

# Mobsf vs our tool

## Activity detection :

The screenshot displays the MobSF static analysis interface. The left sidebar shows the 'APP SCORES' section with a Security Score of 33/100. The main area is divided into 'FILE INFORMATION' and 'APP INFORMATION'. The 'APP INFORMATION' section lists details such as App Name (AES), Package Name (com.apphacking.aes), Main Activity (com.apphacking.aes.MainActivity), Target SDK (30), Min SDK (23), and Android Version Name (1.0). Below this, there are four colored boxes representing different components: EXPORTED ACTIVITIES (0/1), EXPORTED SERVICES (0/0), EXPORTED RECEIVERS (0/0), and EXPORTED PROVIDERS (0/0). The right sidebar shows a terminal window with the command 'python basic-activity\_test12.py AES\_androidVersion12.apk' and its output, which lists the package name and activity details.

## Deep links :

The screenshot displays the MobSF static analysis interface, focusing on the 'DEEP LINKS' section. The left sidebar shows the 'ISSUE' section with a list of 7 issues. The main area shows the 'DEEP LINKS' section with a list of detected deep links. The right sidebar shows a terminal window with the command 'python basic-deep-links\_test12.py AES\_androidVersion12.apk' and its output, which lists the package name and deep link details.

NO	ISSUE	SEVERITY
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info
4	Debug Enabled For App [android:debuggable=true]	high
5	Application Data can be Backed up [android:allowBackup=true]	warning
6	Activity (com.apphacking.deeplinks.WebLink) is not Protected. [android:exported=true]	warning
7	Activity (com.apphacking.deeplinks.DeepLink) is not Protected. [android:exported=true]	warning

**Mobsf only detect that these activities ( which handle the links ) are exported and what intent invoke them but never tells if the deep links are hijackable or not which matters in both bug hunter's perspective and penetration tester**