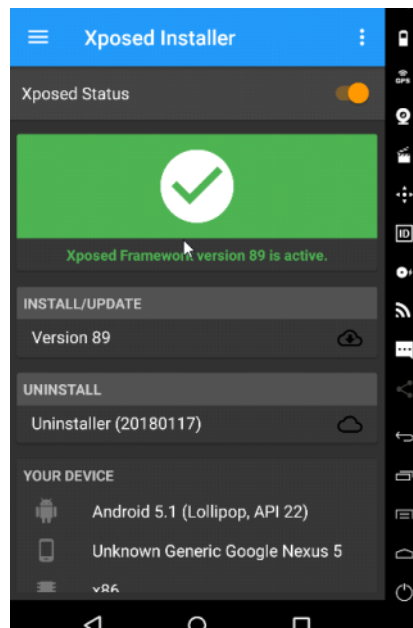


2nd WAY to solve this challenge

Wednesday, July 24, 2019 10:15 AM

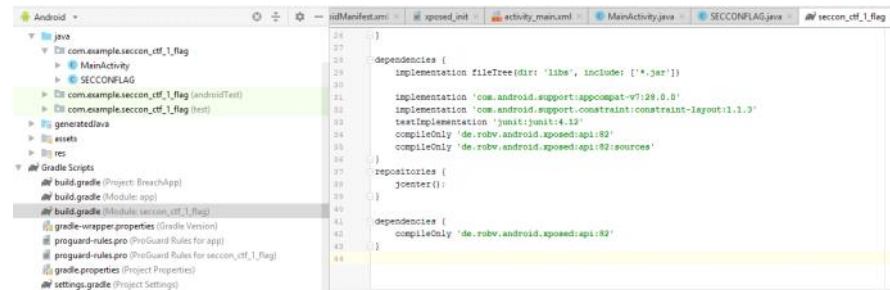
1. At first install xposed on genymotion/knox player and on any rooted device.



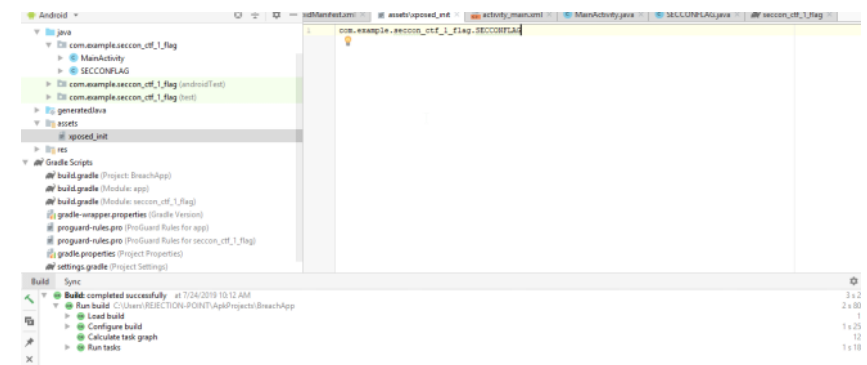
2. Now open ANDROID STUDIO AND CREATE A NEW PROJECT.
3. NOW GOTO GRADLE FILE AND PASTE BELOW COMMANDS:

```
compileOnly 'de.robv.android.xposed:api:82'
compileOnly 'de.robv.android.xposed:api:82:sources'
}
repositories {
    jcenter()
}

dependencies {
    compileOnly 'de.robv.android.xposed:api:82'
}
```



4. Now create a new folder in your application **assets**
 - And Create a new file with name **xposed_init** in assets folder.
 - In file write **package_name.class**



5. Now create a class for example I created from name SECCONFLAG

```
package com.example.secon_ctf_1_flag; //PACKAGE NAME
import android.view.View;

import de.robv.android.xposed.IXposedHookLoadPackage;
import de.robv.android.xposed.XC_MethodHook;
import de.robv.android.xposed.XposedBridge;
import de.robv.android.xposed.XposedHelpers;
import de.robv.android.xposed.callbacks.XC_LoadPackage.LoadPackageParam;

//ALL XPOSED MODULE IMPORT
```

```

Public class SECCONFLAG implements IXposedHookLoadPackage
{
    Public void handleLoadPackage(final LoadPackageParam lpparam) throws Throwable{
        XposedBridge.log("Loadedapp:"+lpparam.packageName);
        StringPackagename="com.example.seccon2015.rock_paper_scissors";
        StringMethod="onClick";
        Stringclasstohook=Packagename+".MainActivity";
        if(lpparam.packageName.equals(Packagename)){

            XposedHelpers.findAndHookMethod(classtohook,lpparam.classLoader,Method,View.class,newX
            C_MethodHook(){
                @Override
                protectedvoidafterHookedMethod(MethodHookParamparam) throwsThrowable{
                    //od
                    XposedHelpers.setIntField(param.thisObject,"cnt",999);
                    XposedHelpers.setIntField(param.thisObject,"m",0);
                    XposedHelpers.setIntField(param.thisObject,"n",1);

                }

            });

        }

    }
}

```

6. NOW INSTALL THE APP AND ACIVATE THE MODULE IN XPOSED AND RUN THE MAIN APPLICATION
7. RESTART THE DEVICE AND CLICK ON ANY BUTTON AND SEE OUTPUT

