JSDroid

General description

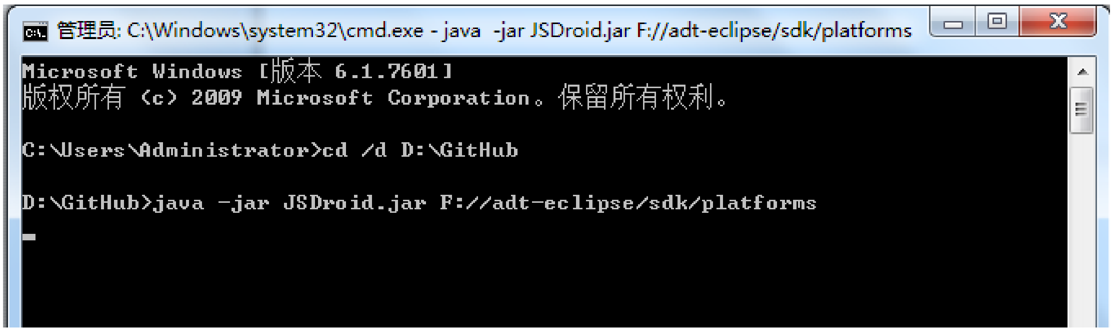
We herein present our tool named JSDroid which can automatically detect JavaScript-related vulnerabilities in large-scale Android apps. The input of JSDroid is a number of Android apps (APK files). The tool is used to detect whether these Android apps contain any of the three JavaScript-related vulnerabilities, including *File-based cross-zone vulnerabilities*, *WebView UXSS vulnerabilities*, and *JS-to-Java interface vulnerabilities*. Accordingly, the output of JSDroid is a vulnerability detection report showing the JavaScript-related vulnerabilities each app involves. In the folder "Samples", we provide some APK files of Android apps for readers to use/test our tool.

Usage

Please follow the steps to use JSDroid in Windows (other operating systems are similar):

1. **Open the file JSDroid.jar.** You can open the command line window and input the following command. Note that the parameter *android-platforms* represents the file path of android platforms in your machine.

   java –jar JSDroid.jar android-platforms


管理员: C:\Windows\system32\cmd.exe - java -jar JSDroid.jar F://adt-eclipse/sdk/platforms

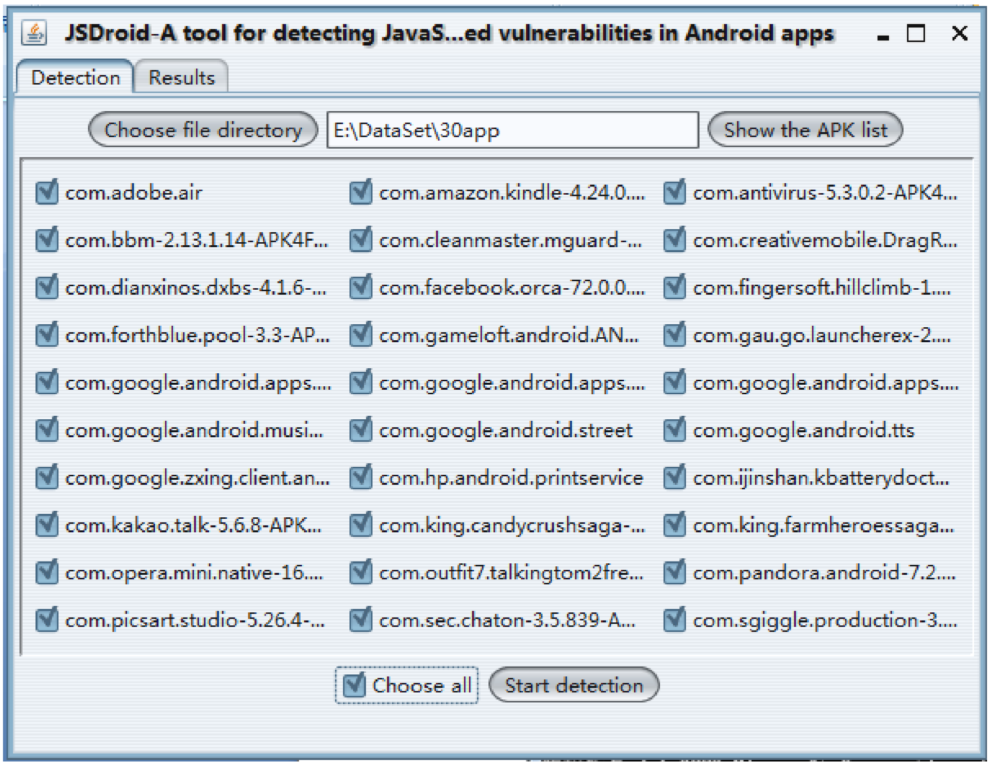
```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd /d D:\GitHub

D:\GitHub>java -jar JSDroid.jar F://adt-eclipse/sdk/platforms
_
```

2. **Choose APK files.** By Clicking "Choose file directory", you can choose the directory where your APK files located. You can click

"Show the APK list" to see all APK files in the directory. Here you can cancel the selection of some APK files.

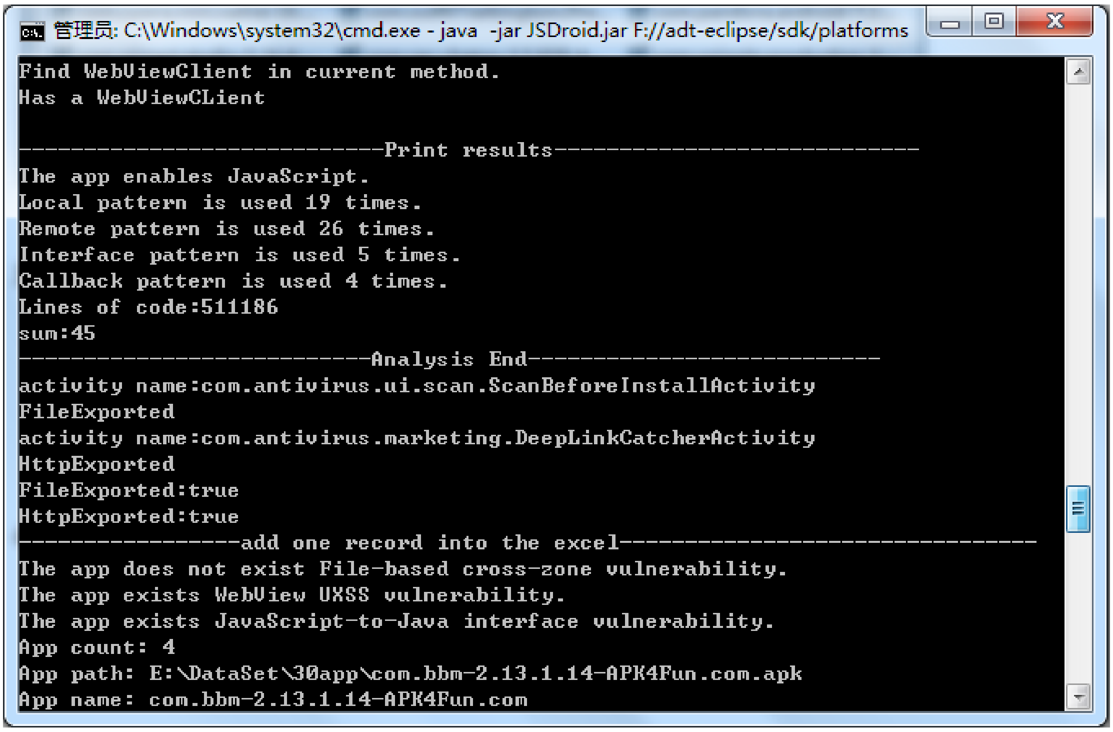

JSDroid-A tool for detecting JavaS...ed vulnerabilities in Android apps
Detection
Results
Choose file directory
Show the APK list
Start detection

E:\DataSet\30app

☑ com.adobe.air ☑ com.amazon.kindle-4.24.0.... ☑ com.antivirus-5.3.0.2-APK4...
☑ com.bbm-2.13.1.14-APK4F... ☑ com.cleanmaster.mguard-... ☑ com.creativemobile.DragR...
☑ com.dianxinos.dxbs-4.1.6-... ☑ com.facebook.orca-72.0.0.... ☑ com.fingersoft.hillclimb-1....
☑ com.forthblue.pool-3.3-AP... ☑ com.gameloft.android.AN... ☑ com.gau.go.launcherex-2....
☑ com.google.android.apps.... ☑ com.google.android.apps.... ☑ com.google.android.apps....
☑ com.google.android.musi... ☑ com.google.android.street ☑ com.google.android.tts
☑ com.google.zxing.client.an... ☑ com.hp.android.printservice ☑ com.ijinshan.kbatterydoct...
☑ com.kakao.talk-5.6.8-APK... ☑ com.king.candycrushsaga-... ☑ com.king.farmheroessaga...
☑ com.opera.mini.native-16.... ☑ com.outfit7.talkingtom2fre... ☑ com.pandora.android-7.2....
☑ com.picsart.studio-5.26.4-... ☑ com.sec.chaton-3.5.839-A... ☑ com.sgiggle.production-3....

☑ Choose all

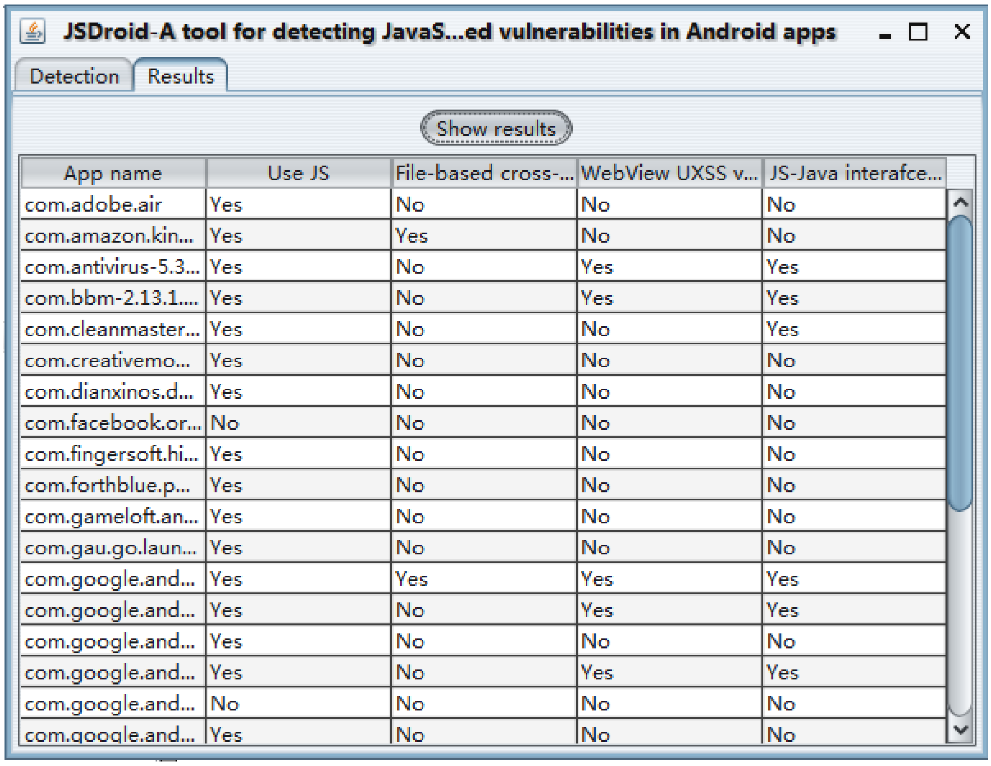
3. **Detect vulnerabilities.** After clicking "Start detection", you can start the detection of JavaScript vulnerabilities in the chosen apps. The detection process can be seen from the command line window.


管理员: C:\Windows\system32\cmd.exe - java -jar JSDroid.jar F://adt-eclipse/sdk/platforms

```
Find WebViewClient in current method.
Has a WebViewCLient

----------------------------Print results----------------------------
The app enables JavaScript.
Local pattern is used 19 times.
Remote pattern is used 26 times.
Interface pattern is used 5 times.
Callback pattern is used 4 times.
Lines of code:511186
sum:45
---------------------------Analysis End---------------------------
activity name:com.antivirus.ui.scan.ScanBeforeInstallActivity
FileExported
activity name:com.antivirus.marketing.DeepLinkCatcherActivity
HttpExported
FileExported:true
HttpExported:true
-----------------add one record into the excel-------------------------------
The app does not exist File-based cross-zone vulnerability.
The app exists WebView UXSS vulnerability.
The app exists JavaScript-to-Java interface vulnerability.
App count: 4
App path: E:\DataSet\30app\com.bbm-2.13.1.14-APK4Fun.com.apk
App name: com.bbm-2.13.1.14-APK4Fun.com
```

4. **Show results.** After the detection is completed, an excel file of the detailed results is generated in the current directory. You can also turn to the "Results" panel and click the "results". A table of the brief results will be shown in this panel.


JSDroid-A tool for detecting JavaS...ed vulnerabilities in Android apps
Detection
Results
Show results

App name	Use JS	File-based cross-...	WebView UXSS v...	JS-Java interafce...
com.adobe.air	Yes	No	No	No
com.amazon.kin...	Yes	Yes	No	No
com.antivirus-5.3...	Yes	No	Yes	Yes
com.bbm-2.13.1....	Yes	No	Yes	Yes
com.cleanmaster...	Yes	No	No	Yes
com.creativemo...	Yes	No	No	No
com.dianxinos.d...	Yes	No	No	No
com.facebook.or...	No	No	No	No
com.fingersoft.hi...	Yes	No	No	No
com.forthblue.p...	Yes	No	No	No
com.gameloft.an...	Yes	No	No	No
com.gau.go.laun...	Yes	No	No	No
com.google.and...	Yes	Yes	Yes	Yes
com.google.and...	Yes	No	Yes	Yes
com.google.and...	Yes	No	No	No
com.google.and...	Yes	No	Yes	Yes
com.google.and...	No	No	No	No
com.google.and...	Yes	No	No	No

More information

If you are interested in JSDroid and want to know more information about it, please refer to our paper:

Understanding JavaScript Vulnerabilities in Large Real-World Android Applications.