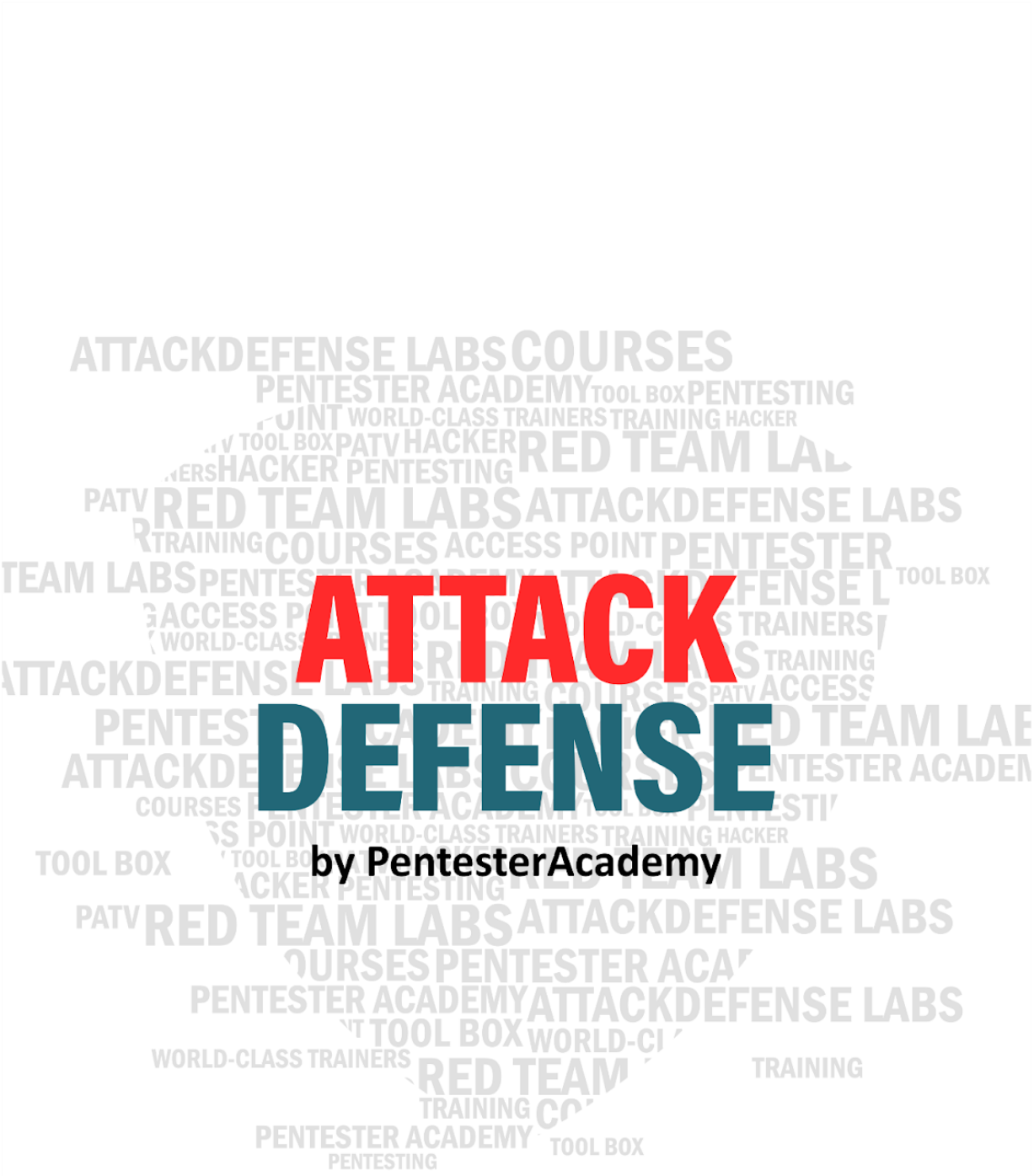

ATTACK
DEFENSE
by PentesterAcademy

Name	Bad Permission II
URL	https://attackdefense.com/challengedetails?cid=1624
Type	Android Pentesting : Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Use aapt to extract the permissions from APK and identify the unnecessary/ suspicious permission.

Solution:

Step 1: Start the lab and check the contents of the home directory.

Command: ls -l

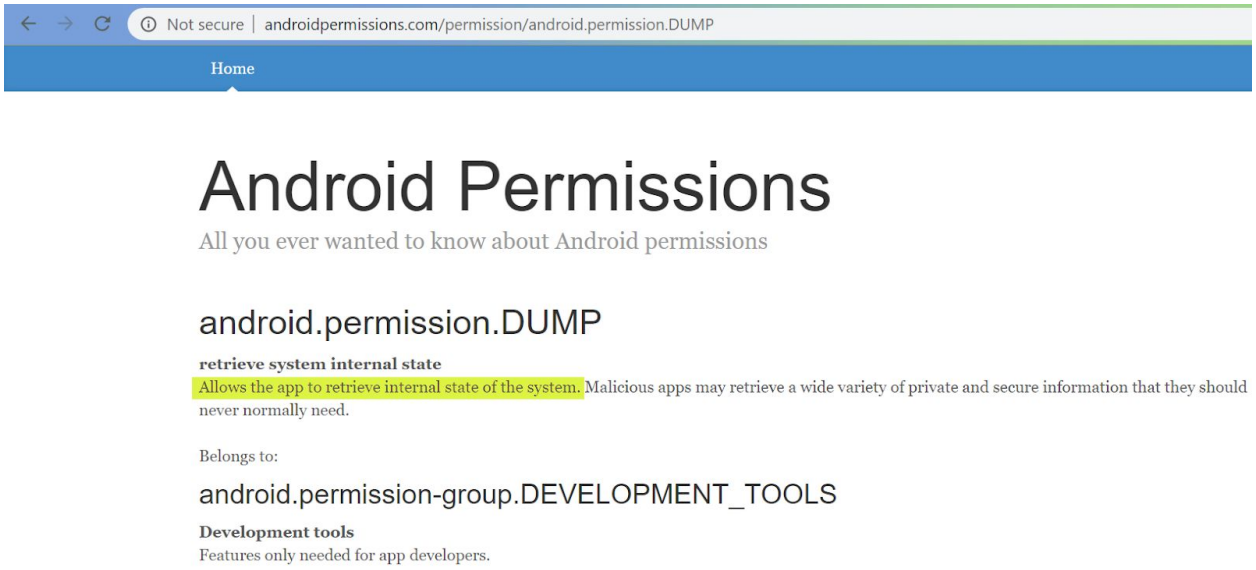
```
root@attackdefense:~# ls -l
total 64
-rw-r--r-- 1 root root 61662 Jan 22 22:45 sample-expense-manager.apk
root@attackdefense:~#
```

Step 2: Dump the permissions from APK using aapt tool and check these permissions

Command: aapt dump permissions sample-expense-manager.apk

```
root@attackdefense:~# aapt dump permissions sample-expense-manager.apk
package: com.code44.finance
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.ACCESS_NETWORK_STATE'
uses-permission: name='android.permission.GET_ACCOUNTS'
uses-permission: name='android.permission.USE_CREDENTIALS'
uses-permission: name='android.permission.WAKE_LOCK'
uses-permission: name='android.permission.WRITE_EXTERNAL_STORAGE'
uses-permission: name='android.permission.READ_EXTERNAL_STORAGE'
uses-permission: name='com.google.android.c2dm.permission.RECEIVE'
uses-permission: name='android.permission.DUMP'
uses-permission: name='android.permission.CAMERA'
root@attackdefense:~#
```

Step 3: The android.permission.DUMP allows the application to retrieve the internal state of the system.



There is no reason for an expense manager application to have this permission. So, this is the answer.

References:

1. AndroidManifest.xml (https://developer.android.com/guide/topics/manifest/manifest-intro)
2. Information on permissions: http://androidpermissions.com/
3. DUMP (http://androidpermissions.com/permission/android.permission.DUMP)
4. Base AndroidManifest.xml is taken from here: https://github.com/mvarnagiris/financius