2021年7月5日

github配置流程

1. 配置本地密钥

```
ssh-keygen -t rsa -C "your_email@youremail.com"
```

2. 配置用户名和地址

```
$ git config --global user.name "your name"
$ git config --global user.email "your_email@youremail.com"
```

3. 初始化仓库

```
git init
```

4. 推送

```
git add <文件>
git commit -m "提交信息"
git remote git remote add origin <仓库地址>
git push origin master
```

5. 同步代码到本地

```
git remote add origin <仓库地址>
git pull origin master
```

xposed模块开发基本操作

1. 编辑AndroidManifest.xml文件

添加下列 meta-data 代码

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.batchathook">
```

```
    <application
        android:allowBackup="true"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.BatChatHook">
        <meta-data
            android:name="xposedmodule"
            android:value="true" />
        <meta-data
            android:name="xposeddescription"
            android:value="这是一个Xposed例程" />
        <meta-data
            android:name="xposedminversion"
            android:value="53" />
    </application>
</manifest>
```

2. 修改build.gradle

配置gradle报错时，修改gradle version版本为7.0 在 “项目名称/app/src/main/”目录下找到build.gradle，添加代码

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

3. 写hook代码

```
public class batChatHook implements IXposedHookLoadPackage {
    public void handleLoadPackage(XC_LoadPackage.LoadPackageParam
loadPackageParam) throws Throwable {
        if
(loadPackageParam.packageName.equals("com.example.root.xposd_hook_new")) {
            XposedBridge.log(" has Hooked!");
            Class clazz = loadPackageParam.classLoader.loadClass(
                    "com.example.root.xposd_hook_new.MainActivity");
            XposedHelpers.findAndHookMethod(clazz, "toastMessage", new
XC_MethodHook() {
                protected void beforeHookedMethod(MethodHookParam param) throws
Throwable {
                    super.beforeHookedMethod(param);
                    //XposedBridge.log(" has Hooked!");
                }
                protected void afterHookedMethod(MethodHookParam param) throws
Throwable {
```

```
                    param.setResult("你已被劫持");
                }
            });
        }
    }
}
```

4. 添加入口，方便xp找到hook类

右键点击 "main " 文件夹 ，选择new --> Folder -->Assets Folder，新建assets 文件夹，然后右键点击 assets文件夹，new--> file，文件名为xposed_init（文件类型选text），并在其中写上入口类的完整路径（就是自己编写的那一个Hook类），这样， Xposed框架就能够从这个 xposed_init 读取信息来找到模块的入口，然后进行Hook操作了。

脱壳打包

1. dex->smali

dex->smali dex2->smali_classes2

2. 把smali塞回去

3. 修改Androidmainfest.xml入口

4. apktool打包

```
java -jar apktool.jar b apkFile/
```

frida脱壳基本操作

2021年7月7日 汤德源

1. 安装python环境

安装frida

```
pip install frida-tools
```

2. 下载frida-server

GitHub地址 ***进入后 ctrl+F查找 frida-server,找到对应架构***

```
https://github.com/frida/frida/releases/tag/15.0.0
```

3. 启动frida-server

注意frida-server和frida版本要一置 将frida-server放到data/local/tmp下，设置权限chmod 777 frida-server 启动frida-server

```
./frida-server
```

4. 查看frida是否运行

出现进程pid和进程名就是运行成功

```
frida-ps -U
```

5. 下载脱壳脚本

```
pip install frida-dexdump
```

6. 开始脱壳

手机运行要脱壳的应用

```
frida-dexdump
```

此时开始脱壳

7. 脱壳后dex存放的路径

```
C:\Users\xxx\package_name
```

jdk免登录下载

1. 右击要下载的版本，复制链接获取真实免登录下载地址。

https://www.oracle.com/webapps/redirect/signon？nexturl=https://download.oracle.com/otn/java/jdk/8u271-b09/61ae65e088624f5aaa0b1d2d801acb16/jdk-8u271-windows-x64.exe

2. 替换直链中，otn为otn-pub，真实直链下载地址为

https://download.oracle.com/otn-pub/java/jdk/8u271-b09/61ae65e088624f5aaa0b1d2d801acb16/jdk-8u271-windows-x64.exe

小米查看版本

1. adb下

```
adb shell getprop ro.product.name
```

2. fastboot下

```
fastboot getvar product
```

蝙蝠解密步骤说明

仓库地址：https://github.com/best0127/batChatSql.git

1. 在database下找到batchatsql+uid.db数据库

2. 运行蝙蝠聊天数据库密钥-大写.jar，得到数据库密钥

```
java -jar 蝙蝠聊天数据库密钥-大写.jar
```

3. 在sqlcipher-3.0.1\bin下打开cmd

- 先打开加密数据库

```
sqlcipher.exe 加密数据库.db;
```

- 输入密钥

```
PRAGMA key = 'xxxxxx';
```

- 页大小

```
PRAGMA cipher_page_size = 4096;
```

- 导出解密数据库

```
ATTACH DATABASE 'batchatsql.db' AS batchatsql KEY '';
SELECT sqlcipher_export('batchatsql');
```

```
DETACH DATABASE batchatsql;
```

- 退出

```
.exit
```

4. 在当前目录下就能找到batchatsql.db的解密数据库