# Lab 5 — MobSF Setup & Mobile App Static/Dynamic Scan

**Target:** Local MobSF instance (Kali Linux or Windows)  
**Tools Used:** MobSF (Docker or source), Git, Python 3.8/3.9, JDK, wkhtmltopdf, jadx, apktool, adb, emulator/device, Burp   
**Author:** Ishan Chowdhury

## Checklist

### 1. Environment preparation

Update system & install Git:

sudo apt-get update

sudo apt-get install -y git

Install Python 3.8/3.9, JDK, and required libs:

sudo apt-get install -y python3.8 python3-dev python3-venv python3-pip openjdk-11-jdk \

build-essential libffi-dev libssl-dev libxml2-dev libxslt1-dev libjpeg62-turbo-dev zlib1g-dev wkhtmltopdf

### 2. Download MobSF

Clone repo:

git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git

cd Mobile-Security-Framework-MobSF

### 3. Install & setup (Kali Linux)

Run setup script:

sudo ./setup.sh

Start MobSF (bind to localhost:8000):

./run.sh 127.0.0.1:8000

Open browser: <http://127.0.0.1:8000>

**Windows alternative (if using Windows):**

Install prerequisites (Git, Python 3.8/3.9, JDK, OpenSSL, wkhtmltopdf) and add wkhtmltopdf to PATH.

Clone repo and run:

git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git

cd Mobile-Security-Framework-MobSF

.\setup.bat

.\run.bat 127.0.0.1:8000

### 4. Verify MobSF UI & initial scan

Browse to http://127.0.0.1:8000 and confirm dashboard loads.

Upload sample vulnerable.apk via **Static Analysis** → **Upload & Scan**.

Save the generated report (HTML/JSON).

### 5. Static analysis follow-ups

Decompile and inspect with jadx:

jadx-gui vulnerable.apk

Decode resources with apktool:

apktool d vulnerable.apk -o vulnerable\_src

Search for hard-coded secrets or insecure settings:

grep -R "API\_KEY\|password\|SECRET\|hardcode" vulnerable\_src || true

### 6. Dynamic analysis — prepare device/emulator

Start adb and connect:

adb start-server

adb devices

Install APK on emulator/device:

adb install vulnerable.apk

Route device traffic through Burp (set proxy on device / emulator) and install Burp CA cert if intercepting TLS.

### 7. Cleanup

Stop MobSF:

pkill -f run.sh

Uninstall test app:

adb uninstall com.example.vulnapp