🐮

Frida

Frida is a dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.

Doc: https://frida.re/docs/home/

Installation:

1. Install on miniconda. If installation failed using company network, try to use self mobile network (tethering).

```
# Make sure install the latest version
pip install frida-tools

# Make sure install the latest version and same version wi
pip install frida
```

Running Emulator via CLI:

1. Open Miniconda Prompt.
2. Show list of emulator .

```
# Showing all available avd
emulator -list-avds
```

3. Select emulator. (example Pixel 4).

```
# -read-only is optional, you can't access file system.
# remove -read-only to access file system.
emulator -read-only -avd Pixel_4_API_30
```

3. Running adb shell

```
# Enter to the terminal devices
adb shell
```

4. Get device architecture, to download correct frida server

```
# Make sure the architecture same with frida server (x86 /
adb shell getprop ro.product.cpu.abi
```

Push Frida Server to Emulator:

1. After get device architecture (point 5 above), go to https://github.com/frida/frida/releases and download the correct frida server. example: frida-server-15.2.2-android-x86.xz

   (nb: download version same as frida on python. see pip list frida)

2. Extract downloaded file above, and rename it to '*frida-server*'.
3. Push frida to emulator. path on emulator */data/local/tmp*

```
# Make sure the tmp folder still empty.
# Or delete if the folder contain other version of frida-s
adb push frida-server /data/local/tmp
```

4. Run this command, to make sure frida server already pushed.

```
frida-ps -U
```

Install APK to Emulator:

1. Download APK and run this code

```
# You can run this command, or just drag an drop apk to th
adb install test.apk
```

Inject Script Into Application:

1. Open Miniconda Prompt → Select Emulator
2. Decompile APK target using JADX-GUI / APKTools

   UnCrackable-Level1.zip

3. Analyze Code and choose class to hook
4. Create inject script. For example (uncrackable1.js):

```
setImmediate(function() { //prevent timeout
    console.log("[*] Starting script");

    Java.perform(function() {

      var bClass = Java.use("sg.vantagepoint.uncrackable1.
      bClass.onClick.implementation = function(v) {
         console.log("[*] onClick called");
      }
      console.log("[*] onClick handler modified");

    })
})
```

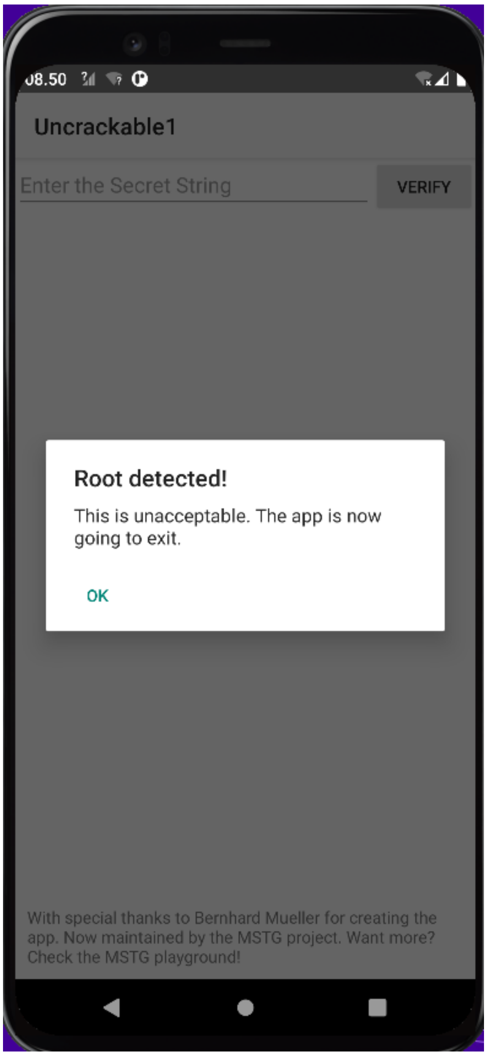
5. Open New Miniconda Prompt
6. Run command below

```
# Starting Device
adb devices

# Starting ADB as Root
adb root

# Ensure root access
adb root
adb remount
```

```
# Push Frida-Server to Emulator
adb push frida-server /data/local/tmp

# Change Permission
adb shell "chmod 755 /data/local/tmp/frida-server"

# Running Frida-Server
# Keep this terminal on, and open another conda terminal t
adb shell "/data/local/tmp/frida-server &"

# Install APK
adb install UnCrackable-Level1.apk

# Open Application on emulator

# Inject Script to Application
frida -U -l uncrackable1.js uncrackable1
```

7. Before Inject:

   If we press ‘OK’, Application will close automatically.



Uncrackable1

Enter the Secret String

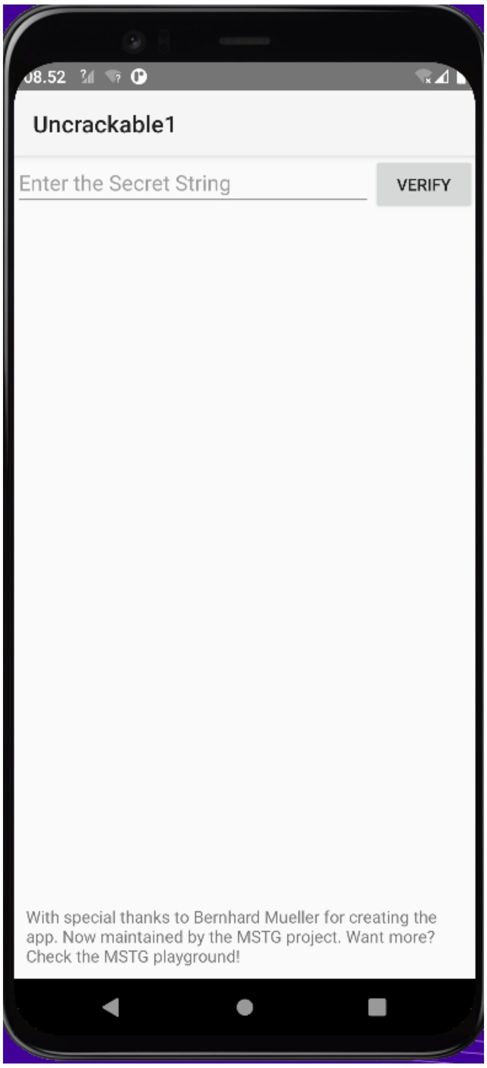
Root detected!

This is unacceptable. The app is now going to exit.

With special thanks to Bernhard Mueller for creating the app. Now maintained by the MSTG project. Want more? Check the MSTG playground!

8. After Inject:

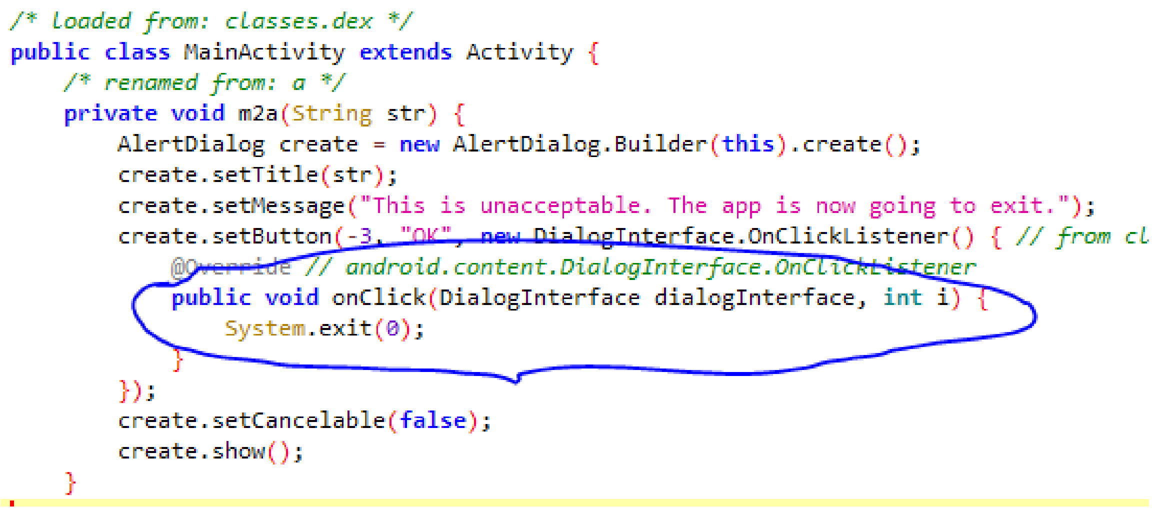
   If we Press ‘OK’, Application will enter to the next page like image below.



With special thanks to Bernhard Mueller for creating the app. Now maintained by the MSTG project. Want more? Check the MSTG playground!

9. Analyze:

   We inject method onClick below with script uncrackable1.js, and change to do nothing.



```
/* loaded from: classes.dex */
public class MainActivity extends Activity {
    /* renamed from: a */
    private void m2a(String str) {
        AlertDialog create = new AlertDialog.Builder(this).create();
        create.setTitle(str);
        create.setMessage("This is unacceptable. The app is now going to exit.");
        create.setButton(-3, "OK", new DialogInterface.OnClickListener() { // from cl
            @Override // android.content.DialogInterface.OnClickListener
            public void onClick(DialogInterface dialogInterface, int i) {
                System.exit(0);
            }
        });
        create.setCancelable(false);
        create.show();
    }
```

UPDATE

This command execute to spawn application. Example on OWASP Level 2.

```
# -D for device (frida-ls-devices) to check all devices
# -l to load javascript
# -f to set the target app (frida-ps -D emulator-5554 -ai)

#Example
frida -D emulator-5554 -l owasp_lv2.js -f owasp.mstg.uncracka
```