ANDROID TAMER

WHAT IS ANDROID TAMER

Single Point of Reference / Resources for Android

Contains

1. Virtual machine for Android (Security) Professionals
2. Debian 8 Compatible Tools Repository
3. Custom Emulator for arm devices (Work In Progress)
4. f-droid repository of tools (Work in Progress)
5. Documentation (tools.androidtamer.com) (ever evolving)
6. KnowledgeBase (kb.androidtamer.com) (Work in Progress)

WHO USES ANDROID TAMER

1. Trainers
2. Security professionals
3. Developers
4. iOT Hackers

Friendly Plug

- Catch Sneha Rajguru using AndroidTamer at
  - BSidesLV (whole day 3 Aug 2016)
  - Defcon Workshop (5 Aug 2016 : 10 AM - 2 PM)
- Catch Anto Joseph using AndroidTamer with Droid-FF at
  - Arsenal Booth (4 Aug 2016 - 2 PM - 3:50 PM)
  - Defcon Workshop (6 Aug 2016 : 2 PM - 6 PM)

OPENSOURCE ALL THE WAY

1. Automated VM Building Process : Vagrant Ansible script (https://github.com/AndroidTamer/VagrantBuild)
2. Automated Debian Package Building Scripts (https://github.com/AndroidTamer/Packaging_Tools)
3. Documentation source markdown (https://github.com/AndroidTamer/Tools)
4. Open to all https://github.com/AndroidTamer
5. To be added
    1. APK repository
    2. apk building process
    3. emulator building process
    4. Live ISO Creation
    5. and more

VIRTUAL MACHINE

Swiss Army knife for Android Security Professionals.

Supports

- VirtualBox
- VMWare
- Vagrant / Ansible

WHY

Saves time while

- Finding and installing tools
- Configuring them
- Ensuring all other tools are still working
- Multiple language versions (java, python, perl, ruby more)
- Managing updates of each tool

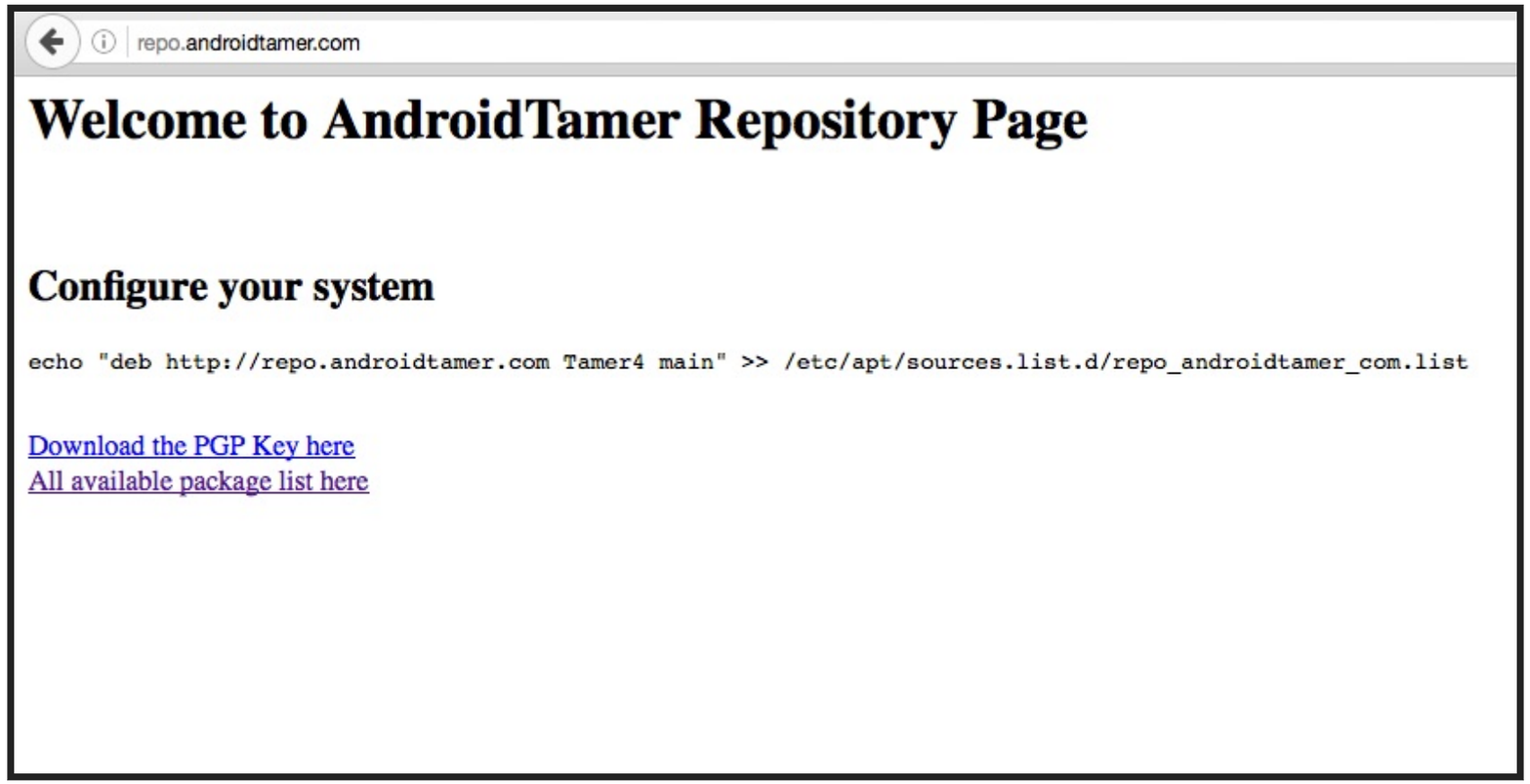
TOOLS INCLUDE

1. adb / fastboot / android-sdk
2. dex2jar / **enjarify**
3. apktool
4. jad / jd-gui / jadx / jadx-gui
5. drozer / **MobSF** / jaadas
6. DFF / ddrescueview
7. SQLiteManager / SQLiteMan
8. Burp Free / OWASP-ZAP
9. pidcat
10. **Droid-FF (Fuzzing Framework)**
11. dextra, simplify, imgtool
12. and more....

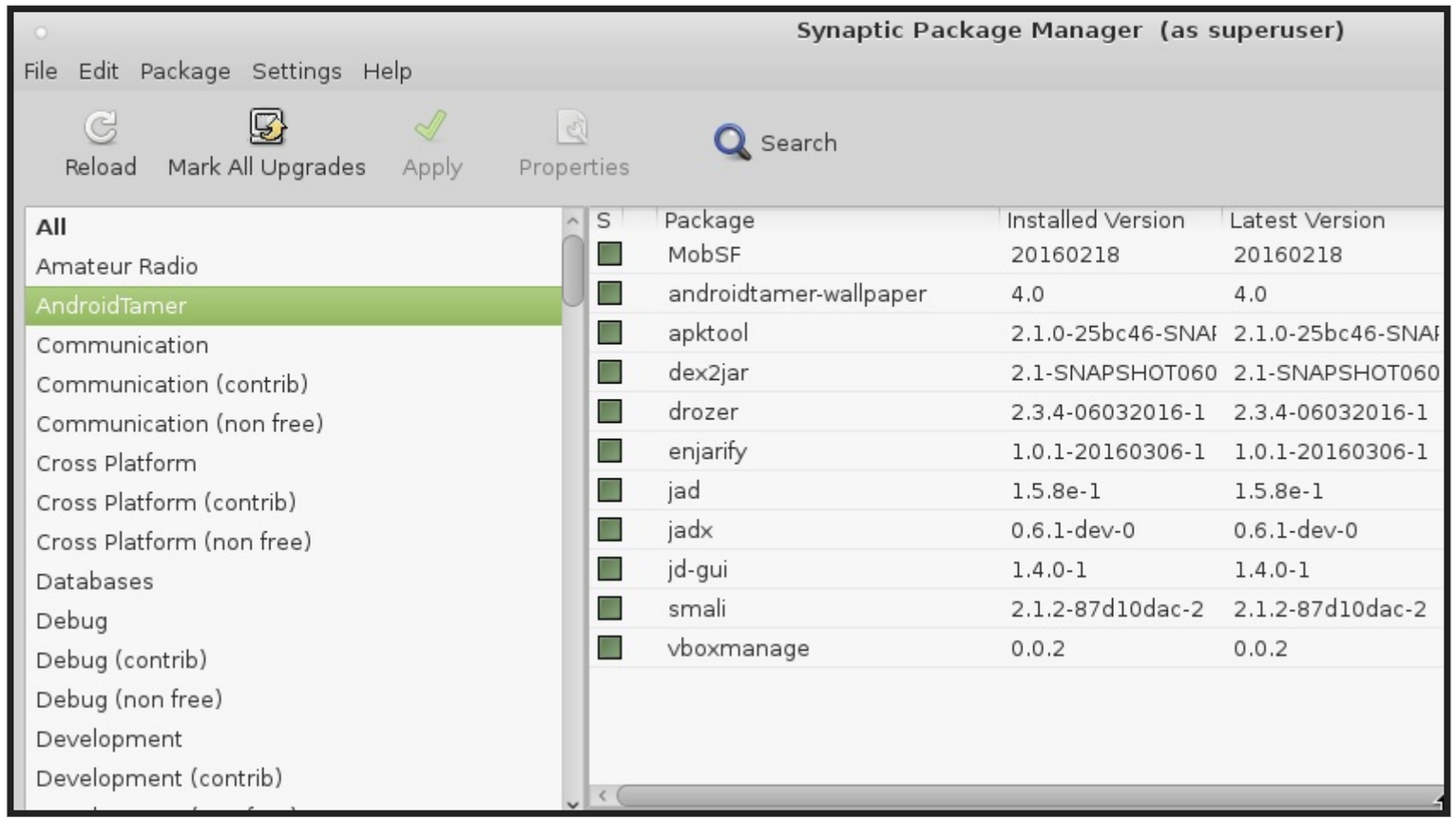
CUSTOM FEATURES

1. Easy Management of multiple devices
2. One liner commands (apk2java, drozer_start etc)
3. Scripts for automated analysis
4. Software update managed over apt-get repository (alpha phase) (http://repo.androidtamer.com/)
5. All Tools pre-configured in PATH (no need to switch directories)
6. ZSH with autosuggestion

TOOLS REPOSITORY

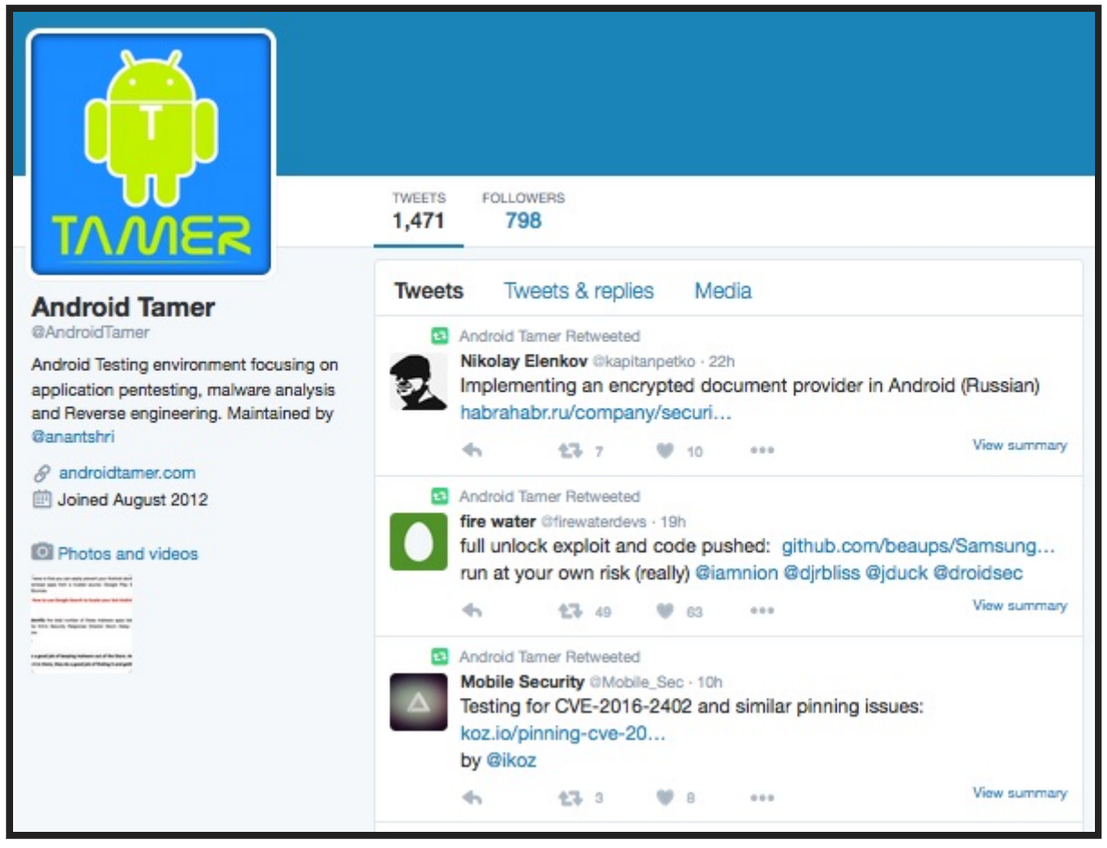


REPOSITORY IN USE



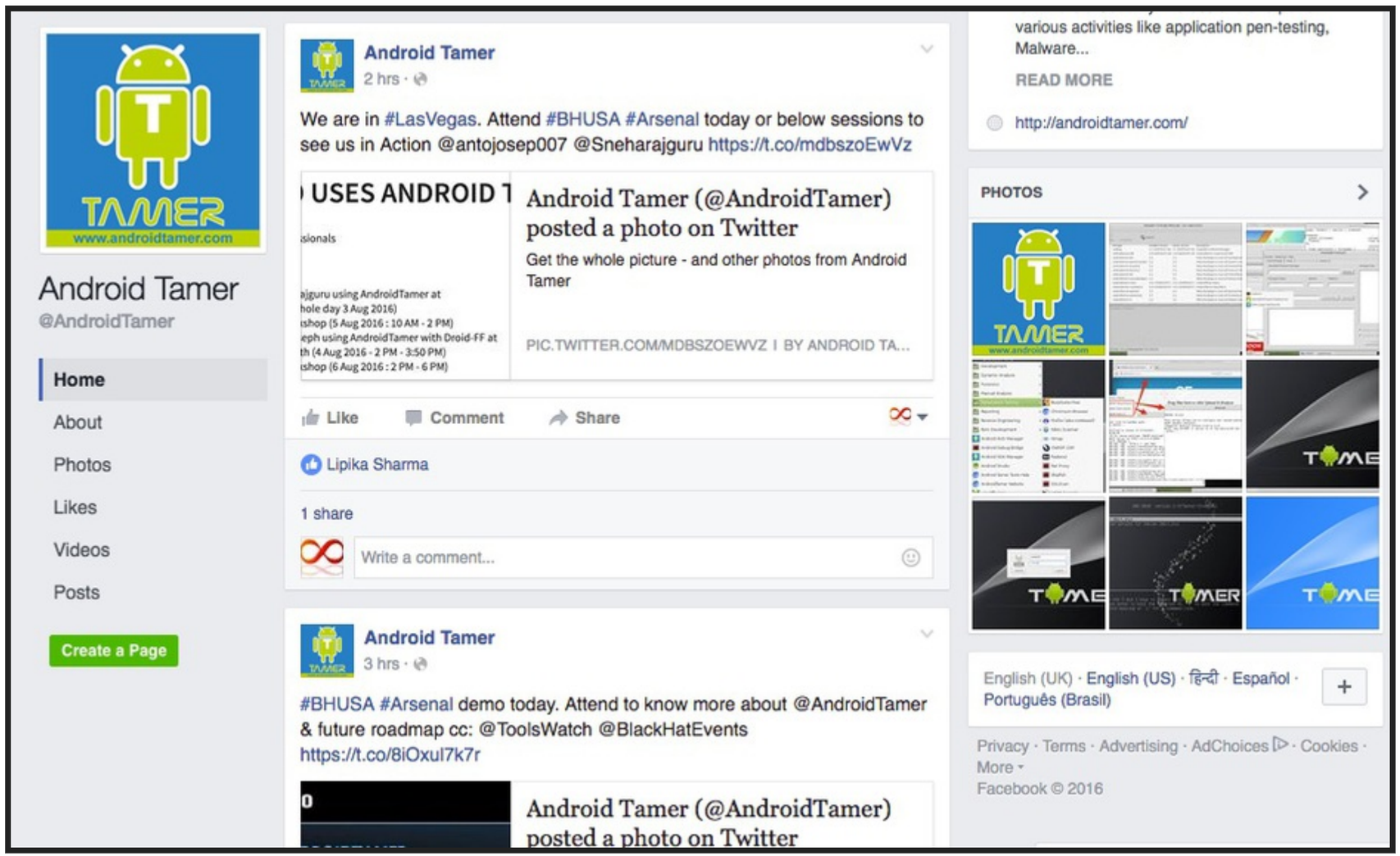
THAT'S NOT IT

@ TWITTER

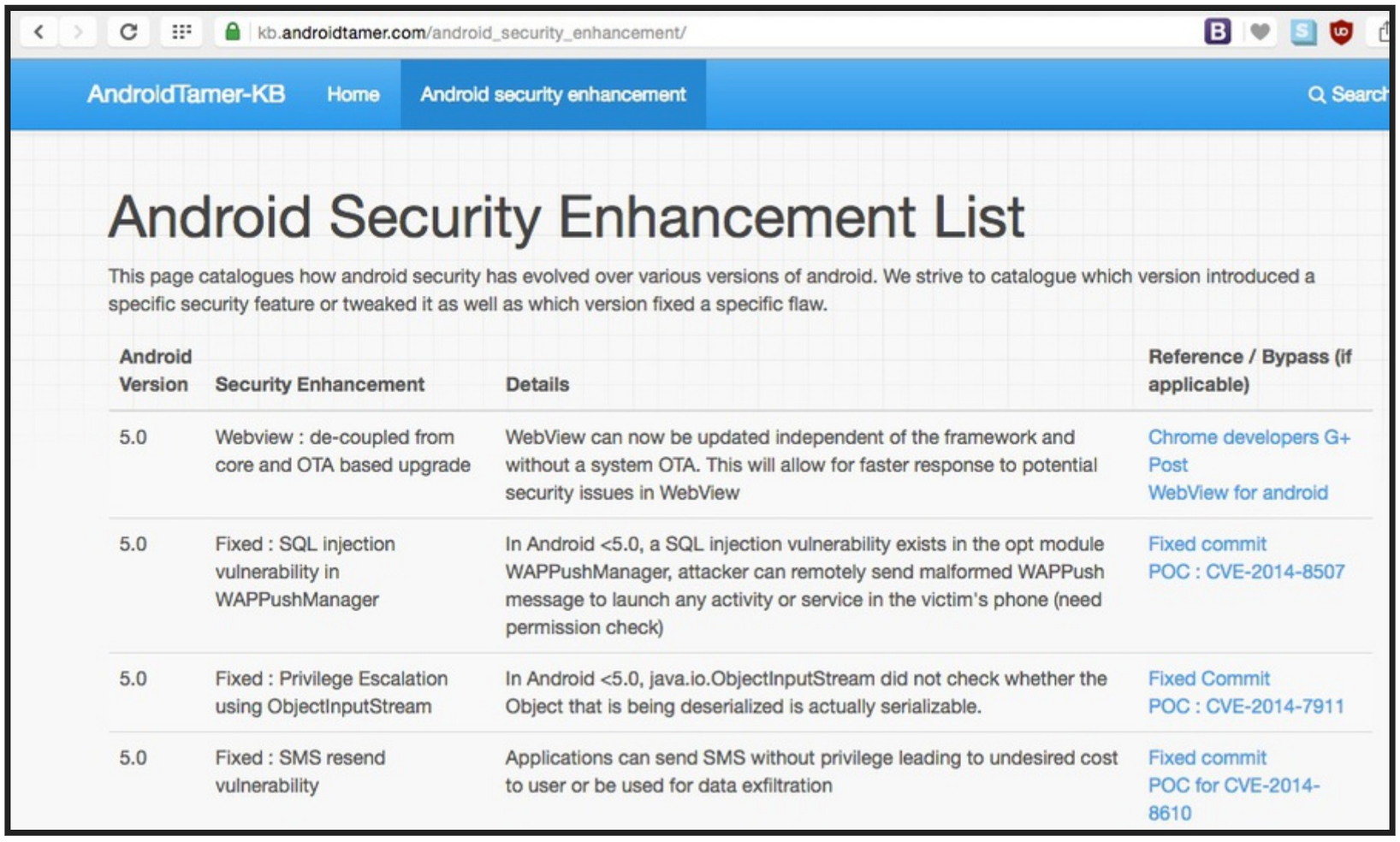


Follow Us @AndroidTamer to get Latest Android News

FB/ANDROIDTAMER

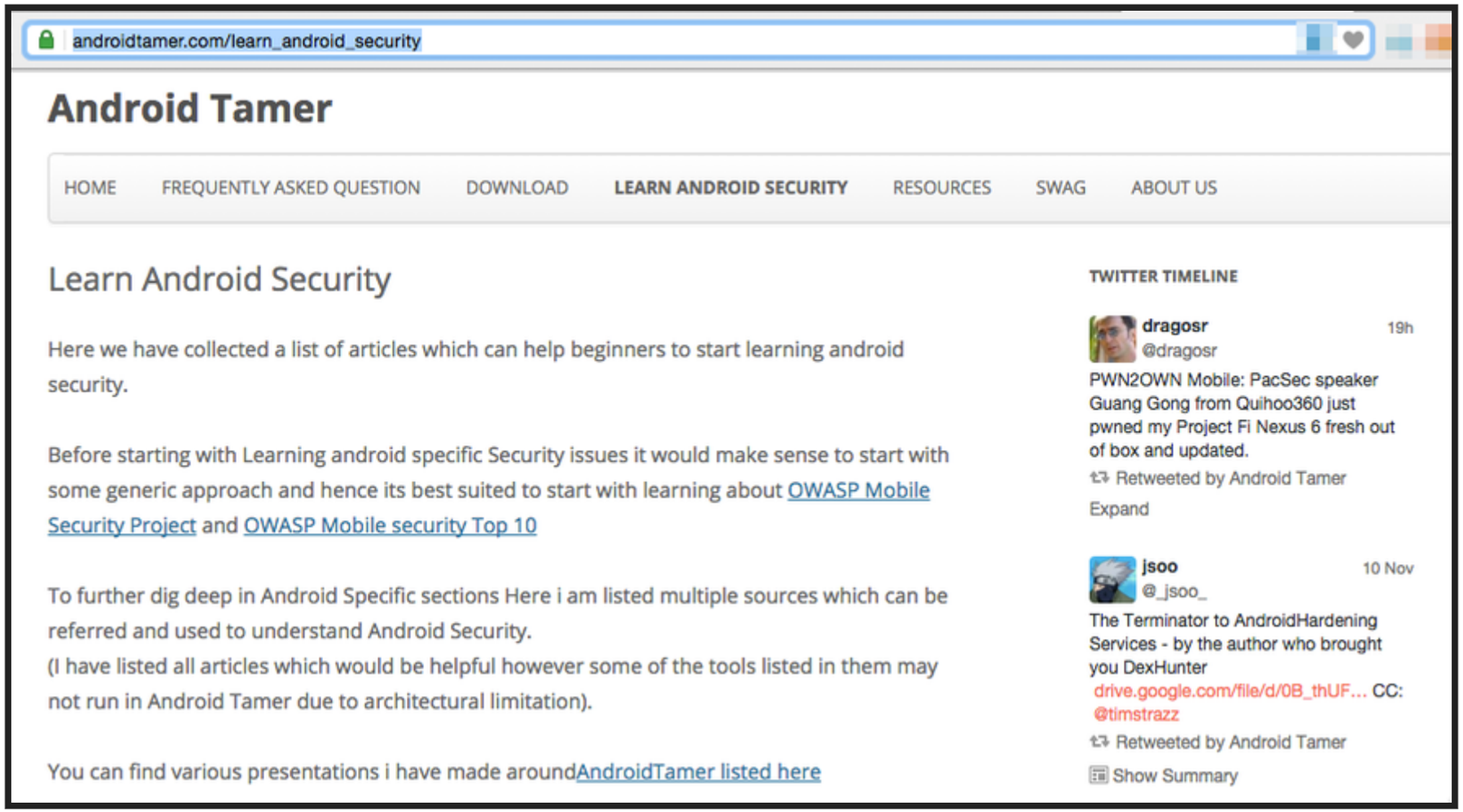


SECURITY ENHANCEMENTS



https://kb.androidtamer.com/android_security_enhancement/

LEARN ANDROID



https://androidtamer.com/learn_android_security

DEMO TIME

1. Application decompiling
2. Automated assessment (drozer_checks)
3. Multi devices management (adb list)
4. MobSF
5. Droid Fuzzing Framework
6. Build / Enhance your own Distro (Debian compatible Repository)

DEMO: APK2JAVA

```
android@tamer:~/Desktop/Arsenal/demo7$ apk2java CMFileManager.apk
APK TO JAVA source code extraction script
This is a script created by Anant Shrivastava
http://anantshri.info
This script will work on automating the work of extracting the source code
Starting APK Decompile
/usr/local/bin/apk2java CMFileManager.apk
CMFileManager.apk
APK to JAVA/SRC conversion Utility
CMFileManager
CMFileManager.apk
/home/android/Desktop/Arsenal/demo7/CMFileManager.apk
/home/android/Desktop/Arsenal/demo7
APK TOOLS extracting files
Doing APKtool now
apktool decode -f -o /home/android/Desktop/Arsenal/demo7/CMFileManager.apk
leManager.apk_src/
I: Using Apktool 2.1.0-25bc46-SNAPSHOT on CMFileManager.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/android/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
```

DEMO: DROZER_CHECK

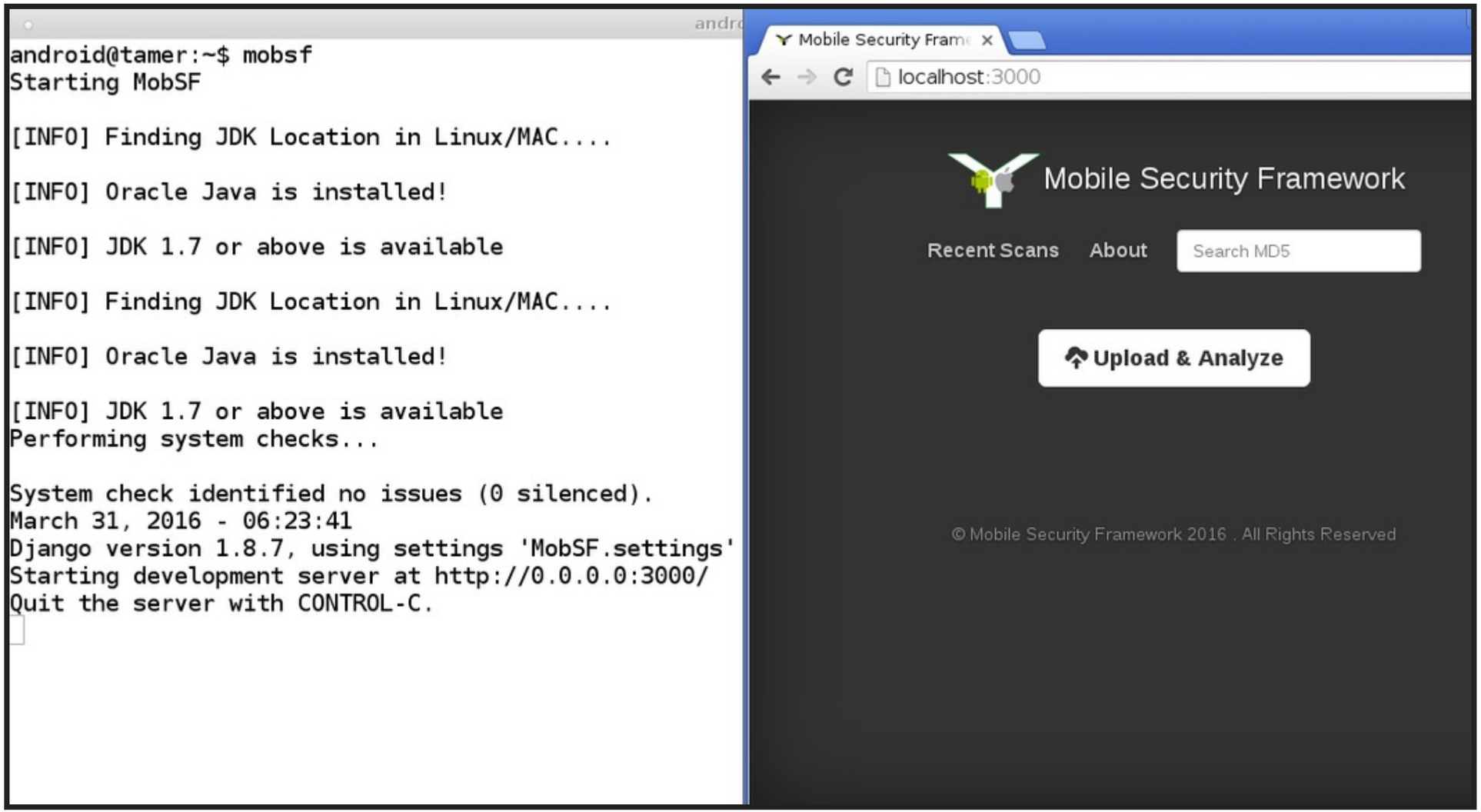
```
android@tamer:~$ drozer_check.sh jakhar.aseem.diva
Selecting dadcb63e00e6dbf9 (Genymotion Xtreme_Android_Exploitation_Lab 4.4.4)

Package: jakhar.aseem.diva
  Application Label: Diva
  Process Name: jakhar.aseem.diva
  Version: 1.0
  Data Directory: /data/data/jakhar.aseem.diva
  APK Path: /data/app/jakhar.aseem.diva-1.apk
  UID: 10090
  GID: [1028, 1015, 3003]
  Shared Libraries: null
  Shared User ID: null
  Uses Permissions:
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.READ_EXTERNAL_STORAGE
  - android.permission.INTERNET
  Defines Permissions:
  - None

Selecting dadcb63e00e6dbf9 (Genymotion Xtreme_Android_Exploitation_Lab 4.4.4)

<manifest versionCode="1"
          versionName="1.0"
          package="jakhar.aseem.diva"
```

DEMO: ADB LIST

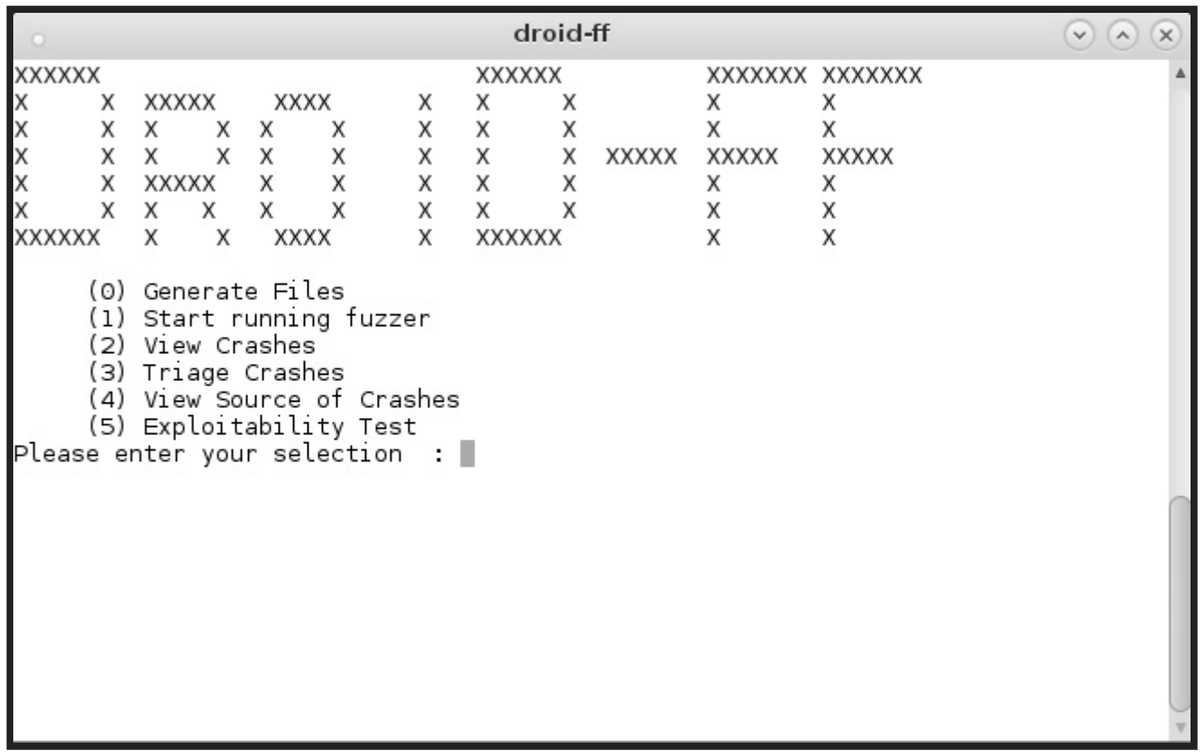
```
android@tamer:~$ adb list
ADB Status  : DeviceName  : Device SerialNo
device      : geny        : 192.168.57.101:5555
unknown     : nexus4      :
unknown     : spice       :
unknown     : nexus4      :
unknown     : nexus7      :
unknown     : oneplusx    :
unknown     : oneplus     :
unknown     : redmi       :
unknown     : geny2       : 192.168.56.102:5555
unknown     : geny3       : 192.168.56.103:5555
unknown     : grand2      :
unknown     : genynew     : 172.28.128.3:5555
android@tamer:~$
```

1. Add entries in ~/.adb_list
2. format of entries "ABC;SERIALNO"
3. echo "abc;1234567890" >> ~/.adb_list

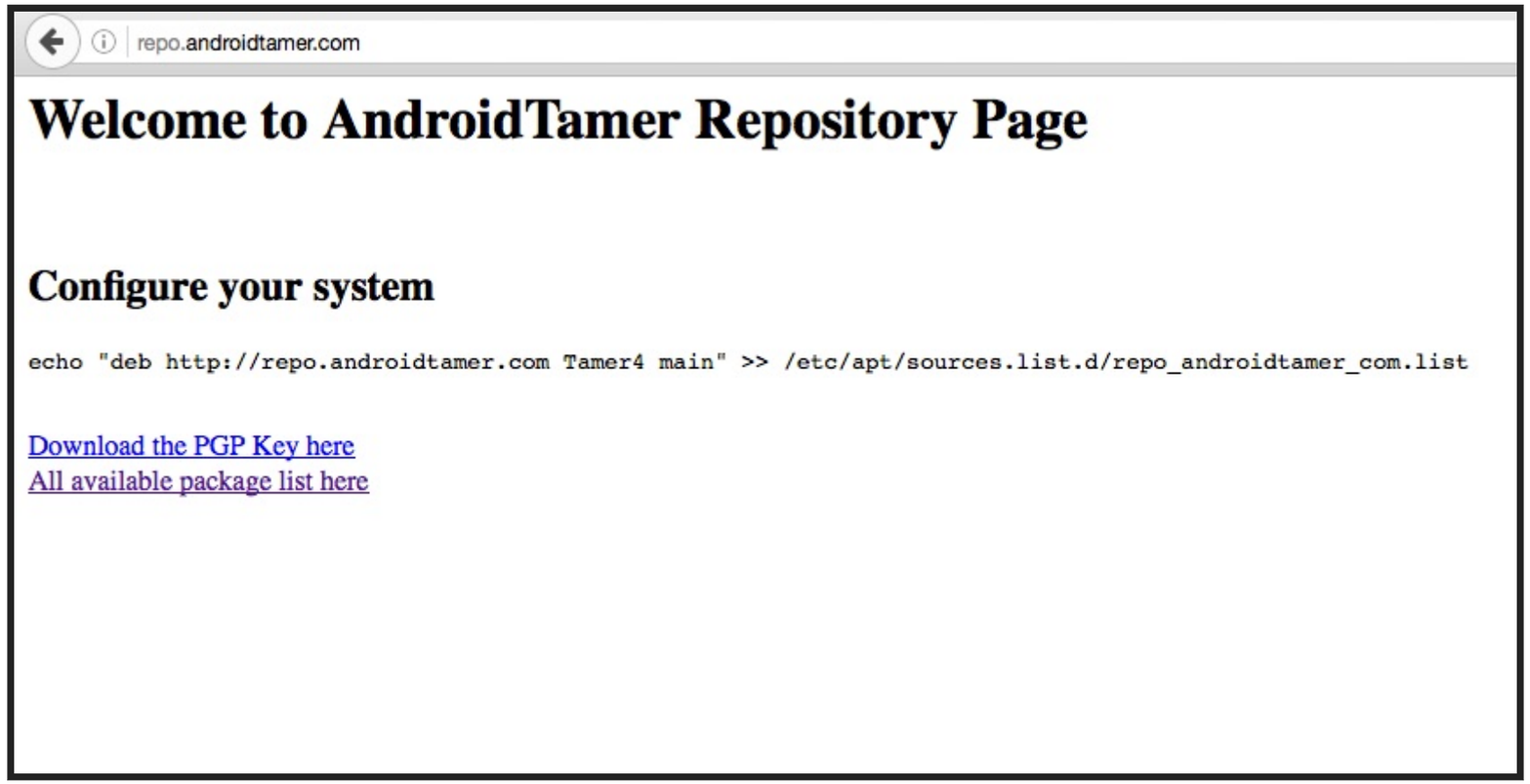
DEMO: MOBSF


android@tamer:~$ mobsf
Starting MobSF
[INFO] Finding JDK Location in Linux/MAC....
[INFO] Oracle Java is installed!
[INFO] JDK 1.7 or above is available
[INFO] Finding JDK Location in Linux/MAC....
[INFO] Oracle Java is installed!
[INFO] JDK 1.7 or above is available
Performing system checks...
System check identified no issues (0 silenced).
March 31, 2016 - 06:23:41
Django version 1.8.7, using settings 'MobSF.settings'
Starting development server at http://0.0.0.0:3000/
Quit the server with CONTROL-C.
Mobile Security Frame
localhost:3000
Mobile Security Framework
Recent Scans
About
Search MD5
Upload & Analyze
© Mobile Security Framework 2016 . All Rights Reserved

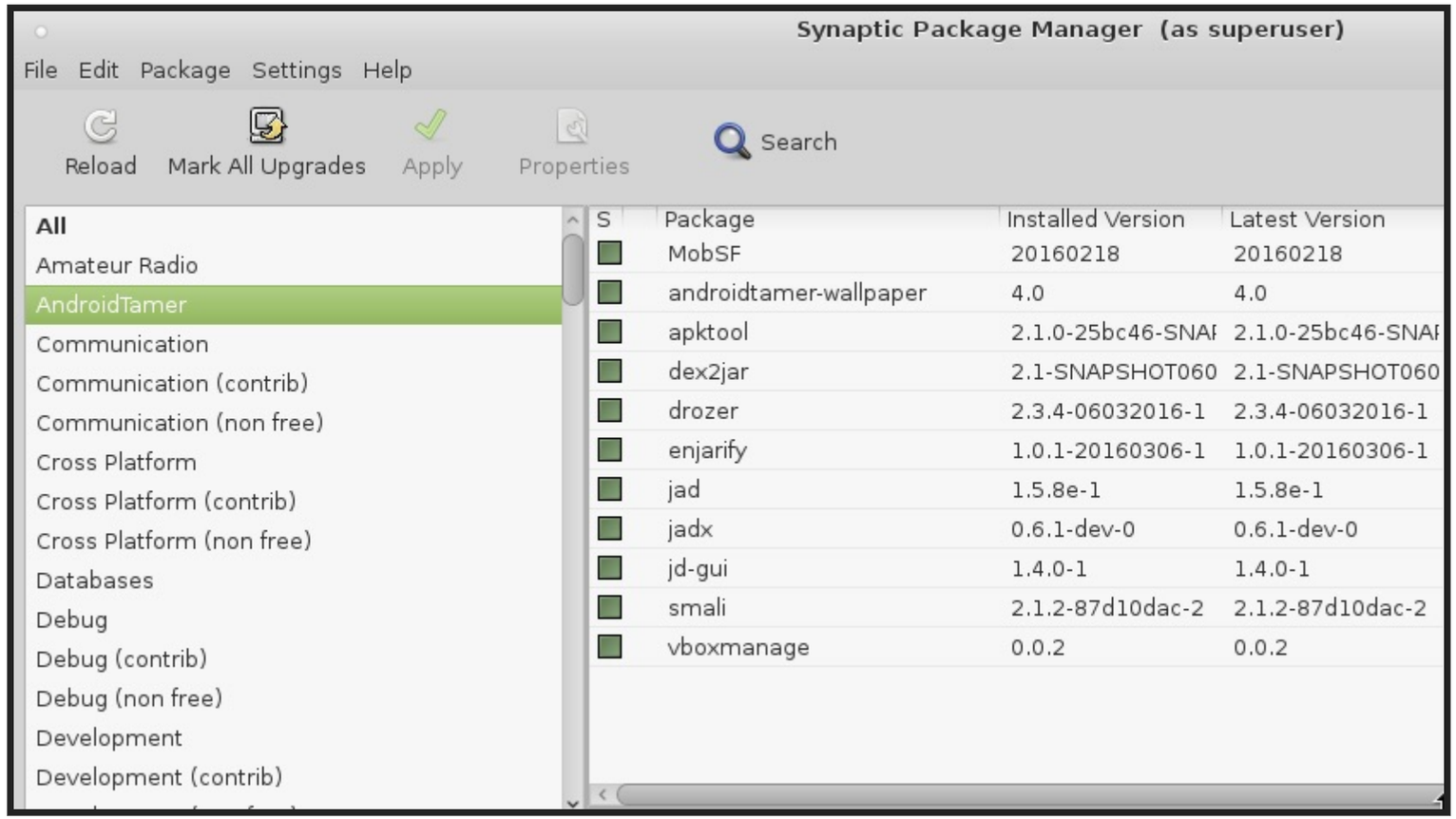
DEMO: DROID-FF



BUILD YOUR OWN



PACKAGE REPOSITORY



HOW TO CONTRIBUTE

1. Test the tools, suggest changes or improvements / enhancements
2. Use / Promote / Write about the tool
3. Add tools : https://github.com/AndroidTamer/Packaging_Tools/Build
4. Report / track / suggest / fix Issues
5. Test Repo on (https://repo.androidtamer.com) other distributions (Kali / Ubuntu / other pentest distro and more)

Report all issues(https://github.com/AndroidTamer/Tools_Repository/issues)

How to setup : (https://tools.androidtamer.com/General/repo_configure/)

THANKS

Follow @AndroidTamer for all Updates