Mobile Application Pentesting-Part 5

Piyush Patil
May 17 · 3 min read ★

Andbug

It provides much more interactive shell compared to JDB

adb shell ps | grep -i bank =>to find PID

```
root@ornon:/scratch/ppatil/tools# adb shell ps | grep -i bank
u0_a140   30275 297   892220 50924 sys_epoll_ 00000000 S com.android.insecureban
k
```

andbug shell -p 30275

```
-- com.android.insecurebank.InsecureBankActivity
-- com.android.insecurebank.PostLogin
-- com.android.insecurebank.InsecureBankActivity$1
-- com.android.insecurebank.PostLogin$1
-- com.android.insecurebank.PostLogin$2
-- com.android.insecurebank.LoginScreen
-- com.android.insecurebank.Preferences
-- com.android.insecurebank.LoginScreen$1
-- com.android.insecurebank.LoginScreen$2
-- com.android.insecurebank.RestClient
```

methods class_path

```
>> methods com.android.insecurebank.RestClient
## Methods Lcom/android/insecurebank/RestClient;
   -- com.android.insecurebank.RestClient.<init>()V
   -- com.android.insecurebank.RestClient.doLogin(Ljava/lang/String;Ljava/lang/S
      tring;Ljava/lang/String;Ljava/lang/String;)I
   -- com.android.insecurebank.RestClient.dotransfer(Ljava/lang/String;Ljava/lan
      g/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)I
   -- com.android.insecurebank.RestClient.getHttpContent(Ljava/lang/String;)Ljav
      a/lang/String;
   -- com.android.insecurebank.RestClient.parseError(Ljava/lang/String;)I
   -- com.android.insecurebank.RestClient.postHttpContent(Ljava/lang/String;Ljav
      a/util/Map;)Ljava/lang/String;
   -- com.android.insecurebank.RestClient.sidechannel(Ljava/lang/String;Ljava/la
      ng/String;)V
```

We can hook into these methods using **method-trace** command and monitor them while the application is running. If you want to analyze all the methods within a class, you can simply run **ct** command, which is short for **class-trace**.

method-trace com.android.insecurebank.RestClient.dotransfer

When you click on Transfer ,you see the all parameters

One of drawback of Andbug is it does not allow bydefault to setup breakpoint and change the variable at that point of time.

adb forward tcp:localport jdwp:App_PID

jdb -attach localhost:localport

classes => show all the classes

methods com.android.insecurebank.RestClient

stop in com.android.insecurebank.RestClient.dotransfer

locals =>to see all parameters

We can also change any parameter and forward it.

set amount=”50"

locals => to see if it changed or not

resume

. . .

Android Backup Vulnerability

Android allows backups and restoration of its data. Attacker could take the backup of the app, modify the contents and restore it back again.

https://sourceforge.net/projects/adbextractor/

Extract the downloaded folder from sourceforge, there will be **abe.jar .**

adb backup package_name -f backup.ab

java -jar abe.jar unpack backup.ab backup.tar

tar -tf backup.tar > backup.list

tar -xvf backup.tar

//Editing//

Android Security Cybersecurity Bug Bounty Penetration Testing

50 claps

WRITTEN BY

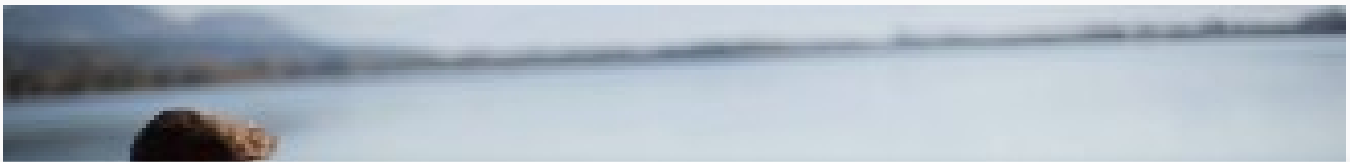
Piyush Patil

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Follow

More From Medium

Top on Medium



Do They All Want To Sleep With Me? — And Other Questions Of A Guys' Girl

Tesia Blake in P.S. I Love You
Nov 21 · 7 min read ★

Top on Medium

How to Predict the End of a Relationship

Colleen Murphy in Mindful Muse

Nov 22 · 5 min read ★

2.4K