

# ANDROID TAMER



<https://androidtamer.com>

# WHAT

Virtual machine 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
- Managing updates of each tool

# TOOLS INCLUDE

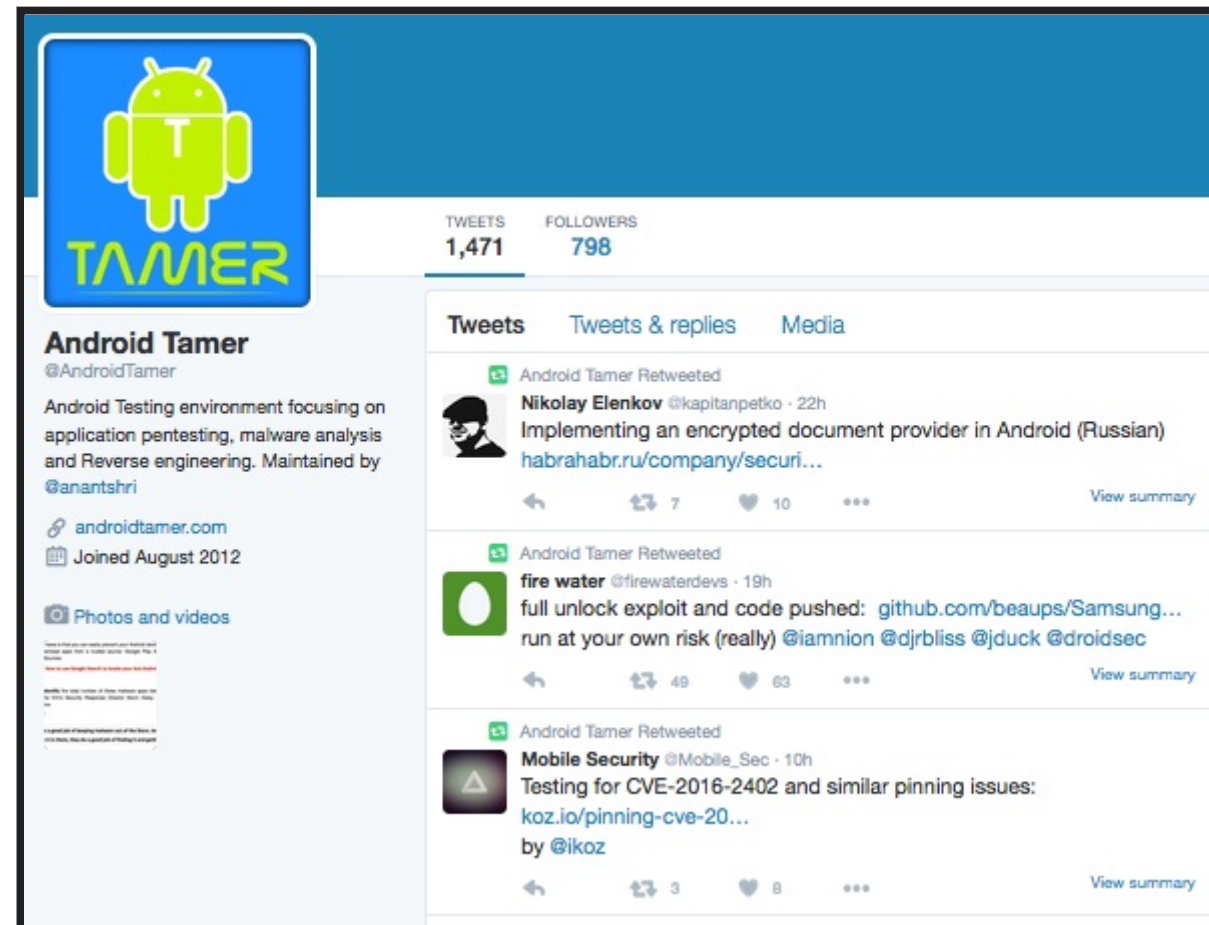
1. adb / fastboot / android-sdk
2. dex2jar / **enjarify**
3. apktool
4. jad / jd-gui / jadx / jadx-gui
5. drozer
6. DFF / ddrescueview
7. SQLiteManager / SQLiteMan
8. Burp Free / OWASP-ZAP
9. pidcat
10. MobSF (in-progress)
11. Cukoo-droid (in-progress)
12. and more....

# 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)

**THAT'S NOT IT**

# @ TWITTER



Follow Us [@AndroidTamer](https://twitter.com/AndroidTamer) to get Latest Android News

# FB/ANDROIDTAMER



## Android Tamer

Software

Use App Liked Message

Timeline About Photos Likes Videos

Search for posts on this Page

730 people like this  
Ashish Shrivastava and 248 other friends

Invite friends to like this Page

**ABOUT**

Android Tamer is a virtual Machine environment for Android Security Professionals to perform various activities like application pen-testing, Malware...

<http://androidtamer.com/>

**PHOTOS**

**Android Tamer**  
4 hrs ·

Retweeted Nikolay Elenkov (@kapitanpetko):  
Implementing an encrypted document provider in Android (Russian)  
<https://t.co/qFFhPZuSw9>



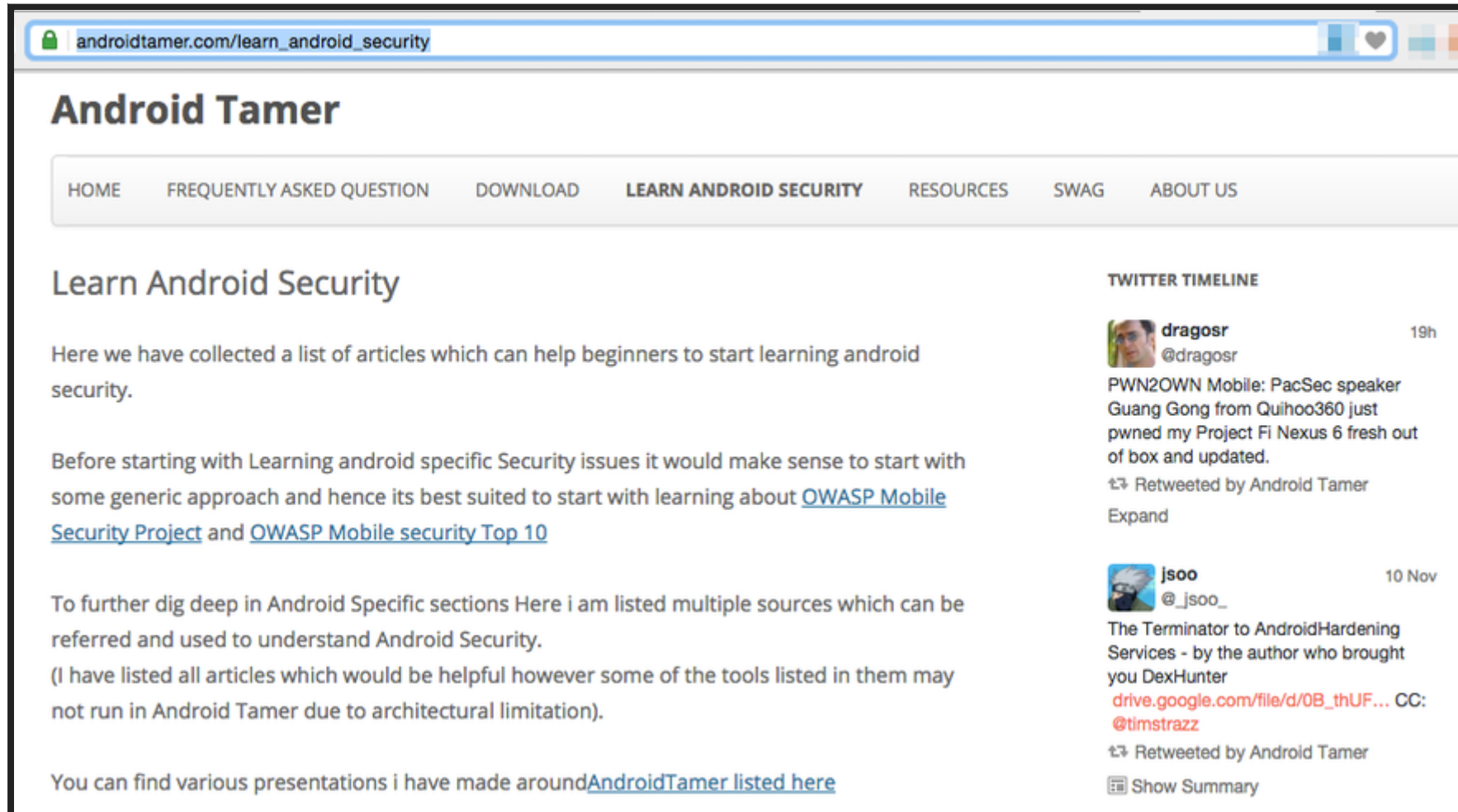
Сказ о том, как ГОСТ-шифрование диска в Android реализовывали



# SECURITY ENHANCEMENTS

ANDROID VERSION	SECURITY ENHANCEMENT	DETAILS	REFERENCE / BYPASS (IF APPLICABLE)
5.0	Webview : de-coupled from core and OTA based upgrade	WebView can now be updated independent of the framework and without a system OTA. This will allow for faster response to potential security issues in WebView	<a href="#">Chrome developers G+ Post</a> <a href="#">WebView for android</a>
5.0	Fixed : SQL injection vulnerability in WAPPushManager	In Android <5.0, a SQL injection vulnerability exists in the opt module WAPPushManager, attacker can remotely send malformed WAPPush message to launch any activity or service in the victim's phone (need permission check)	<a href="#">Fixed commit</a> <a href="#">POC : CVE-2014-8507</a>
5.0	Fixed : Privilege Escalation using ObjectInputStream	In Android <5.0, java.io.ObjectInputStream did not check whether the Object that is being deserialized is actually serializable.	<a href="#">Fixed Commit</a> <a href="#">POC : CVE-2014-7911</a>
5.0	Fixed : SMS resend vulnerability	Applications can send SMS without privilege leading to undesired cost to user or be used for data exfiltration	<a href="#">Fixed commit</a> <a href="#">POC for CVE-2014-8610</a>
5.0	FORTIFY_SOURCE improvements	Protection against memory-corruption vulnerabilities involving stpcpy(), stpncpy(), read(), recvfrom(), FD_CLR(), FD_SET(), and FD_ISSET() libc functions	
5.0	non-PIE linker support removed	Enhancing Address Space Layout Randomization (ASLR) by requiring all dynamically linked executables to support PIE (Position-Independent Executables)	

# LEARN ANDROID



The screenshot shows a web browser window with the address bar displaying [androidtamer.com/learn\\_android\\_security](https://androidtamer.com/learn_android_security). The website header features the title "Android Tamer" and a navigation menu with links: HOME, FREQUENTLY ASKED QUESTION, DOWNLOAD, LEARN ANDROID SECURITY (which is highlighted), RESOURCES, SWAG, and ABOUT US.

## Learn Android Security

Here we have collected a list of articles which can help beginners to start learning android security.

Before starting with Learning android specific Security issues it would make sense to start with some generic approach and hence its best suited to start with learning about [OWASP Mobile Security Project](#) and [OWASP Mobile security Top 10](#)

To further dig deep in Android Specific sections Here i am listed multiple sources which can be referred and used to understand Android Security.  
(I have listed all articles which would be helpful however some of the tools listed in them may not run in Android Tamer due to architectural limitation).

You can find various presentations i have made around [AndroidTamer listed here](#)

### TWITTER TIMELINE

**dragosr** @dragosr 19h  
PWN2OWN Mobile: PacSec speaker Guang Gong from Quihoo360 just pwned my Project Fi Nexus 6 fresh out of box and updated.  
Retweeted by Android Tamer  
Expand

**js00** @\_js00\_ 10 Nov  
The Terminator to AndroidHardening Services - by the author who brought you DexHunter  
[drive.google.com/file/d/0B\\_thUF...](https://drive.google.com/file/d/0B_thUF...) CC: @timstrazz  
Retweeted by Android Tamer  
Show Summary

[https://androidtamer.com/learn\\_android\\_security](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. Build 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)

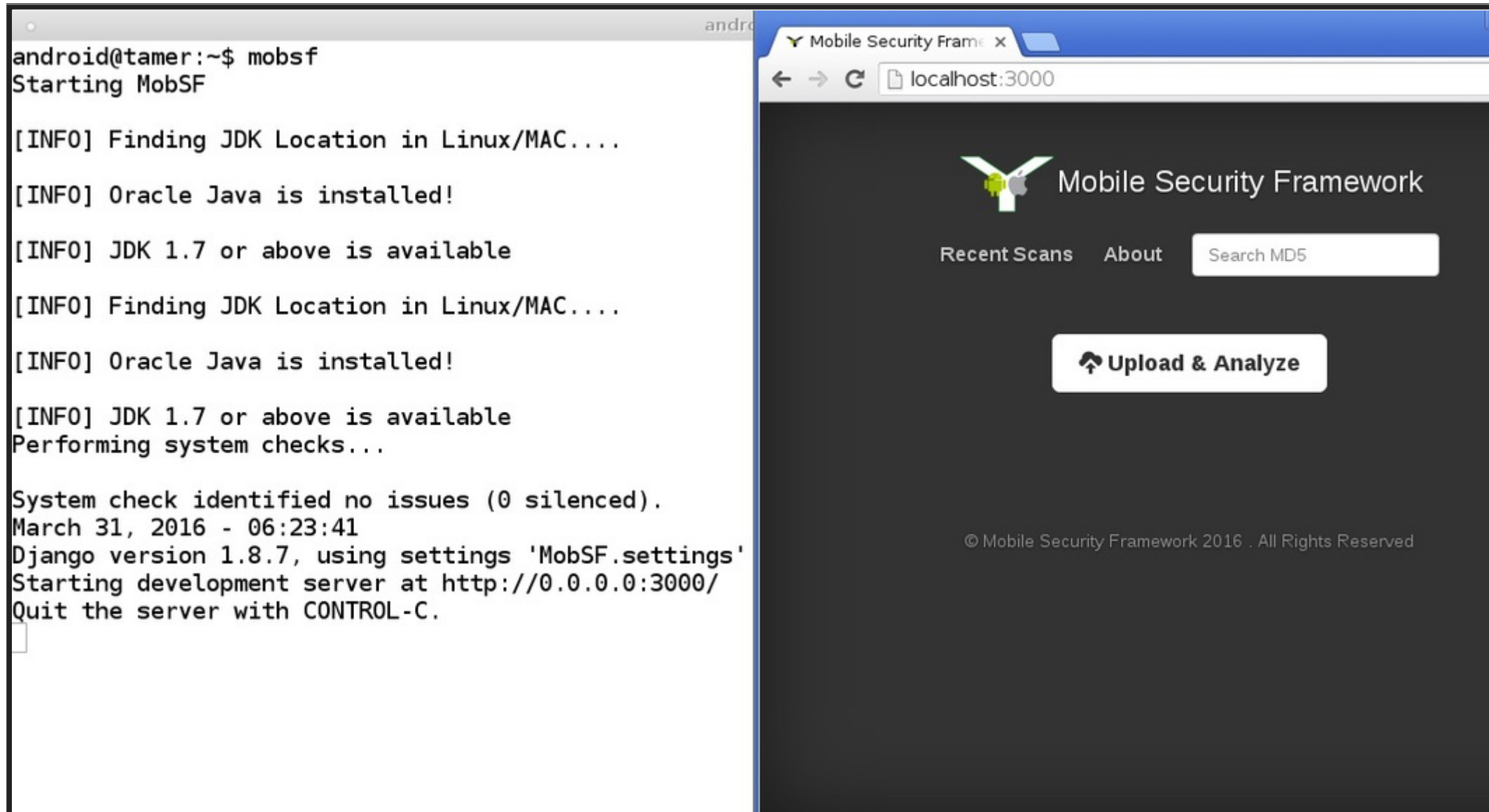
<manifest versionCode="1"
          versionName="1.0"
          package="jakhar.aseem.diva"
```

# 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



The image shows a terminal window on the left and a web browser on the right, both displaying the MobSF (Mobile Security Framework) interface.

**Terminal Window:**

```
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...

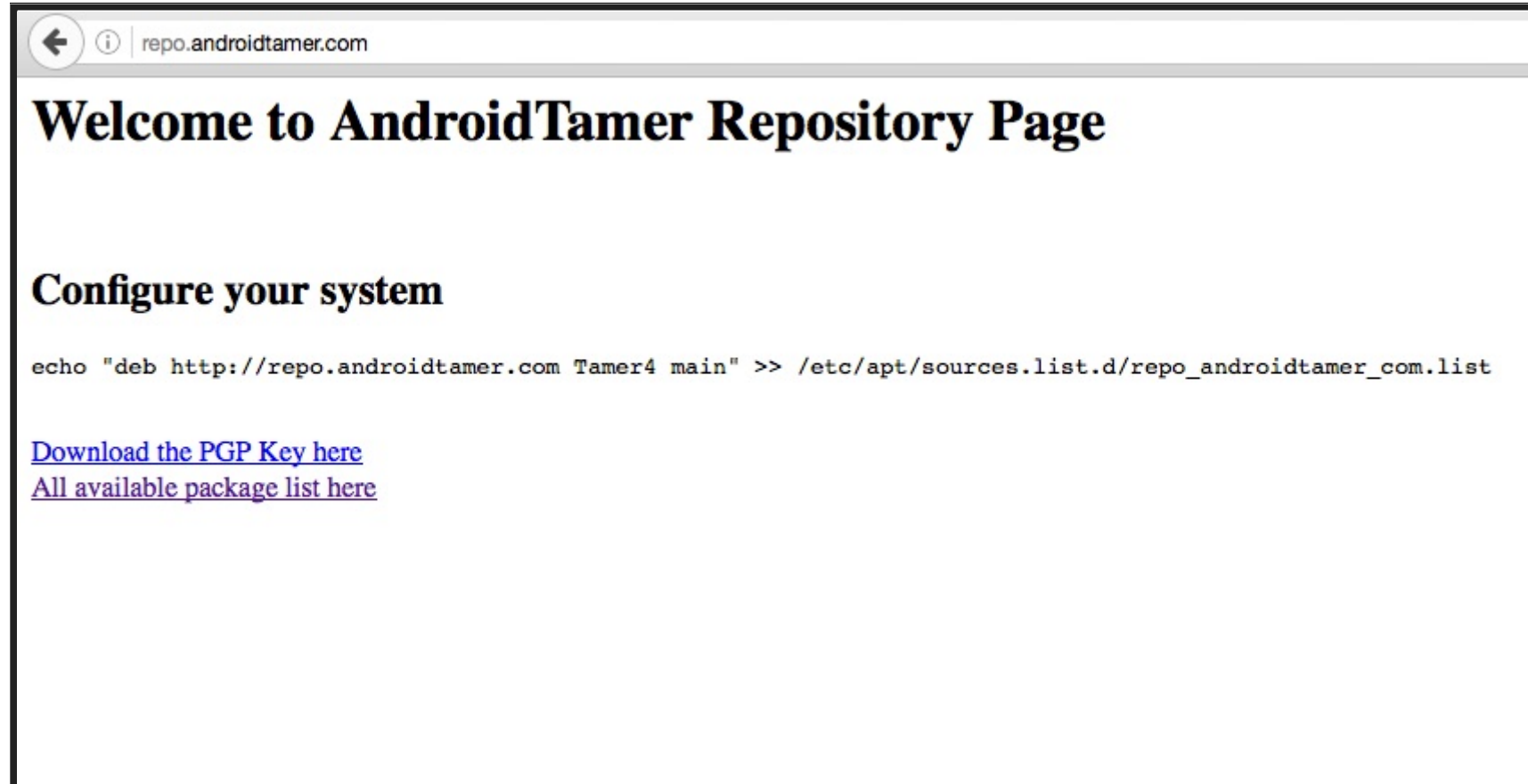
System check identified no issues (0 silenced).
March 31, 2016 - 06:23:41
Django version 1.8.7, using settings 'MobSF.settings'
Starting development server at http://0.0.0.0:3000/
Quit the server with CONTROL-C.
```

**Web Browser:**

The browser shows the MobSF web interface at `localhost:3000`. The interface includes a logo, navigation links for "Recent Scans" and "About", a "Search MD5" input field, and a prominent "Upload & Analyze" button. The footer indicates "© Mobile Security Framework 2016 . All Rights Reserved".

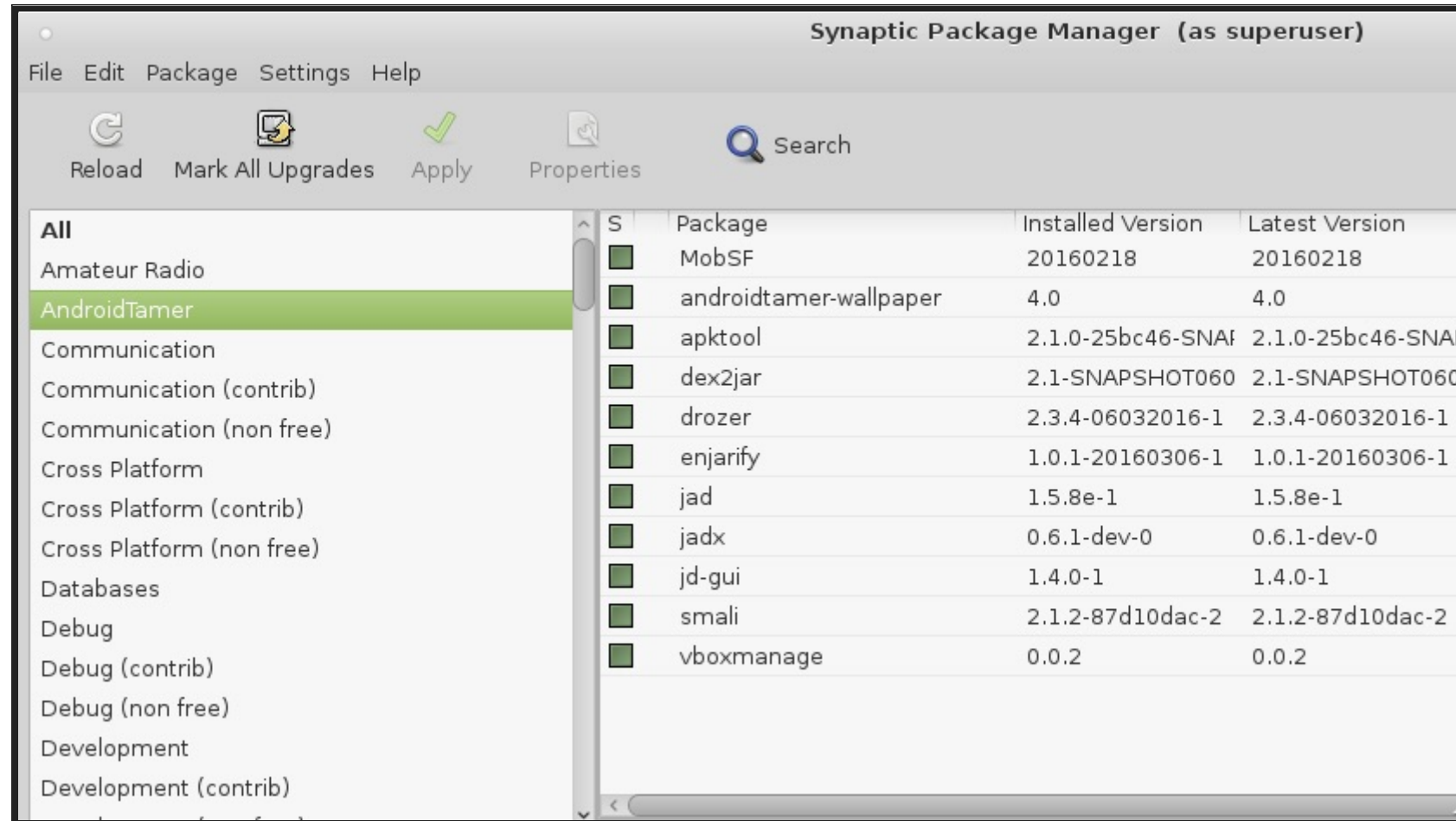


# BUILD YOUR OWN





# PACKAGE REPOSITORY



# SUGGESTIONS & SUPPORT

1. Suggest more tools
2. Issues / Challenges faced
3. Support by contributing to the project
4. Write articles & blogposts

# THANKS



Follow @AndroidTamer for all Updates