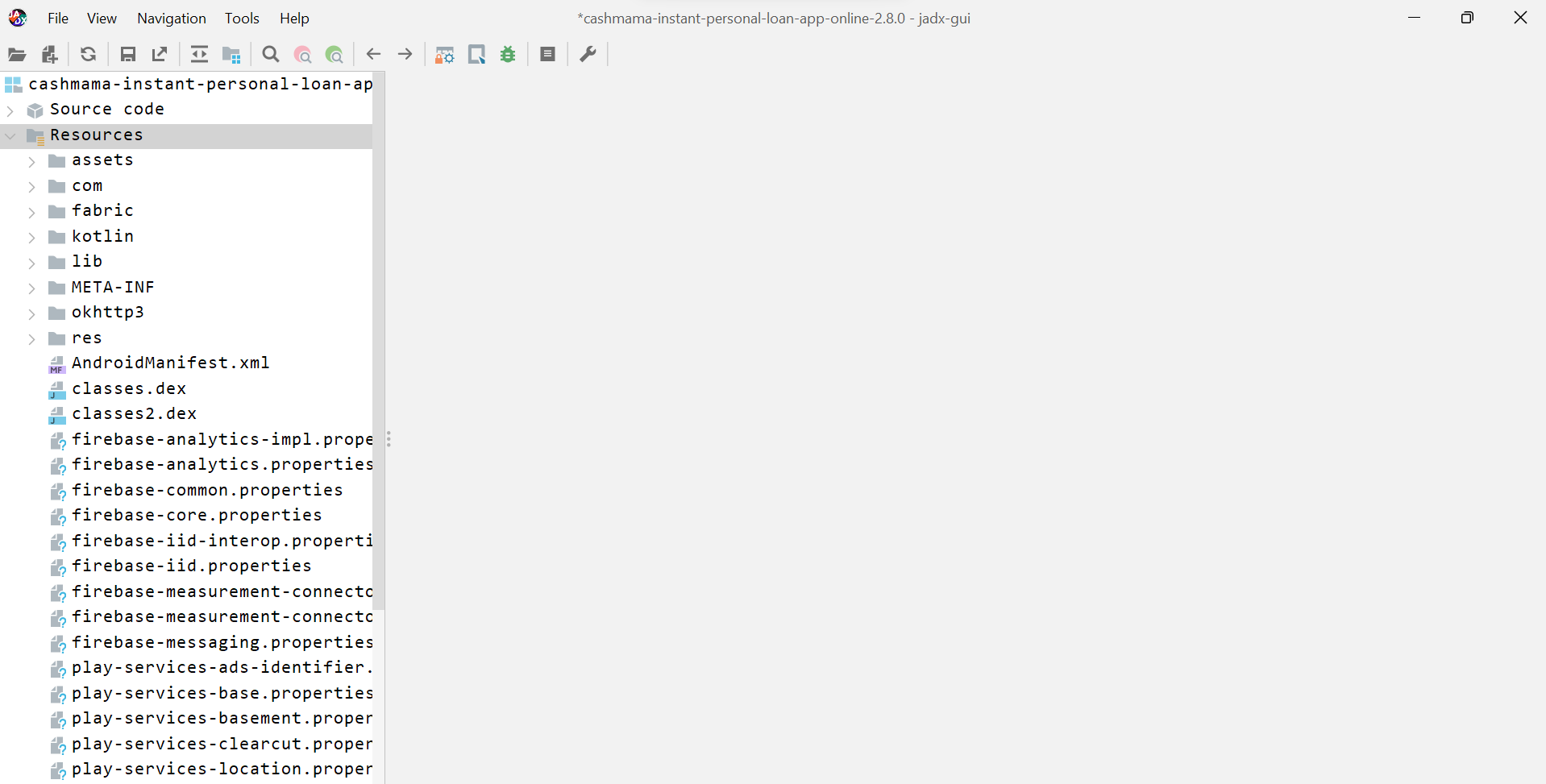
Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

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 doing RE.
2. Open the application in the JADX .

After opening, you can see the whole list of class files as mentioned in the screenshot below.



1. Double click the androidmanifest.xml

After opening the androidmanifest.xml file in JADX

you can find **READ\_SMS**  at **line 24 .**

A screenshot of a computer

Description automatically generated

Here you can see READ\_SMS permission which is suspicious related to spyware

First, we will check READ\_CONTACTS , if we will not get any url and disclosure then we will check READ\_CONTACT.

1. Now click on  button in JADX to find for sms usage.
2. Search for **Content://sms** as mentioned in below screenshot .

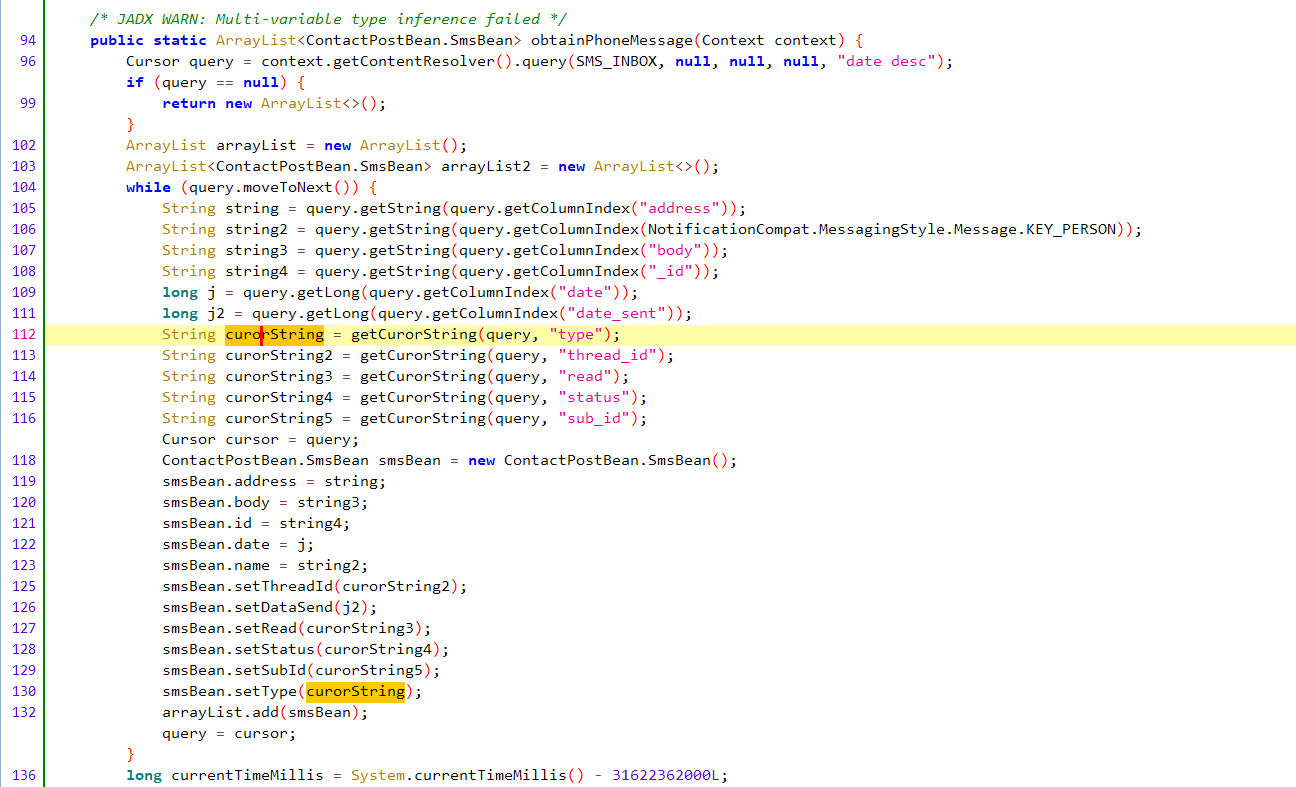
A screenshot of a computer

Description automatically generated

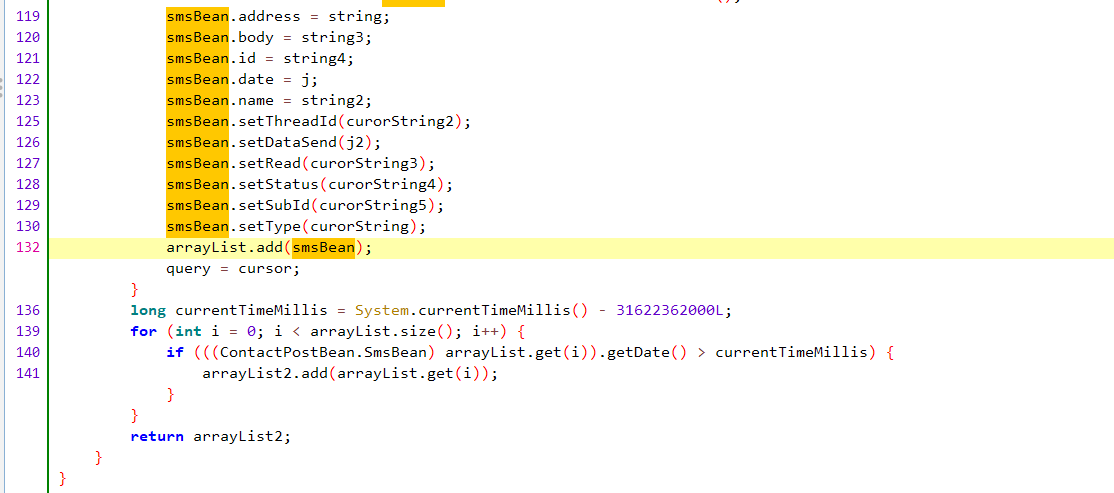
We will check line 3 as uri is declared

1. Double click the line 3 .

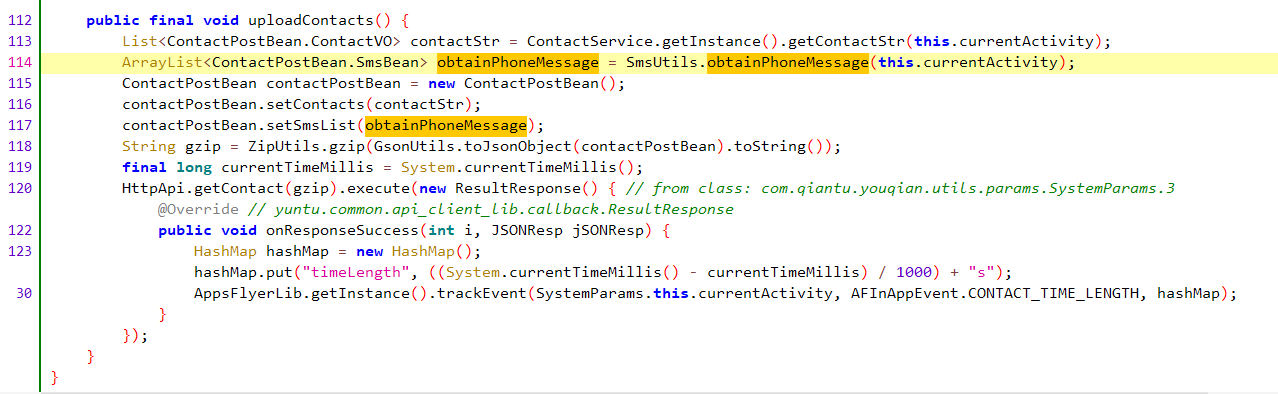
Here we can see that in obtainPhoneMessage( ) method arraylist of sms is being returned.





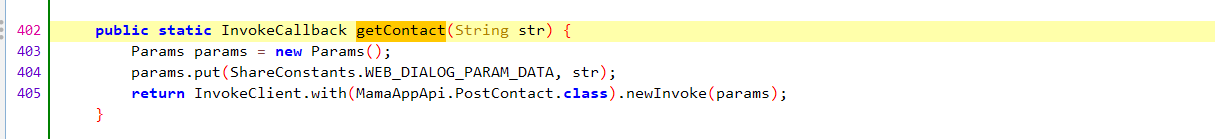


1. We will check the usage the obtainPhoneMessage( ) method to know where this method is being used.





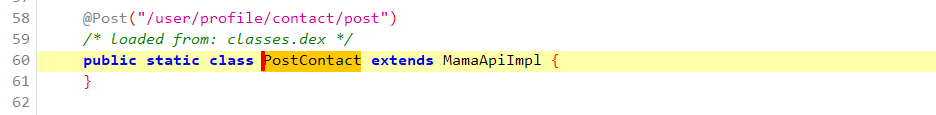
1. We will check the declaration of getContact( ) method used at **line 120.**





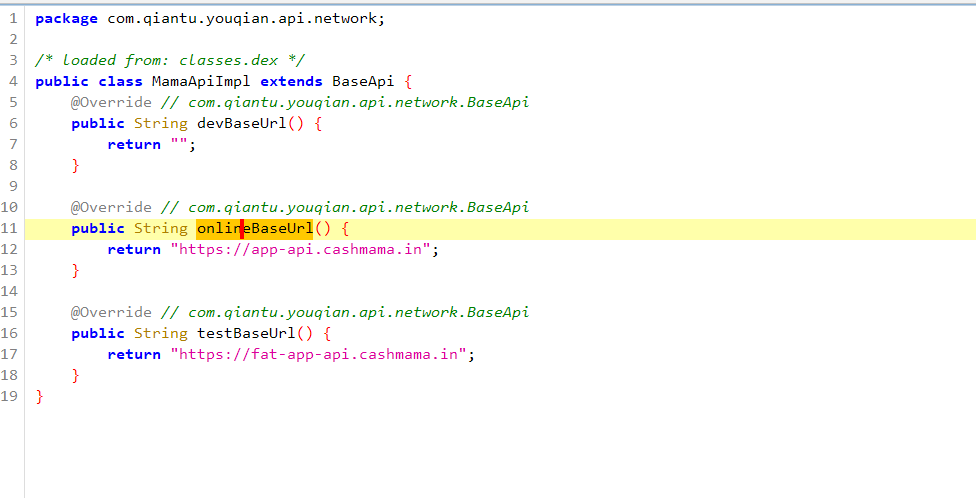
Here we can see that PostContact.class is being passed in a method at line 405 which is being returned.

1. We will check the declaration of PostContact.class



Here we can see post method is being defined

1. Now we will check declaration of MamaApiImpl class

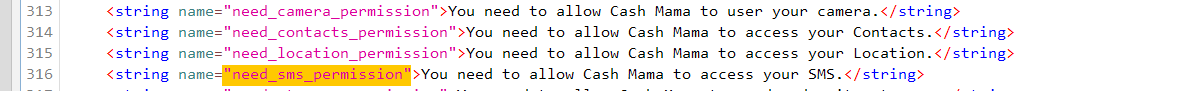




Here we can see that baseurl is being defined on which sms is passed.

1. Now we will check disclosure part.

Search sms keyword and check res/value/string.xml



Here we can see that app is requesting permission from user.

So this is not spyware.