

# Xposed从入门到弃坑：一、Xposed初探



WrBug (/u/348b77e56202) [+ 关注](#)

0.6 2017.04.26 14:28\* 字数 1017 阅读 11504 评论 11 喜欢 20

(/u/348b77e56202)

最近心血来潮，开始折腾xposed框架，xposed框架可以说得上是款Android系统God级别的开源hook框架，拥有非常高的权限，不过目前还暂不支持Android 7.0 以上的系统。这也是我一直没有升级的原因

## 什么是xposed

Xposed框架是一款可以在不修改APK的情况下影响程序运行(修改系统)的框架服务，基于它可以制作出许多功能强大的模块，且在功能不冲突的情况下同时运作。Xposed理论上能够hook到系统任意一个Java进程，由于是从底层hook，所以需要root权限，并且每次更新都要重新启动

Xposed官方git上面有几个开源项目，包括**XposedInstaller**、**Xposed**、**XposedBridge**、**XposedTools**，这里就不具体介绍了，感兴趣的可以查找相关资料，附上官方git地址：<https://github.com/rovo89> (<https://link.jianshu.com?t=https://github.com/rovo89>)

## Xposed模拟器环境搭建

由于Xposed项目每次安装都要重新启动，在真机上是非常耗时间的，所以在这里选择Genymotion模拟器，老版本的Genymotion模拟器有免费版本的，我提供一款mac版的模拟器。win自己百度下载，mac版下载地址：<https://pan.baidu.com/s/1pLDbymn> (<https://link.jianshu.com?t=https://pan.baidu.com/s/1pLDbymn>)，密码：j3rf。镜像选择Android5.0系统，其他版本类似。然后到官网下载Android5.0对应的框架，飞机直达 (<https://link.jianshu.com?t=http://dl-xda.xposed.info/framework/sdk21/x86/>)，选择.zip结尾的文件，下载完成后运行模拟器，将zip包拖到模拟器界面刷入即可，完成后重启模拟器。安装XposedInstaller\_3.1.1.apk ([https://link.jianshu.com?t=http://www.mandroid.cn/upload/2017/04/XposedInstaller\\_3.1.1%20.apk](https://link.jianshu.com?t=http://www.mandroid.cn/upload/2017/04/XposedInstaller_3.1.1%20.apk))应用，再次重启。进入刚刚安装的app，提示已激活即安装成功



## 第一个项目

### 创建Xposed工程

为了方便今后的教程，工程已传到github，可以直接clone该工程到本地。项目地址：<https://github.com/WrBug/XposedDemo> (<https://link.jianshu.com?t=https://github.com/WrBug/XposedDemo>)，后面的教程的代码也都将在这个工程里面，通过clone的可忽略下面创建工程的步骤。通过命令切换到提交：

(<https://log.yex.youda.com/slot=30edcd3f2-4f89-3e8aa0cb0Qld2p3NYclick.youdad3f2-4f89-3e8aa0cb0>)



```
git checkout 20195ce
```

创建一个新工程，build.gradle添加依赖：

```
provided 'de.robv.android.xposed:api:82'
```

编辑AndroidManifest.xml，添加：

```
<meta-data
    android:name="xposedmodule"
    android:value="true"/>
<meta-data
    android:name="xposeddescription"
    android:value="hello xposed"/>
<meta-data
    android:name="xposedminversion"
    android:value="82"/>
```

配置完成后，安装到模拟器，状态栏弹出如下提示：



(https://log  
yex.youda  
slot=30edc  
d3f2-4f89-i  
3e8aa0cb0  
Qld2p3NY  
click.youda  
d3f2-4f89-i  
3e8aa0cb0

## 第一个框架：Hello Xposed

git提交：43e4ba39e95988f0fa699ad5eddb1e55b9613638 (<https://link.jianshu.com?t=https://github.com/WrBug/XposedDemo/tree/43e4ba39e95988f0fa699ad5eddb1e55b9613638>)

## Activity创建

编辑activity\_main.xml，放入一个TextView：

```
<?xml version="1.0" encoding="utf-8"?>
<LinearLayout
    xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:orientation="vertical"
    tools:context="com.wrbug.xposeddemo.MainActivity">

    <TextView
        android:id="@+id/textview"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        app:layout_constraintBottom_toBottomOf="parent"
        app:layout_constraintLeft_toLeftOf="parent"
        app:layout_constraintRight_toRightOf="parent"
        app:layout_constraintTop_toTopOf="parent"/>

</LinearLayout>
```

MainActivity 里面设置文本信息：



```
public class MainActivity extends AppCompatActivity {
    TextView textView;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        textView = (TextView) findViewById(R.id.textview);
        textView.setText("WrBug");
    }
}
```

Activity很简单。就是一个textview的显示。安装到模拟器上，界面显示一行WrBug，下面通过xposed将WrBug修改成Hello Xposed显示。

思路：Xposed hook onCreate方法。在该方法执行完后获取TextView的实例。通过setText方法设置文本

## Xposed实现

新建一个类XposedInit实现IXposedHookLoadPackage，关于IXposedHookLoadPackage等接口，后面的文章会有说明。

```
public class XposedInit implements IXposedHookLoadPackage {
    @Override
    public void handleLoadPackage(final XC_LoadPackage.LoadPackageParam lpparam){
        //app启动时调用
    }
}
```

新建assets文件夹，文件夹下新建xposed\_init文件，编辑文件，填写XposedInit的完整包名：`com.wrbug.xposeddemo.XposedInit`

在XposedInit中handleLoadPackage方法会在应用启动时调用。所以需要筛选需要hook的app的包名，这里选择同个应用：

```
@Override
public void handleLoadPackage(final XC_LoadPackage.LoadPackageParam lpparam){
    if (lpparam.packageName.equals("com.wrbug.xposeddemo")) {

    }
}
```

通过XposedHelpers的findAndHookMethod方法hook onCreate 方法，获取到TextView实例，在方法执行后通过setText设置方法。

(https://log  
yex.youda  
slot=30edc  
d3f2-4f89-  
3e8aa0cb(  
Qld2p3NY  
click.youda  
d3f2-4f89-  
3e8aa0cb(  
Qld2p3NY



```
public class XposedInit implements IXposedHookLoadPackage {
    @Override
    public void handleLoadPackage(final XC_LoadPackage.LoadPackageParam lpparam) {
        if (lpparam.packageName.equals("com.wrbug.xposeddemo")) {
            XposedHelpers.findAndHookMethod("com.wrbug.xposeddemo.MainActivity", lpparam.classLoader, "onCreate",
            @Override
            protected void afterHookedMethod(MethodHookParam param) throws Throwable {
                //不能通过Class.forName()来获取Class，在跨应用时会失效
                Class c=lpparam.classLoader.loadClass("com.wrbug.xposeddemo.MainActivity");
                Field field=c.getDeclaredField("textView");
                field.setAccessible(true);
                //param.thisObject 为执行该方法的对象，在这里指MainActivity
                TextView textView= (TextView) field.get(param.thisObject);
                textView.setText("Hello Xposed");
            }
        }
    }
}
```

除了上面通过反射的方法来获取以外，还可以通过findViewById等方法获取TextView对象，**有兴趣的可以思考下如果xml里面没有设置TextView的ID，并且不是MainActivity的成员变量，该怎么获取这个View**，欢迎大家在下方进行讨论。安装重启模拟器后，打开app，这时textView将显示Hello Xposed

后面的文章会讲解具体的使用，欢迎大家关注  
更多精彩文章请关注：<http://www.mandroid.cn> (<https://link.jianshu.com?t=http://www.mandroid.cn>)

(https://log  
yex.youda  
slot=30edc  
d3f2-4f89-  
3e8aa0cb(  
Qld2p3NY  
click.youda  
d3f2-4f89-  
3e8aa0cb(  
)

小礼物走一走，来简书关注我

赞赏支持

📖 日记本 (/nb/4245583) 举报文章 © 著作权归作者所有




WtBug (/u/348b77e56202) ♂

写了 4098 字，被 39 人关注，获得了 31 个喜欢


(/u/348b77e56202)

+ 关注

喜欢 | 20



更多分享



下载简书 App ▶

随时随地发现和创作内容



(/apps/redirect?utm\_source=note-bottom-click)

