



OWASP

Open Web Application
Security Project

Android Mobile Application Pentesting

Williams

wyohanes96@gmail.com

OWASP

29 April 2018



OWASP

Open Web Application
Security Project

Who Am I ?

Who Am I



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~
GNU nano 2.5.3 File: whoami Modified
1. Perkenalkan nama saya williams(aja!).
2. punya mimpi untuk kerja di Google.
3. Masih Muda, jangan dipanggil bapak. Umur saya masih (17+25)/2
4. Sekarang Kuliah di Binus International semester 8, lagi melakukan riset.
5. Sekarang sedang magang ke-3 di PT Datacomm.
6. Salah Satu core member Indonesia HoneyNet Project
7. Sedang menekuni Penetration Testing Android Mobile dan Buffer Overflow
8. Punya blog: http://court-of-testing-analysing.blogspot.co.id/
(materi hari ini saya upload disini)

[ Unknown Command ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Noted to all audience:



OWASP
Open Web Application
Security Project

Semua materi yang diberikan dalam pertemuan hanya untuk tujuan pendidikan. Kerusakan yang terjadi pada suatu aplikasi sistem bukan merupakan tanggung jawab dari pengarang

Peace out yoo!



OWASP

Open Web Application
Security Project

Android Mobile Application Security Testing



OWASP

Open Web Application
Security Project

**TARGET
ACQUIRED!**



Source:

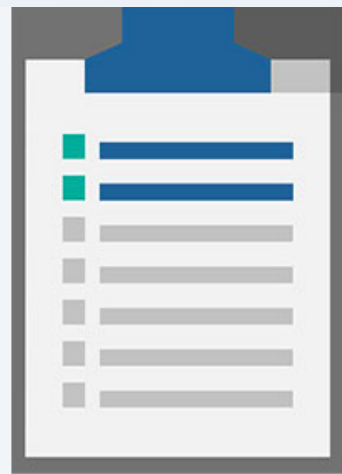


OWASP
Open Web Application
Security Project

OWASP Mobile Security Project



OWASP
Mobile Security Project



Mobile App Security Checklist

A checklist for use in security assessments. Also contains links to the MSTG test case for each requirement. The current release is [version 1.0](#).

Source:

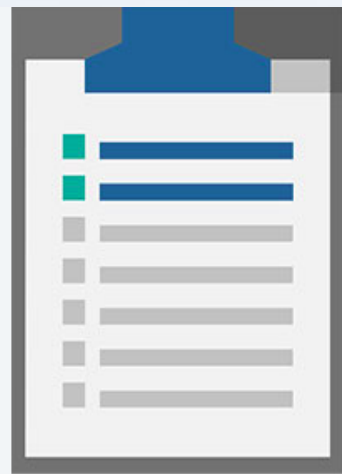


OWASP
Open Web Application
Security Project

OWASP Mobile Security Project



OWASP
Mobile Security Project



Mobile App Security Checklist

A checklist for use in security assessments. Also contains links to the MSTG test case for each requirement. The current release is [version 1.0](#).

FREE

OWASP Mobile top 10 Vulnerability



Top 10 Mobile Risks - Final List 2016

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

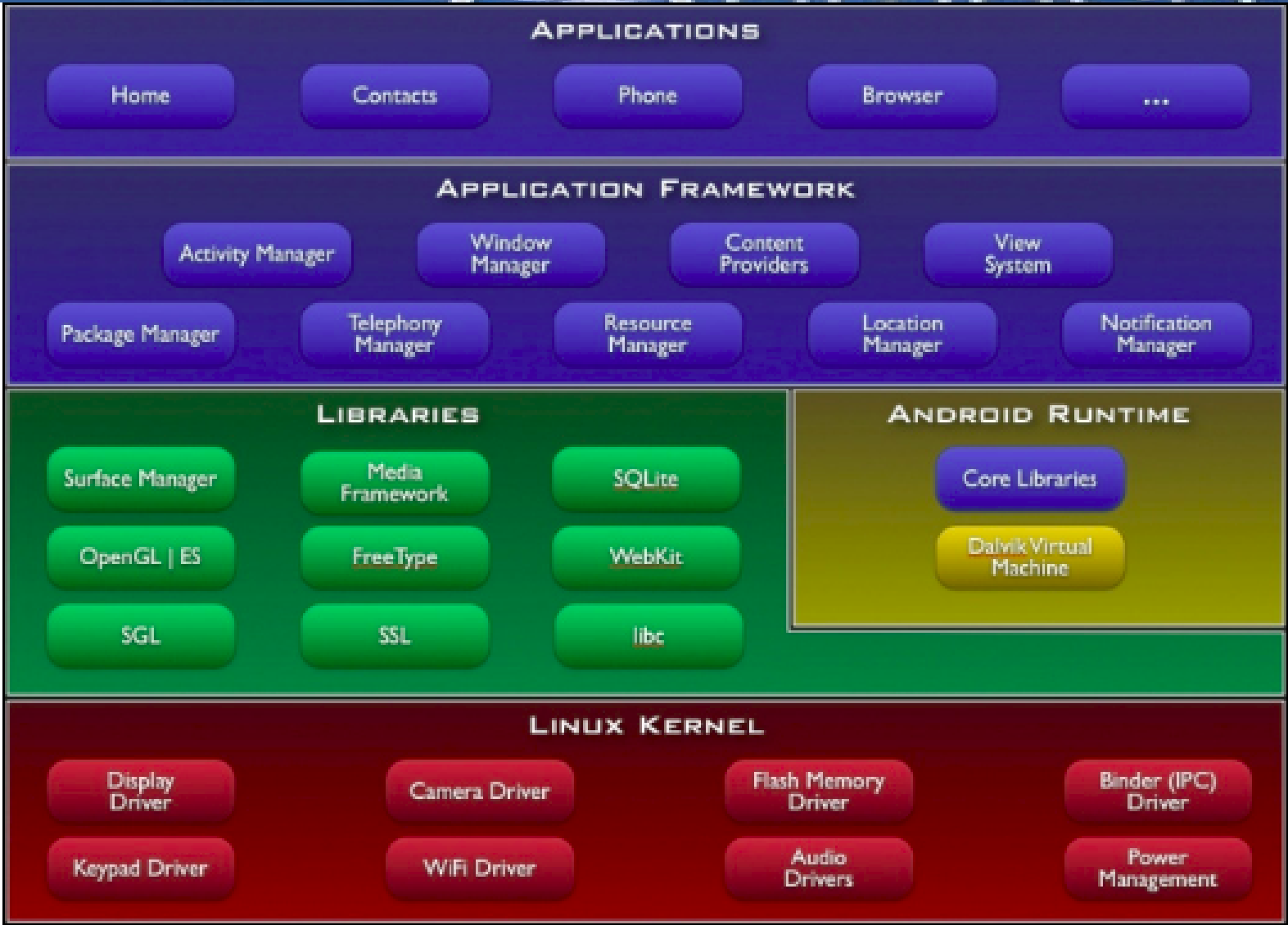
Application

Application framework

Native Libraries

Android Runtime

Linux Kernel



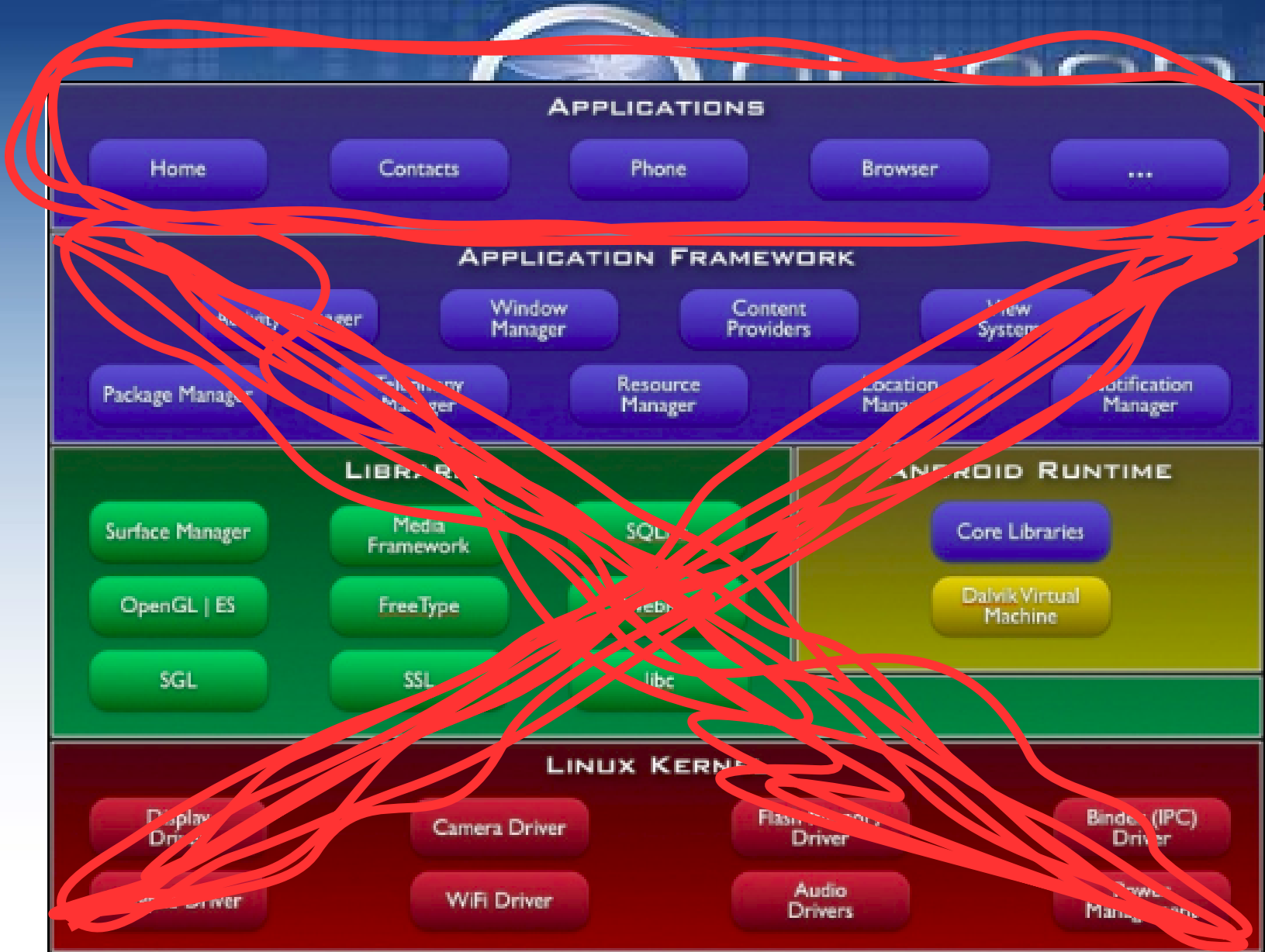
Application

Application framework

Native Libraries

Android Runtime

Linux Kernel



Android Application Package



OWASP

Open Web Application
Security Project

It is just a zip file

Android Application Package

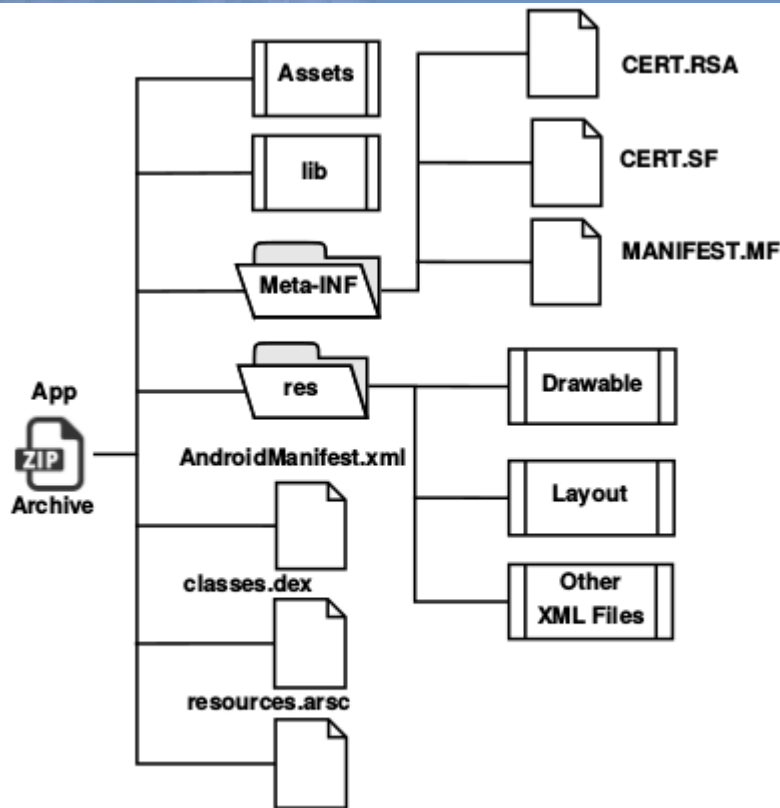


Fig. 2: Android PacKage (APK) Structure

A. App Structure

Android app is packaged into an APK `.apk`, a zip archive consisting several files and folders as shown illustrated in Figure 2. In particular, the `AndroidManifest.xml` stores the meta-data such as package name, permissions required, definitions of one or more components like Activities, Services, Broadcast Receivers or Content Providers, minimum and maximum version support, libraries to be linked etc.. Folder `res` stores icons, images, string/numeric/color constants, UI layouts, menus, animations compiled into the binary. Folder `assets` contains non-compiled resources. Executable file `classes.dex` stores the Dalvik bytecode to be executed on the Dalvik Virtual Machine. `META-INF` stores the signature of the app developer certificate to verify the third party developer identity.

Android Application Package

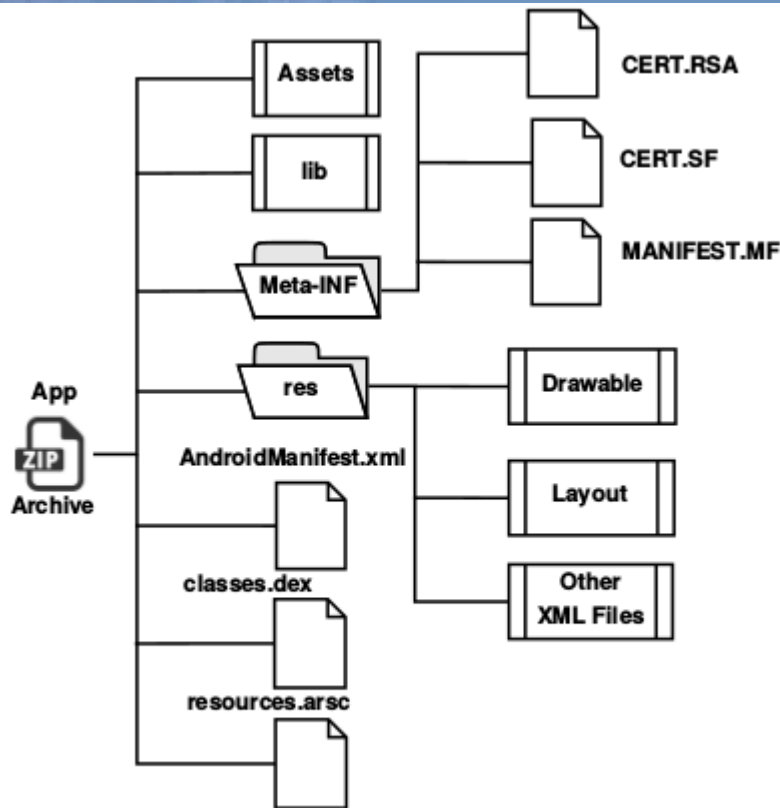


Fig. 2: Android PacKage (APK) Structure

A. App Structure

Android app is packaged into an APK .apk, a zip archive consisting several files and folders as shown illustrated in Figure 2. In particular, the AndroidManifest.xml stores the meta-data such as package name, permissions required, definitions of one or more components like Activities, Services, Broadcast Receivers or Content Providers, minimum and maximum version support, libraries to be linked etc.. Folder res stores icons, images, string/numeric/color constants, UI layouts, menus, animations compiled into the binary. Folder assets contains non-compiled resources. Executable file classes.dex stores the Dalvik bytecode to be executed on the Dalvik Virtual Machine. META-INF stores the signature of the app developer certificate to verify the third party developer identity.

Android Application Package

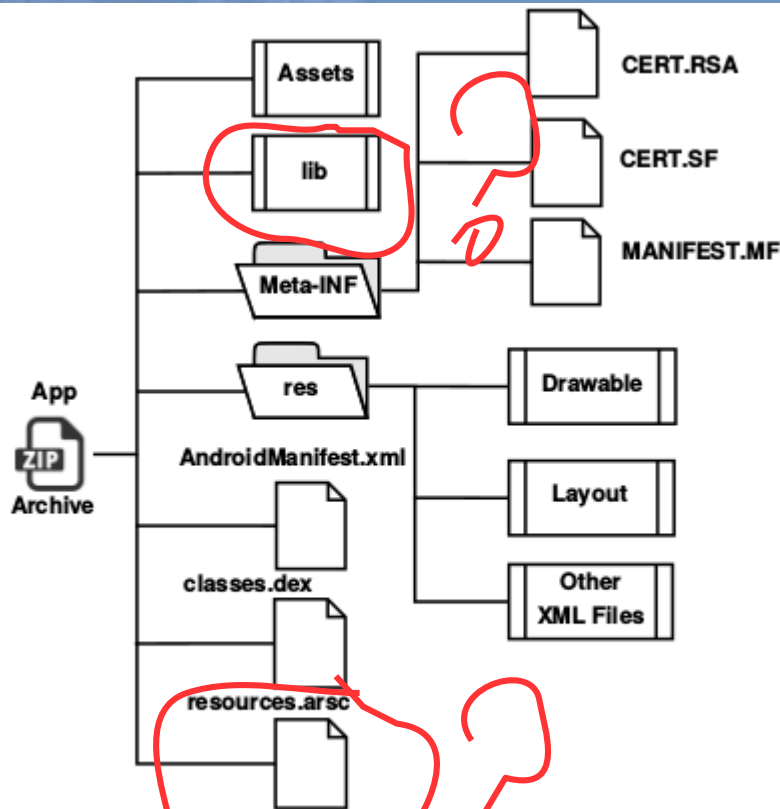


Fig. 2: Android Package (APK) Structure

A. App Structure

Android app is packaged into an APK .apk, a zip archive consisting several files and folders as shown illustrated in Figure 2. In particular, the AndroidManifest.xml stores the meta-data such as package name, permissions required, definitions of one or more components like Activities, Services, Broadcast Receivers or Content Providers, minimum and maximum version support, libraries to be linked etc.. Folder res stores icons, images, string/numeric/color constants, UI layouts, menus, animations compiled into the binary. Folder assets contains non-compiled resources. Executable file classes.dex stores the Dalvik bytecode to be executed on the Dalvik Virtual Machine. META-INF stores the signature of the app developer certificate to verify the third party developer identity.



OWASP

Open Web Application
Security Project

What is an ARSC file?

Application resource file used by programs developed for Google's Android mobile operating system; contains compiled resources in a binary format; may include images, strings, or other data used by the program; usually included in an [.APK](#) package file.

Taken from fileinfo.com

OWASP Mobile top 10 Vulnerability



Top 10 Mobile Risks - Final List 2016

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

OWASP Mobile top 10 Vulnerability



First step into android mobile application penetration testing is to try reverse engineer the application because once u get the code u already do half of the works

wait

With APKTOOLS



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
williams@williams-HP-Pavilion-14-Notebook-PC:~/Documents/android_pentest_tools/a
pk_folder$ java -jar ../apktool/apktool_2.3.0.jar decode --no-src Notes_v2.1.9_a
pkpure.com.apk
I: Using Apktool 2.3.0 on Notes_v2.1.9_apkpure.com.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/williams/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
W: Cant find 9patch chunk in file: "u/cs.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "a0/ct.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "m/cq.9.png". Renaming it to *.png.
```

With Dex2jar



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
williams@williams-HP-Pavilion-14-Notebook-PC:~/Documents/android_pentest_tools/a
pk_folder$ ../dex2jar/dex2jar.sh Notes_v1.1_apkpure.com/classes.dex -o notes.jar
```

With jdx-core



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
williams@williams-HP-Pavilion-14-Notebook-PC:~/Documents/android_pentest_tools/a
pk_folder$ java -jar ../jd-core.jar Notes_v1.1_apkpure.com/classes_dex2jar.jar .
./notes
```

With jdx-core



OWASP
Open Web Application
Project

Open ▾



Save

```
        return;
        if (a == 0) {
            d();
        }
    }
}
a = 2;
finish();
}

public void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    getWindow().setSoftInputMode(3);
    setContentView(2130903047);
    a();
    b = new c(this);
    Bundle localBundle = getIntent().getExtras();
    if (localBundle != null)
    {
        String str1 = localBundle.getString("android.intent.extra.SUBJECT");
        String str2 = localBundle.getString("android.intent.extra.TEXT");
        if (str1 != null) {
            e.setText(str1);
        }
        if (str2 != null) {
            f.setText(str2);
        }
        if ((str1 != null) || (str2 != null)) {
            break label127;
        }
    }
}
label127:
for (Long localLong = Long.valueOf(localBundle.getLong("_id")); localLong = null)
{
    d = localLong;
    if (d == null) {
        break;
    }
    a = 1;
}
```

Java ▾

Tab Width: 8 ▾

Ln 149, Col 44 ▾

INS

Where to get Free apk other than play store?



Apkpure

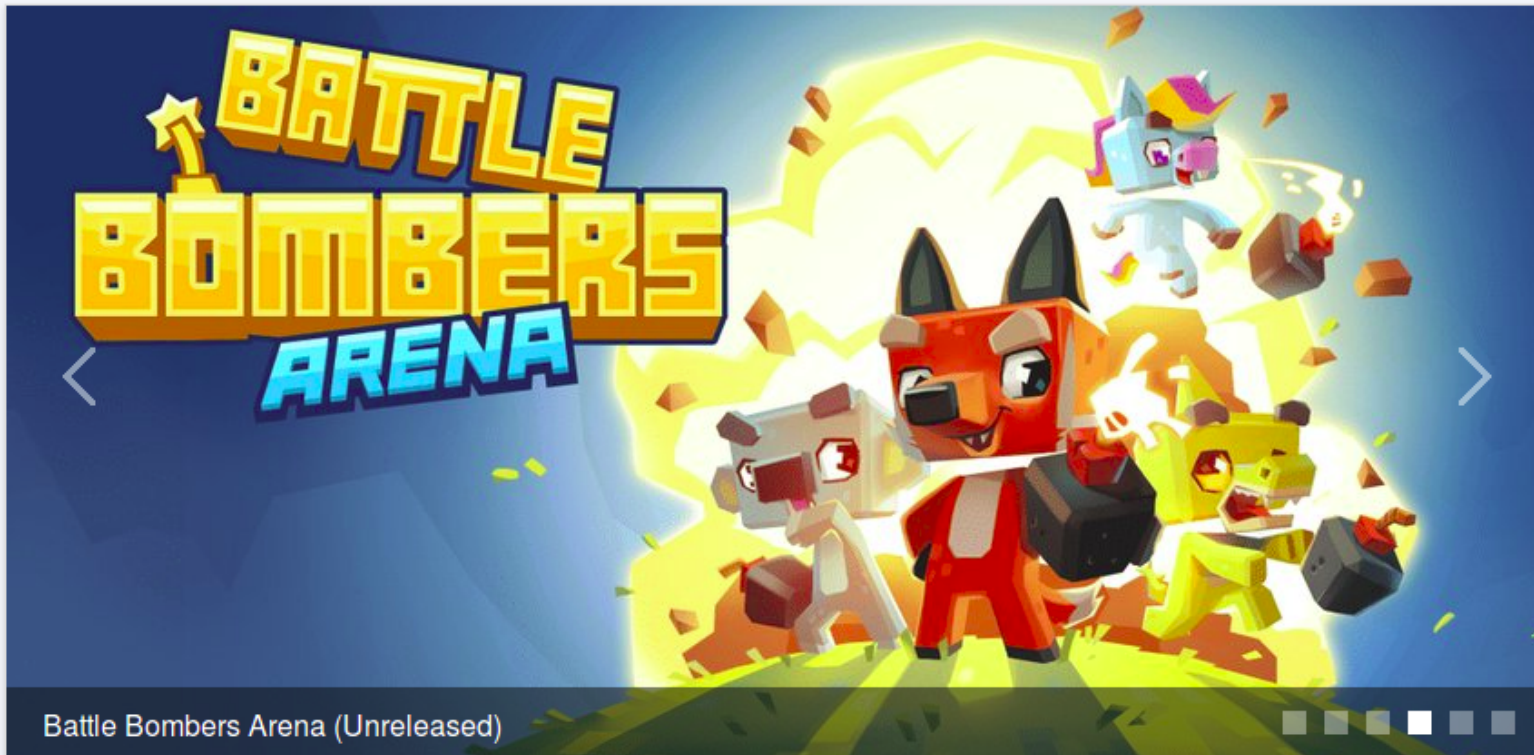
GAMES

APPS

TOPICS

PRODUCTS

EN



APKPure or com.apkpure.aegon



pes 2017

minecraft pocket edition

instagram

youtube

리니지m

pes 2018

gta san andreas

clash of clans

google play services



APKPure 2.7.3



Using APKPure App

Faster, free and saving data!

Download APK (8.1 MB)



30.2K



23.7K

Improper Platform Usage



OWASP

Open Web Application
Security Project



Improper Platform Usage



Android Components

Application components are the essential building blocks of an Android application.



Learn Android Development Free Complete Course 

Improper Platform Usage



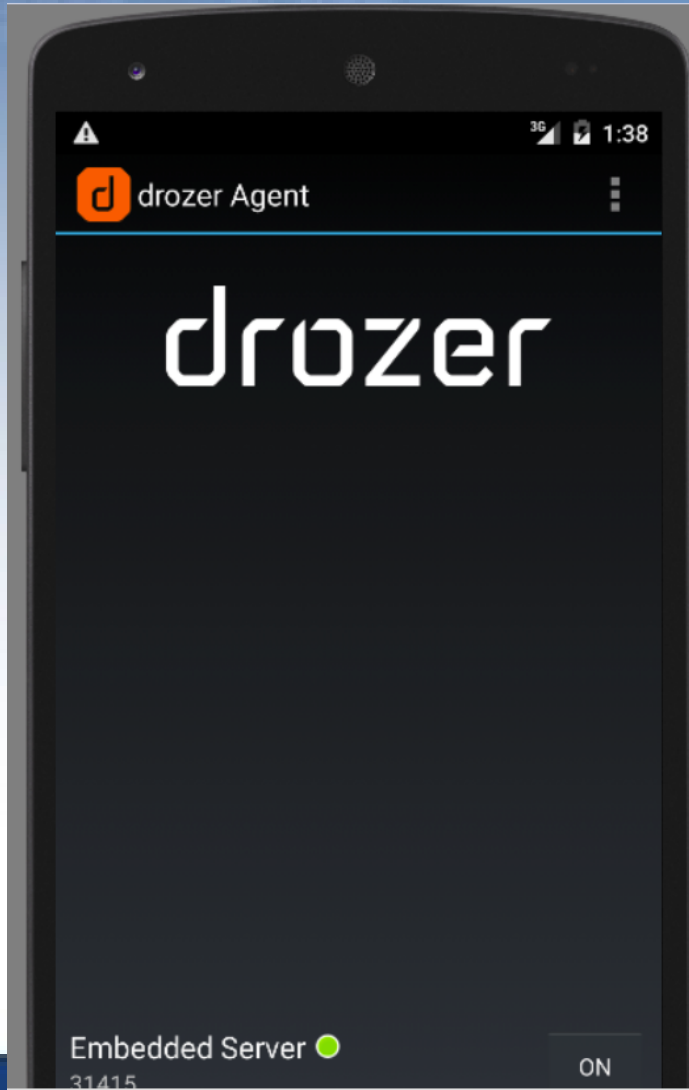
Android Components

Application components are the essential building blocks of an Android application.



Learn Android Development Free Complete Course

A Good Tools that every android pentester must have



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\U[redacted]ar>adb forward tcp:31415 tcp:31415
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

C:\Us[redacted]r>adb forward tcp:31415 tcp:31415

C:\U[redacted]r>drozer console connect
Selecting 6e4562a25327cff (unknown sdk_google_phone_armv7 5.0.2)

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

drozer Console (v2.3.4)
dz>
```

Taken from mac afee blog. All right reserved to the author

Target:



OWASP

Open Web Application
Security Project



QuickNote Notepad Notes APK



★★★★☆ 4.1/5 (0 Discussions)

Author:

Xlusion

Latest Version:

1.2.8

Publish Date:

2014-06-18

Download APK (676.6 KB)



Improper Platform Usage



OWASP

Open Web Application

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
dz> run app.activity.info -a com.xllusion.quicknote
Package: com.xllusion.quicknote
  com.xllusion.quicknote.QuickNote
    Permission: null
  com.xllusion.quicknote.EditNote
    Permission: null
  com.xllusion.quicknote.WidgetConfig
    Permission: null
dz> |
```

```
<activity android:name=".EditImage" android:theme="@style/Theme.quicknote"/>
<activity android:name=".ViewImage" android:theme="@style/Theme.quicknote"/>
-<activity android:name=".EditNote" android:theme="@style/Theme.quicknote">
```

Improper Platform Usage



```
Open [icon] Save Application
ct

return;
if (a == 0) {
    d();
}
}
}
a = 2;
finish();
}

public void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    getWindow().setSoftInputMode(3);
    setContentView(2130903047);
    a();
    b = new c(this);
    Bundle localBundle = getIntent().getExtras();
    if (localBundle != null)
    {
        String str1 = localBundle.getString("android.intent.extra.SUBJECT");
        String str2 = localBundle.getString("android.intent.extra.TEXT");
        if (str1 != null) {
            e.setText(str1);
        }
        if (str2 != null) {
            f.setText(str2);
        }
        if ((str1 != null) || (str2 != null)) {
            break label127;
        }
    }
    label127:
    for (Long localLong = Long.valueOf(localBundle.getLong("_id")); localLong = null)
    {
        d = localLong;
        if (d == null) {
            break;
        }
        a = 1;
    }
}

Java Tab Width: 8 Ln 149, Col 44 INS
```

Improper Platform Usage



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~  
Error: Argument expected after "android.intent.extra.TEXT"  
nt.extra.SUBJECT dumbass -e android.intent.extra.TEXT dumbass <  
Starting: Intent { cmp=com.xllusion.quicknote/.EditNote (has extras) }  
shell@E5803:/ $
```

Package name and the activity

```
~# adb shell am start -n com.xllusion.quicknote/.EditNote -e  
android.intent.extra.SUBJECT dumbass -e android.intent.extra.TEXT dumbass
```

Put the first string

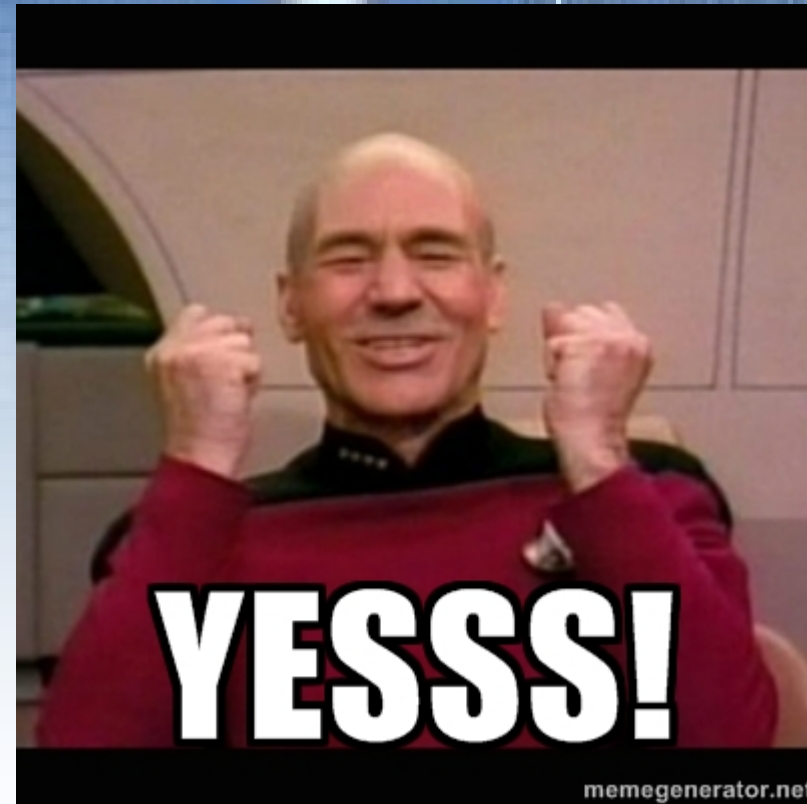
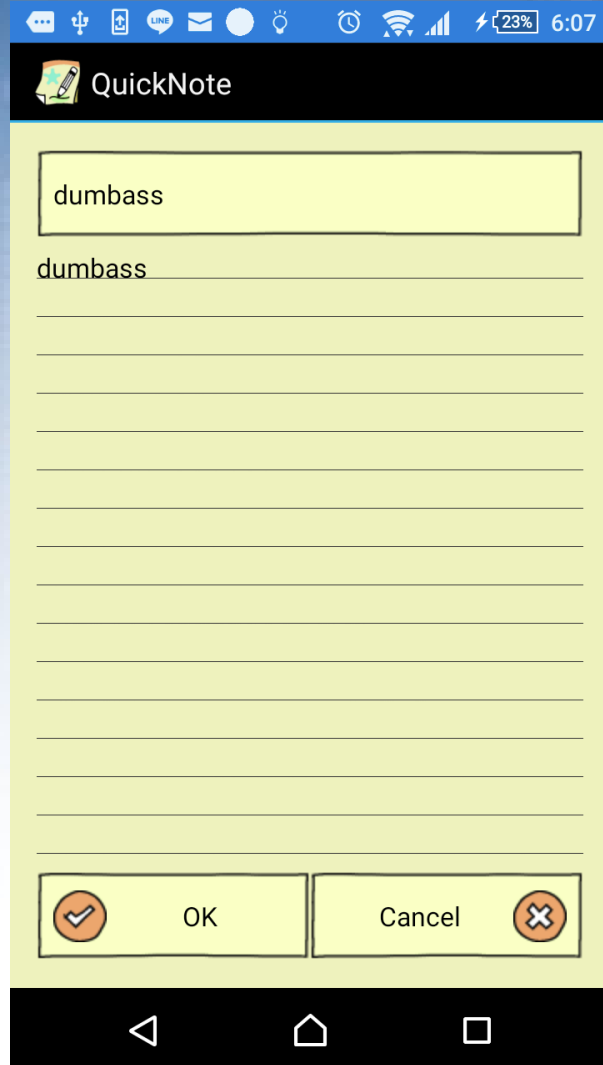
Put the second string

Improper Platform Usage



OWASP

Open Web Application
Project



OWASP Mobile top 10 Vulnerability



Top 10 Mobile Risks - Final List 2016

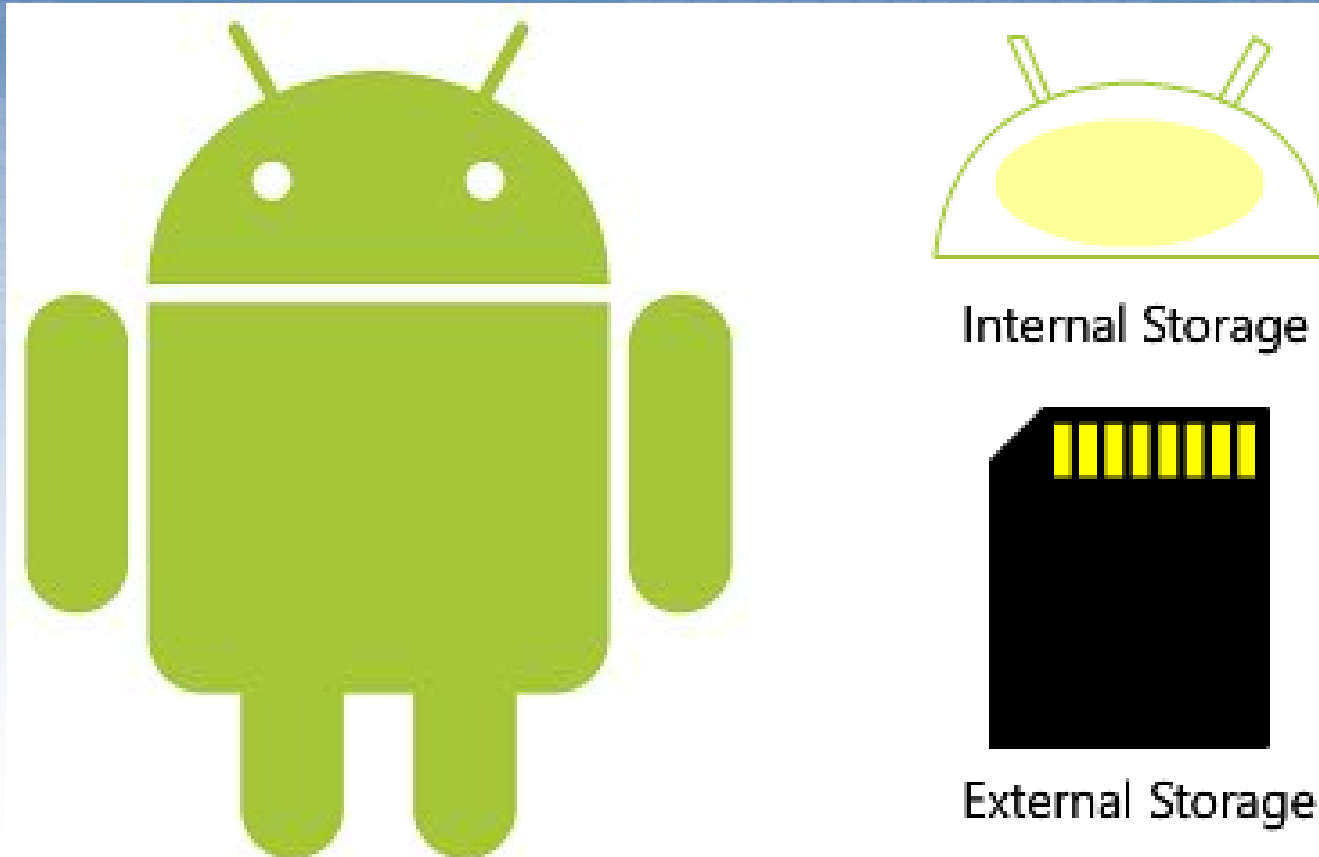
- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

Insecure Data Storage



OWASP

Open Web Application
Security Project



Internal Storage

External Storage

Target:



OWASP

Open Web Application
Security Project



Basketball Shoot APK



★★★★☆ 4.4/5 (3 Discussions)

Author:

[MiniCard](#)

Latest Version:

1.19.34

Publish Date:

2017-09-15

Download APK (8.5 MB)



Insecure Data Storage



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
root@android:/data/data/com.game.basketballshoot # ls
cache
code_cache
databases
files
lib
no_backup
shared_prefs
root@android:/data/data/com.game.basketballshoot #
```

Insecure Data Storage



OWASP

Open Web Application

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Documents/android_pentest_tools/apk
root@android:/data/data/com.game.basketballshoot/shared_prefs # ls
FBAdPrefs.xml
FLURRY_SHARED_PREFERENCES.xml
SDKIDFA.xml
admob.xml
appsflyer-data.xml
com.facebook.ads.FEATURE_CONFIG.xml
com.facebook.internal.preferences.APP_SETTINGS.xml
com.google.android.gms.appid.xml
com.google.android.gms.measurement.prefs.xml
config.xml
game_cfg.xml
multidex.version.xml
sql.xml
root@android:/data/data/com.game.basketballshoot/shared_prefs #
```

Insecure Data Storage



```
Open [icon] Save Application
<int name="pr21" value="0" />
<int name="mi15" value="0" />
<int name="local4" value="0" />
<int name="pr20" value="0" />
<int name="mi16" value="0" />
<int name="local9" value="0" />
<int name="pr27" value="0" />
<int name="pr26" value="0" />
<int name="local7" value="0" />
<int name="pr25" value="0" />
<int name="pr0" value="2" />
<int name="mi19" value="0" />
<int name="local8" value="0" />
<int name="pr24" value="0" />
<int name="pr1" value="0" />
<int name="pr29" value="0" />
<int name="pr28" value="0" />
<int name="local1" value="0" />
<int name="local2" value="0" />
<int name="local0" value="15051" />
<int name="mi12" value="0" />
<int name="mi11" value="0" />
<int name="mi14" value="0" />
<int name="mi13" value="0" />
<int name="ver" value="2" />
<int name="mi10" value="0" />
<int name="pr14" value="0" />
<int name="pr13" value="0" />
<int name="pr16" value="0" />
<int name="pr15" value="0" />
<int name="pr10" value="0" />
<int name="pr12" value="0" />
<int name="pr11" value="0" />
<int name="ghtip" value="0" />
<int name="pr18" value="0" />
<int name="pr17" value="0" />
<int name="pr19" value="0" />
<int name="lbc" value="0" />
<int name="cbc" value="4" />
</map>
```

XML Tab Width: 8 Ln 58, Col 28 INS

Insecure Data Storage



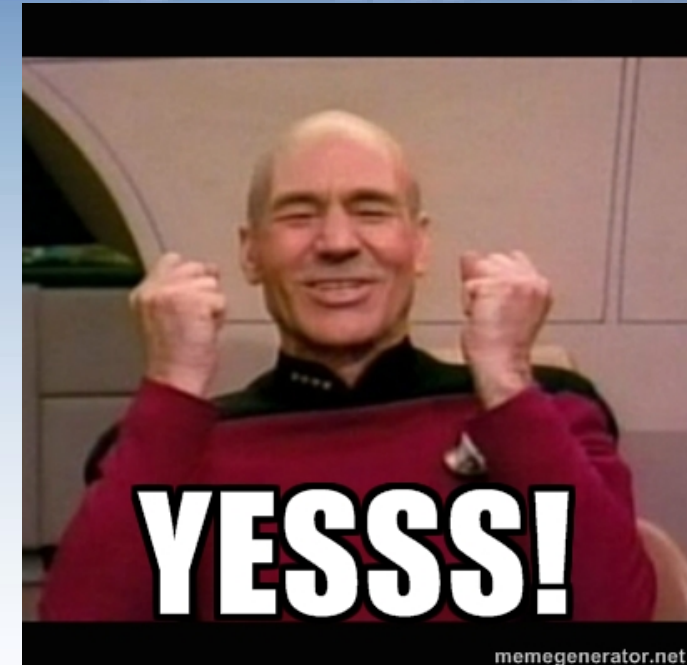
```
Open [icon] Save Application
<int name="pr21" value="0" />
<int name="mi15" value="0" />
<int name="local4" value="0" />
<int name="pr20" value="0" />
<int name="mi16" value="0" />
<int name="local9" value="0" />
<int name="pr27" value="0" />
<int name="pr26" value="0" />
<int name="local7" value="0" />
<int name="pr25" value="0" />
<int name="pr0" value="2" />
<int name="mi19" value="0" />
<int name="local8" value="0" />
<int name="pr24" value="0" />
<int name="pr1" value="0" />
<int name="pr29" value="0" />
<int name="pr28" value="0" />
<int name="local1" value="500" />
<int name="local2" value="1251" />
<int name="local0" value="15051" />
<int name="mi12" value="0" />
<int name="mi11" value="0" />
<int name="mi14" value="0" />
<int name="mi13" value="0" />
<int name="ver" value="2" />
<int name="mi10" value="0" />
<int name="pr14" value="0" />
<int name="pr13" value="0" />
<int name="pr16" value="0" />
<int name="pr15" value="0" />
<int name="pr10" value="0" />
<int name="pr12" value="0" />
<int name="pr11" value="0" />
<int name="ghtip" value="0" />
<int name="pr18" value="0" />
<int name="pr17" value="0" />
<int name="pr19" value="0" />
<int name="lbc" value="0" />
<int name="cbc" value="4" />
</map>
Saving file '/home/williams/Documents/android_pentest_tools/apk_folder/config.xml'...
XML Tab Width: 8 Ln 57, Col 30 INS
```

Insecure Data Storage



OWASP

Open Web Application
Security Project



OWASP Mobile top 10 Vulnerability



Top 10 Mobile Risks - Final List 2016

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

Insecure Communication



OWASP
Open Web Application
Security Project



What do you need ?

Insecure Communication



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
```

```
root@android:/data/system # ls
batterystats.bin
busybox-armv6l
cache
called_pre_boots.dat
device_policies.xml
dropbox
entropy.dat
gesture.key
inputmethod
locksettings.db
locksettings.db-shm
locksettings.db-wal
netpolicy.xml
netstats
packages.list
packages.xml
profiles.xml
registered_services
shared_prefs
sync
tcpdump
throttle
uiderrors.txt
usagestats
users
root@android:/data/system #
```

Insecure Communication



OWASP

Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
root@android:/data/system # ./busybox-armv6l
BusyBox v1.16.0 (2010-02-06 04:31:26 CST) multi-call binary.
Copyright (C) 1998-2009 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
       or: function [arguments]...

       BusyBox is a multi-call binary that combines many common Unix
       utilities into a single executable.  Most people will create a
       link to busybox for each function they wish to use and BusyBox
       will act like whatever it was invoked as.

Currently defined functions:
[, [[, acpid, addgroup, adduser, adjtimex, arp, arping, ash, awk,
basename, bbconfig, beep, blkid, brctl, bunzip2, bzip2, cal,
cat, catv, chat, chatr, chgrp, chmod, chown, chpasswd, chpst, chroot,
chrt, chvt, cksum, clear, cmp, comm, cp, cpio, crond, crontab, cryptpw,
cttyhack, cut, date, dc, dd, dealloct, delgroup, deluser, depmod,
devmem, df, dhcprelay, diff, dirname, dmesg, dnsd, dnsdomainname,
dos2unix, dpkg, dpkg-deb, du, dumpkmap, dumpleases, echo, ed, egrep,
eject, env, envdir, envuidgid, ether-wake, expand, expr, fakeidentd,
false, fbset, fbsplash, fdflush, fdformat, fdisk, fgrep, find, findfs,
flashcp, fold, free, freeramdisk, fsck, fsck.minix, fsync, ftpd,
ftpget, ftpput, fuser, getopt, getty, grep, gunzip, gzip, halt, hd,
hdparm, head, hexdump, hostid, hostname, httpd, hush, hwclock, id,
```

Insecure Communication



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
root@android:/data/system # ./tcpdump -h
tcpdump version 4.9.2
libpcap version 1.8.1
Usage: tcpdump [-aAbdDefhHIJKLLnNOpqStuUvX#] [-B size] [-c count]
        [-C file_size] [-E algo:secret] [-F file] [-G seconds]
        [-i interface] [-j tstamptype] [-M secret] [--number]
        [-Q in|out|inout]
        [-r file] [-s snaplen] [--time-stamp-precision precision]
        [--immediate-mode] [-T type] [--version] [-V file]
        [-w file] [-W filecount] [-y datalinktype] [-z postrotate
-command ]
        [-Z user] [ expression ]
root@android:/data/system #
```

Insecure Communication



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
root@android:/data/system # netcfg
lo          UP          127.0.0.1/8  0x00000049  00:00:00:00:00:00
dummy0     DOWN       0.0.0.0/0   0x00000082  16:68:63:8c:e3:e0
usb0       DOWN       0.0.0.0/0   0x00001002  32:18:5c:22:d6:41
sit0       DOWN       0.0.0.0/0   0x00000080  00:00:00:00:00:00
ip6tnl0    DOWN       0.0.0.0/0   0x00000080  00:00:00:00:00:00
wlan0      UP         0.0.0.0/0   0x00001003  d0:df:c7:3e:9b:84
root@android:/data/system #
```

Insecure Communication



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
127|root@android:/data/system # netcfg
lo          UP                127.0.0.1/8      0x00000049 00:00:00:00:00:00
dummy0     DOWN              0.0.0.0/0       0x00000082 16:68:63:8c:e3:e0
usb0       DOWN              0.0.0.0/0       0x00001002 32:18:5c:22:d6:41
sit0       DOWN              0.0.0.0/0       0x00000080 00:00:00:00:00:00
ip6tnl0    DOWN              0.0.0.0/0       0x00000080 00:00:00:00:00:00
wlan0      UP                192.168.43.79/24 0x00001043 d0:df:c7:3e:9b:84
root@android:/data/system # ./tcpdump -i wlan0 -v -w sniff.pcap
```

Insecure Communication



OWASP
Open Web Application
Security Project

```
williams@williams-HP-Pavilion-14-Notebook-PC: ~/Desktop/coursenet
127|root@android:/data/system # netcfg
lo          UP                127.0.0.1/8      0x00000049 00:00:00:00:00:00
dummy0     DOWN              0.0.0.0/0       0x00000082 16:68:63:8c:e3:e0
usb0       DOWN              0.0.0.0/0       0x00001002 32:18:5c:22:d6:41
sit0       DOWN              0.0.0.0/0       0x00000080 00:00:00:00:00:00
ip6tnl0    DOWN              0.0.0.0/0       0x00000080 00:00:00:00:00:00
wlan0      UP                192.168.43.79/24 0x00001043 d0:df:c7:3e:9b:84
root@android:/data/system # ./tcpdump -i wlan0 -v -w sniff.pcap
```


Insecure Communication



OWASP
Open Web Application
Security Project

http

Time	Source	Destination	src-p	Protoc	Leng	Info
185	52.216.225.227	192.168.43.79	80	HTTP	1208	HTTP/1.1 200 OK (application/javascript)
196	216.58.196.3	192.168.43.79	80	HTTP	468	HTTP/1.1 200 OK (font/ttf)
196	192.168.43.79	104.16.91.120	432...	HTTP	405	GET /favicon.ico HTTP/1.1
203	104.16.91.120	192.168.43.79	80	HTTP	966	HTTP/1.1 200 OK
226	192.168.43.79	104.16.87.120	448...	HTTP	320	GET /s/login/relogin;jsessionid=485A8CB4103C0606F9E69C73E8628658?error=1 HTTP/1.1
227	104.16.87.120	192.168.43.79	80	HTTP	74	HTTP/1.1 200 OK (text/html)
228	192.168.43.79	104.16.87.120	448...	HTTP	221	GET /favicon.ico HTTP/1.1
228	192.168.43.79	74.125.24.154	368...	HTTP	1130	GET /__utm.gif?utmwv=5.7.1dc&utms=2&utm=751537730&utmhn=members.webs.com&utmcs=UTF-8&utmsr=480x800&utm...
228	192.168.43.79	118.214.78.107	473...	HTTP	816	GET /tp?act=1&cid=2932in917575&tz=-7&ref=&page=http%3A%2F%2Fmembers.webs.com%2F%2Flogin%2Flogin%3Bjs...
228	74.125.24.154	192.168.43.79	80	HTTP	476	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
228	192.168.43.79	161.202.1.17	534...	HTTP	1295	GET /track/?data=eyJldmVudCI6ICJtcF9wYldlX3ZpZXRlcXJwcm9wZXJ0aWVzIjogeyIkb3MiOiAiQW5kcm9pZCI6IiRiRm93c2...
228	161.202.1.17	192.168.43.79	80	HTTP	528	HTTP/1.1 200 OK (application/json)
228	104.16.87.120	192.168.43.79	80	HTTP	346	HTTP/1.1 200 OK
228	118.214.78.107	192.168.43.79	80	HTTP	477	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)

Cookie pair: __utmb=1.1.10.1522312045
Cookie pair: __utmc=1
Cookie pair: __utmz=1.1522312045.1.1.utmsr=(direct)|utmccn=(direct)|utmcmd=(none)
Cookie pair [truncated]: mp_58fa82747b4c3f4992b74583e70b8940_mixpanel=%7B%22distinct_id%22%3A%20%2216270de638483-01ba8b198-753f5e64-5dc00-16270de6386ad%22%2C%22%24initial_...
Cookie pair: _msuuid_2932in917575=B1C8A766-5F87-410A-8D60-9B1BA5EA0ABA
Cookie pair: optimizelyEndUserId=oeu1522312046152r0.174021604238078
Cookie pair: optimizelySegments=%7B%22696661447%22%3A%22true%22%2C%22704900824%22%3A%22true%22%2C%221022966592%22%3A%22none%22%2C%221022996374%22%3A%22direct%22%2C%2210265...
Cookie pair: optimizelyBuckets=%7B%7D
Cookie pair: JSESSIONID=485A8CB4103C0606F9E69C73E8628658
Cookie pair: AWSSELB=6919354D10BA5723AEB236FF34B7EF0F1509700814474A4A141E0172C8FD4ABA06C04DA450EFBBCB556ECFEB21762E283C125F19EF2891A187CE7328EA86572588541ECA34A66DF322E1DA5...

Full request URI: <http://members.webs.com/favicon.ico>
[HTTP request 2/2]
[Prev request in frame: 2153]

```
0000 47 45 54 20 2f 66 61 76 69 63 6f 6e 2e 69 63 6f  GET /fav icon.ico
0010 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a  HTTP/1. 1..Host:
0020 20 6d 65 6d 62 65 72 73 2e 77 65 62 73 2e 63 6f  members .webs.co
0030 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b  m..Conne ction: k
0040 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72  eep-aliv e..Refer
0050 65 72 3a 20 68 74 74 70 3a 2f 2f 6d 65 6d 62 65  er: http ://membe
0060 72 73 2e 77 65 62 73 2e 63 6f 6d 2f 73 2f 6c 6f  rs.webs. com/s/lo
```

Frame (221 bytes) | Reassembled TCP (1567 bytes)

This packet will be responded in the packet with this number (http.response_in) | Packets: 2265 · Displayed: 70 (3.1%) · Load time: 0:0.39 | Profile: Default



OWASP

Open Web Application
Security Project

Thank You