**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

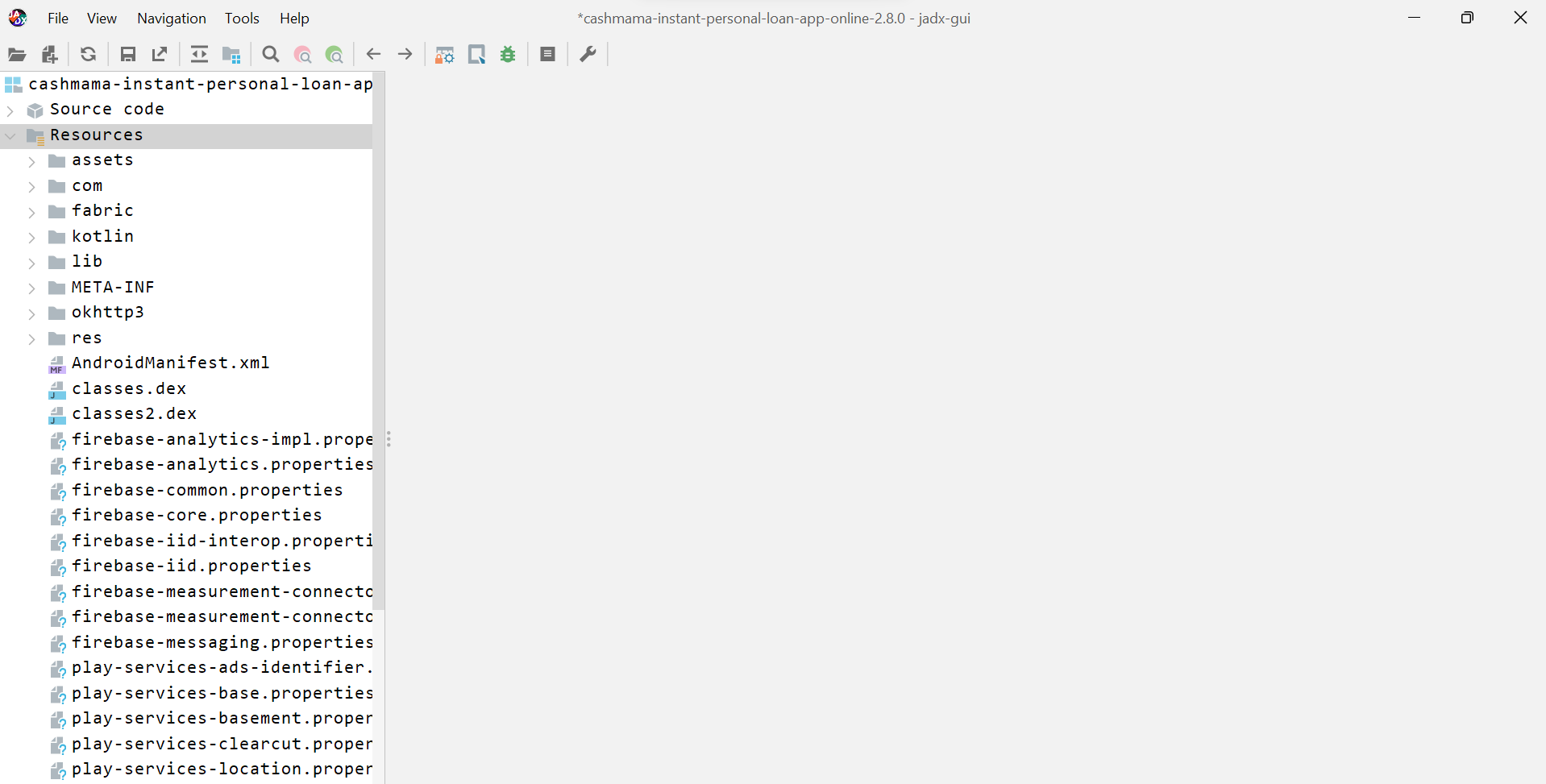
Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

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\_CONTACTS permission in androidmanifest.xml at **line 20** and

**READ\_SMS**  at **line 24 .**

A screenshot of a computer

Description automatically generated

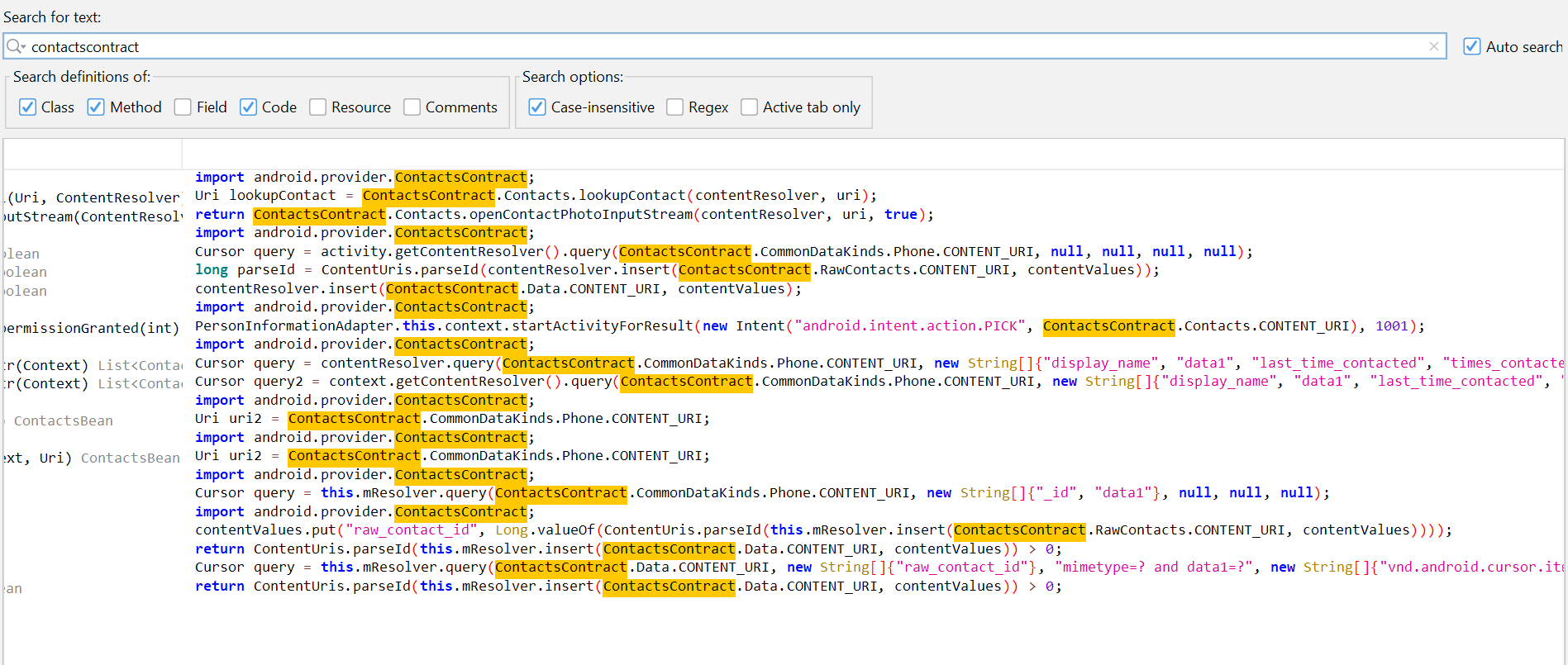
Here you can see READ\_CONTACTS permission which is suspicious related to spyware

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

1. Now click on  button in JADX to find for Contacts usage.
2. Search for **ContactsContract** as mentioned in below screenshot .

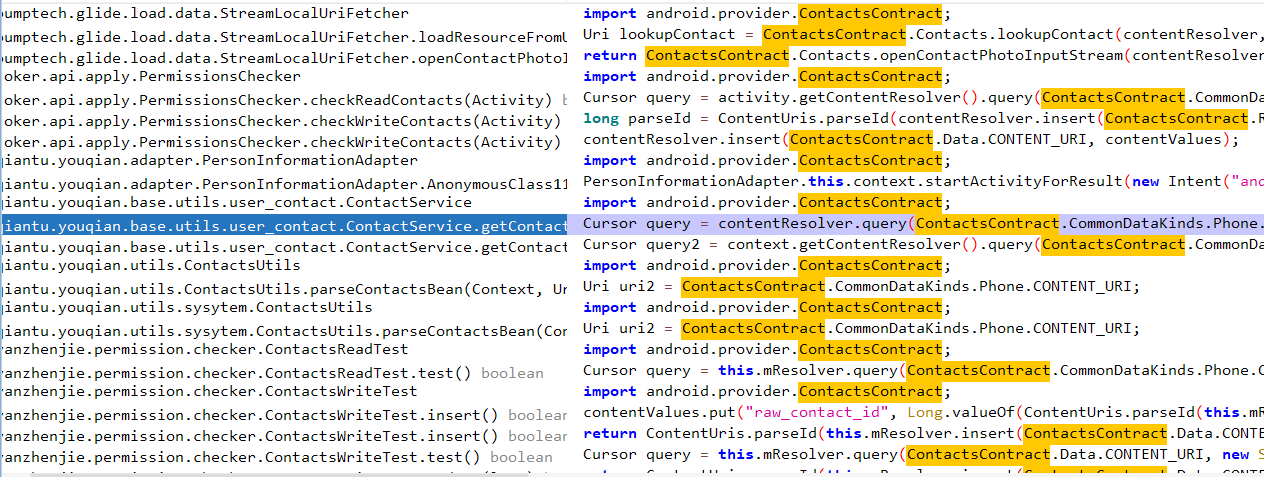
ContactsContract defines an extensible database of contact related information. The contact

between the contents provider and the applications



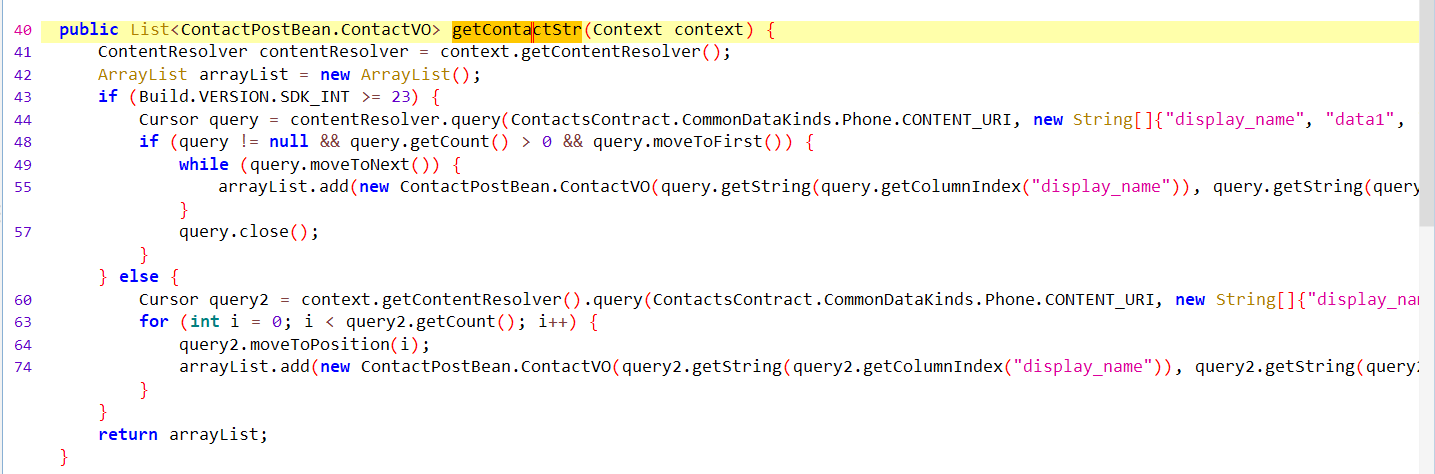
Make sure class, method, code, field and case-insensitive field is checked.

1. Go for **query** since you can find CommonDataKinds.Phone.CONTENT\_URI,null,null and getContentStr ( ) method is returning some value which can be used further.



1. Double click the query line.

Here you can see contactInfo is being added to the arraylist and that arraylist is returned to the getContactStr( ) method





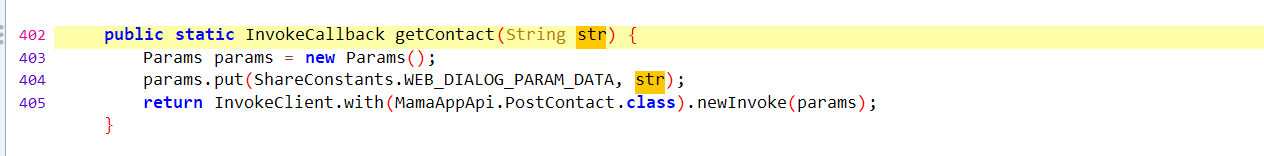
1. Right click on getContactStr( ) method and select find usage(x) to know where the getContactStr( ) method is being used.

A computer code with many text

Description automatically generated with medium confidence



1. Now check the declaration of getContact(gzip) method.





1. Check the declaration of PostContact.class

A close-up of a computer code

Description automatically generated

Here we can see that url is being post

1. Check the declaration of MamaApiImpl.class

A screenshot of a computer program

Description automatically generated



Here we can see that contact is being sent to baseurl.

1. Now check the disclosure in res/value/string.xml

A close up of text

Description automatically generated



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

So app is not spyware.