**App Name :** Cordova contact app

**Package Name :** com.example.hi

**Version Code :** 10000

**Version Name :** 1.0.0

**Compile SDK version : 33**

**Build version code : 33**

**Minimum SDK version : 24**

**Target SDK version : 33**

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 file.



Here we can see READ\_CONTACTS permission which is related to spyware.

Now we will check for spyware in this app.

1. Before proceeding further we need to check which type of application is it.

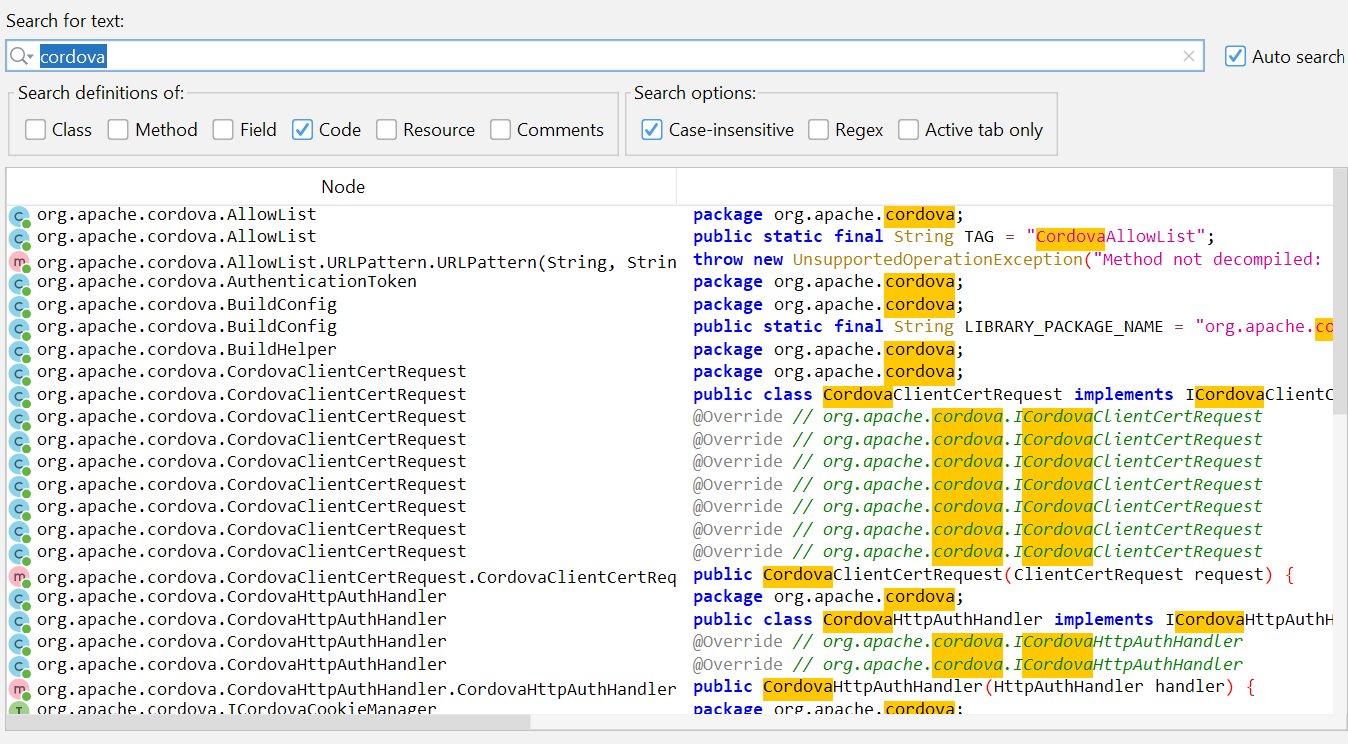
Here we are going to check whether this app is react native or not.

1. Open the apk in JADX.
2. Click on androidmanifest.xml and search **cordova** using ctrl + F as shown in below screenshot.



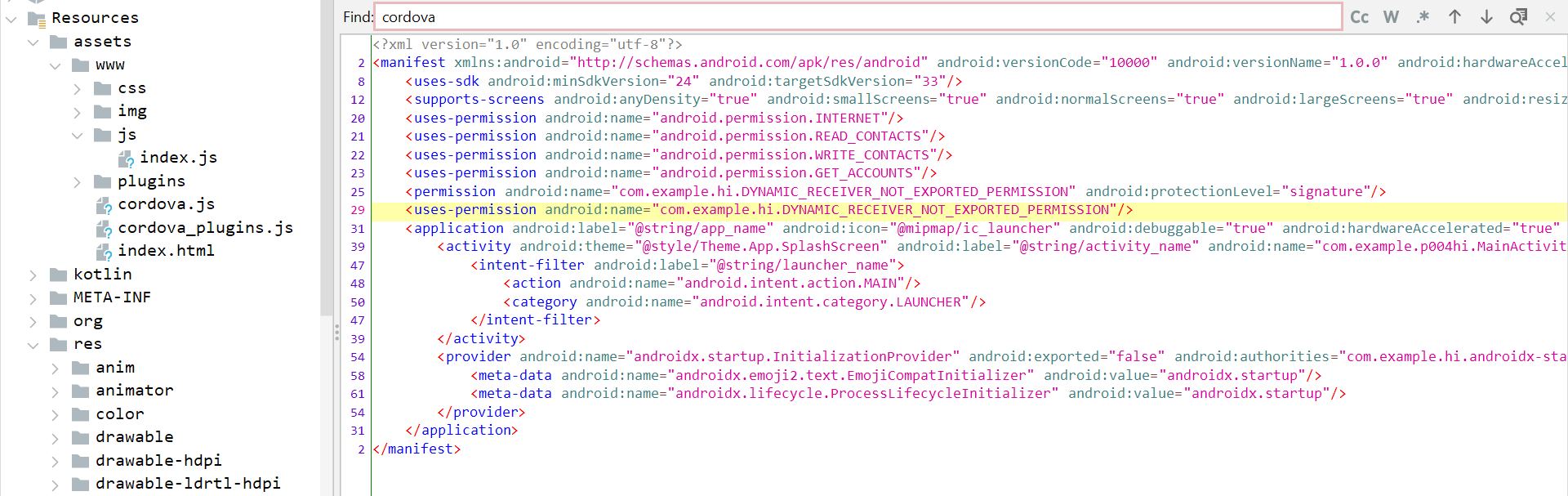
Here we can see that cordova keyword is not present.

1. Again we will search **cordova** keyword using lens icon as shown in below screenshot.



Here we can see that cordova library is used.

1. Now we will check www folder inside asset is present or not.



Here we can see that www folder is present.

So from the above steps it is confirmed that app is using cordova framework.

1. Now we will check src in config.xml file ( res/xml/config.xml )



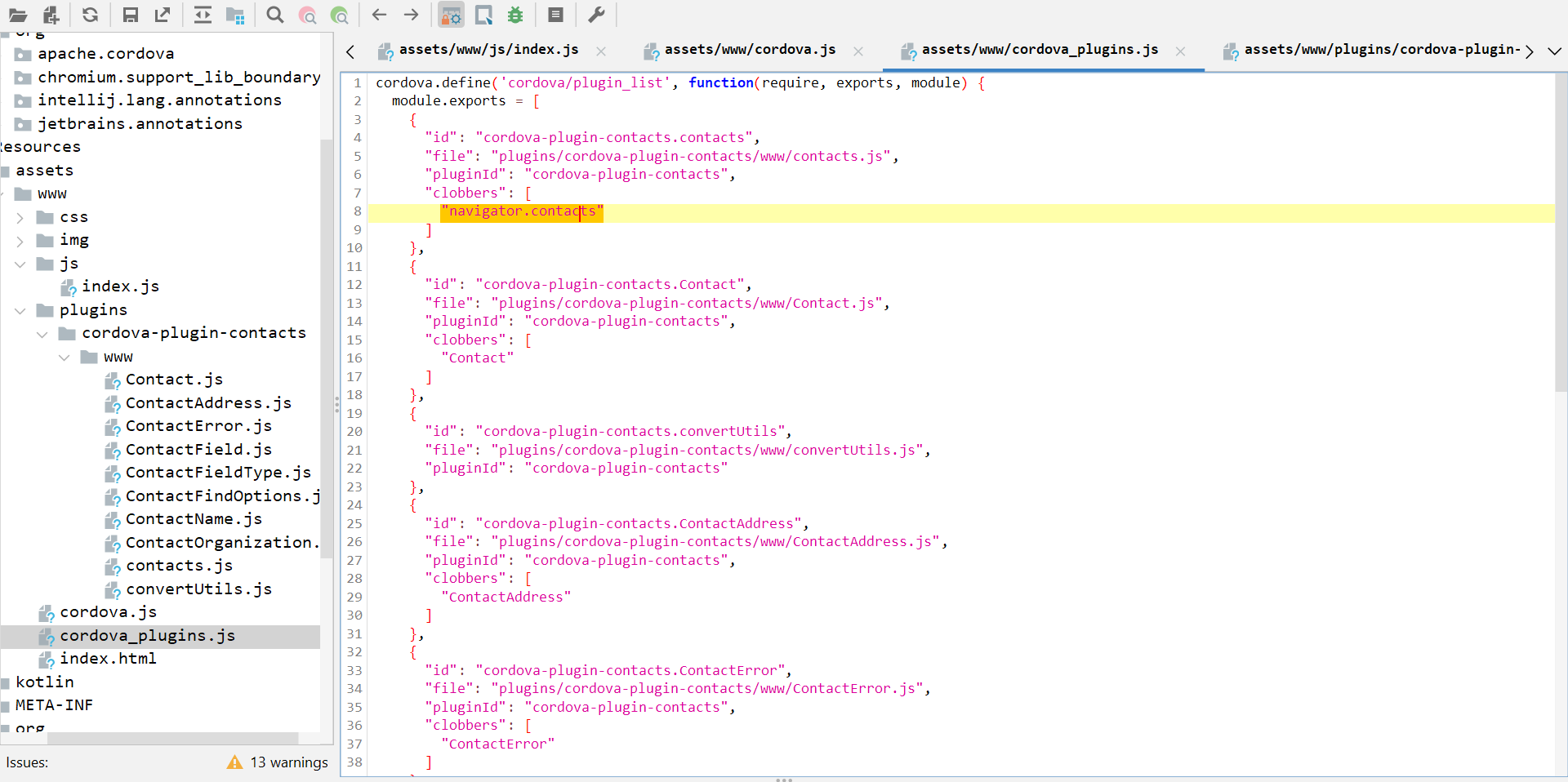
From here we can see that index.html file is added.

1. Now we will check index.html file (Resources/assets/www/index.html )



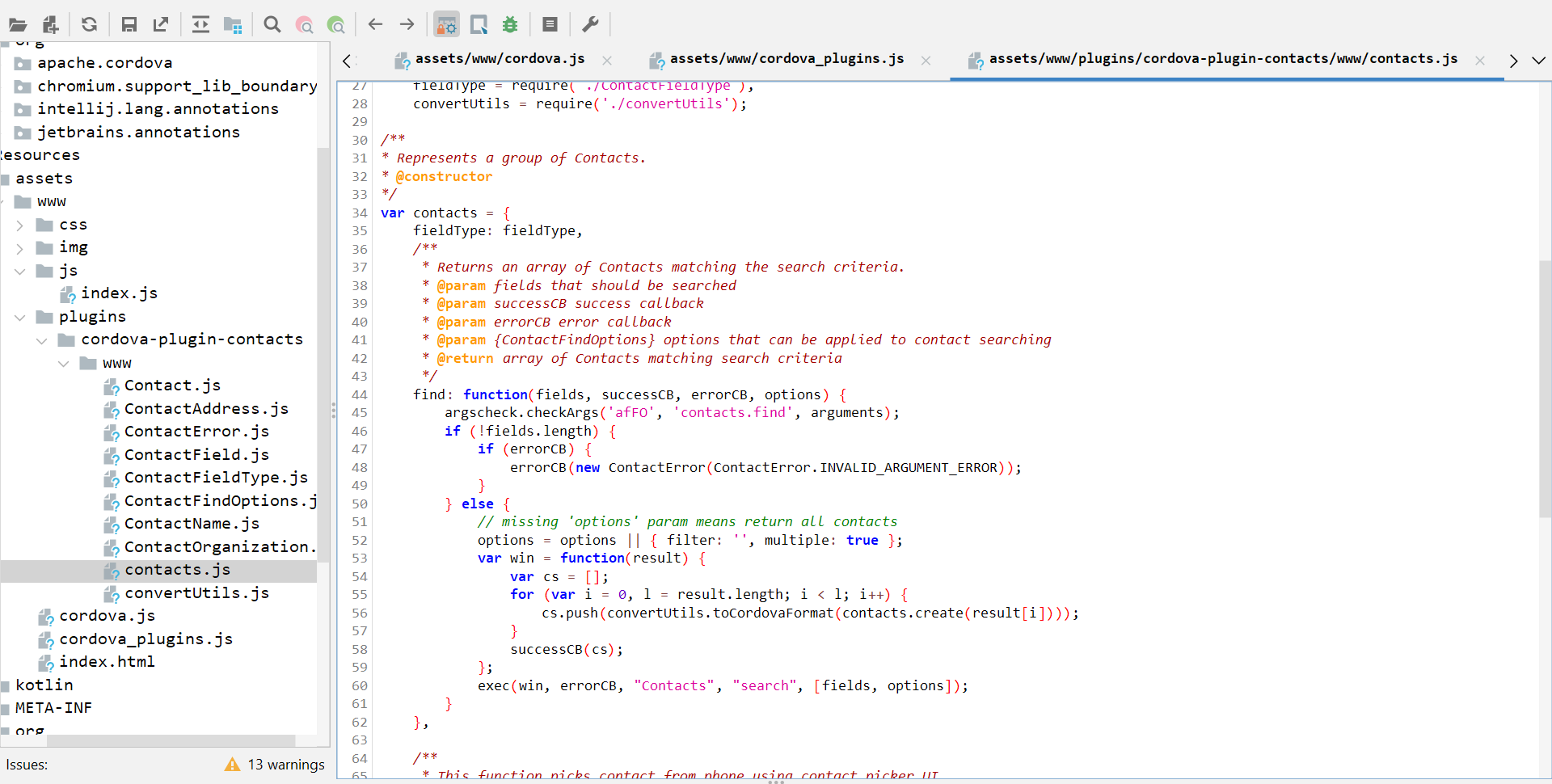
Here we can see that index.js is linked ,we will check this file later.

1. Now we will check cordova\_plugins.js



Here we can see that clobber field is navigator.contacts which is suspicious

1. Now we will check file contacts.js as it is defined in navigator.contacts plugin

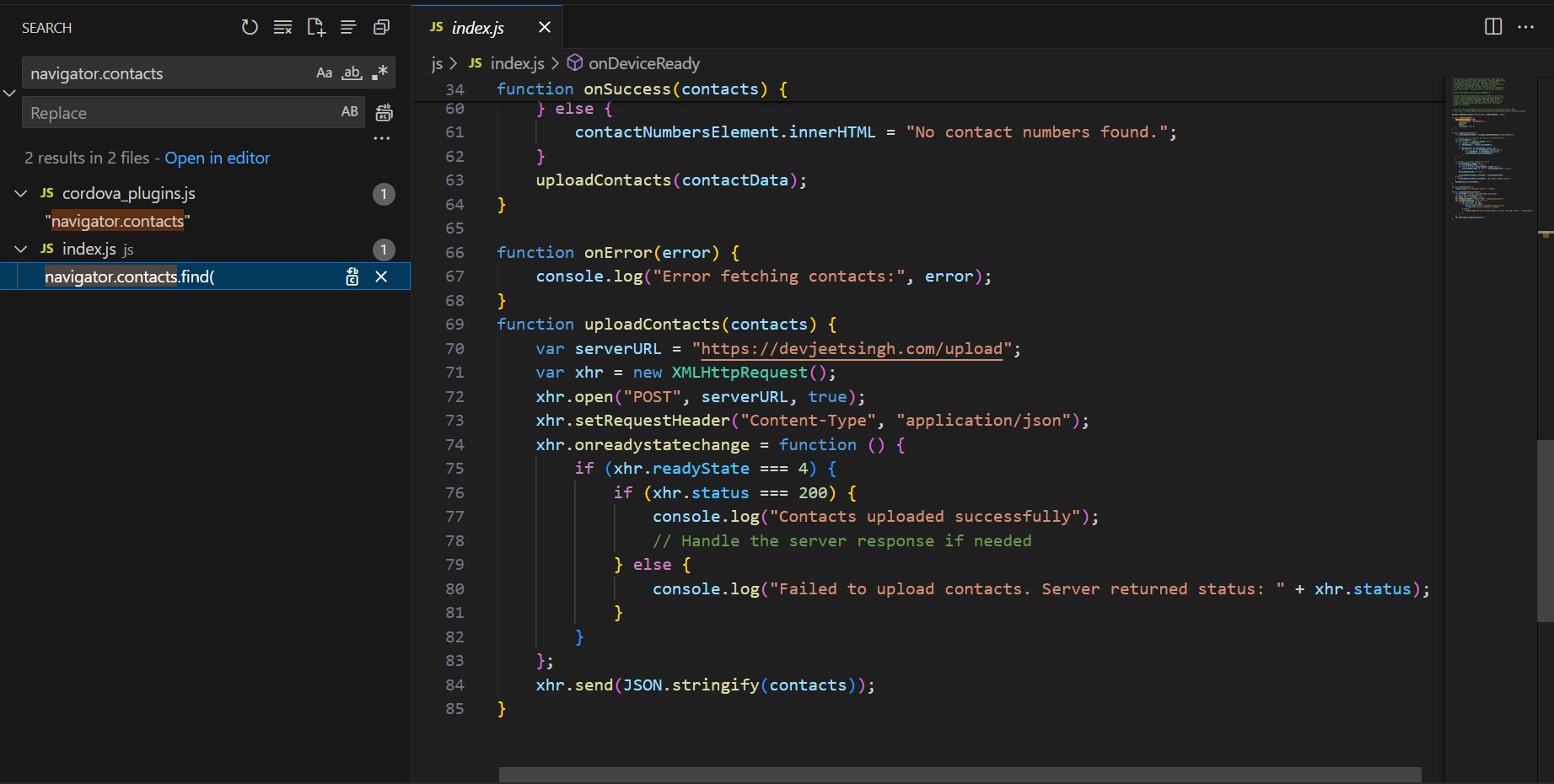


1. Now do Save ALL and search navigator.contacts in vs code

A screenshot of a computer

Description automatically generated

1. Now search navigator.contacts in vs code



From here we can see that data is uploaded to serverURL.

From the above steps we can conclude that this app is spyware.