### 8.1.2 Xposed Hook-上

## 0x01 Hook 修改变量

在编写 hook 类的时候会去实现一个 IXposedHookLoadPackage 接口(加载应用程序,即" Android 软件包"时获得通知), 重写了 handleLoadPackage 方法(加载应用程序时将调用此方法),该方法有一个参数 lpparam(有关该应用程序的信息),这个方法向被实现的模块提供更多关于运行环境上下文的信息。首先我们实验的 app 是一款编写好的XposedDemo,将其安装到模拟器上,打开运行后没有任何效果,如图所示:



使用 jadx-gui 反编译工具查看其代码,注意在一个 Activity 在启动的时候,都会在onCreat()方法中执行 setContentView(R.layout.activity\_main)这行代码,来将指定的资源 xml 文件加载到对应的 activity 中。

The state of the s

相图

```
♦ *New Project - jadx-gui
```

```
文件 视图 导航 工具 帮助
🔤 陷 😘 😩 | 🎤 🔍 | 🐤 💠 | 🗟 | 🕒 | 🥕
및 XposedDemo.apk
                                           ⊙ com. feichen. xposeddemo. MainActivity 🗶
 → 源代码
  android
                                               oackage com.feichen.xposeddemo;
     🖶 🌐 arch

    ⊕ support

                                               import android.support.v7.app.AppCompatActivity;
import android.view.View;
  androidx
     m m core
                                              public class MainActivity extends AppCompatActivity {
     /* access modifiers changed from: prot
public void onCreate(Bundle bundle) {
     ⊞ @ Animal
                                                         er.onCreate(bundle):
                                           10
11
12
13
14
15
16
     ⊕ ⊕ BuildConfig
                                                      setContentView((int) R.layout.activity_main);
     ☐ Demo
☐ MainActivity
☐ myTest(View) void
                                                  public static void myTest(View view) {
    new Demo().test();
          • onCreate(Bundle) void
     - ❷ 资源文件

■ ■ META-INF

  = a res
     🗎 뛀 anim
    color color-v21
     ⊞ a color-v23
     in a drawable
     drawable-anydpi-v21
     🖶 🍃 drawable-hdpi
     ⊞ a drawable-ldpi
     arawable-ldrtl-hdpi-v17
     ⊞ □ drawable-ldrtl-mdpi-v17
     i a drawable-ldrtl-xhdpi-v17
     🖶 📴 drawable-ldrtl-xxhdpi-v17
     drawable-ldrtl-xxxhdni-v17...
```

然后定位到 res/layout/activity\_main.xml,可以发现当我们点击 button 的时候会触发 myTest 方法,回到 MainActivity,跟进 myTest()的 Demo 类。

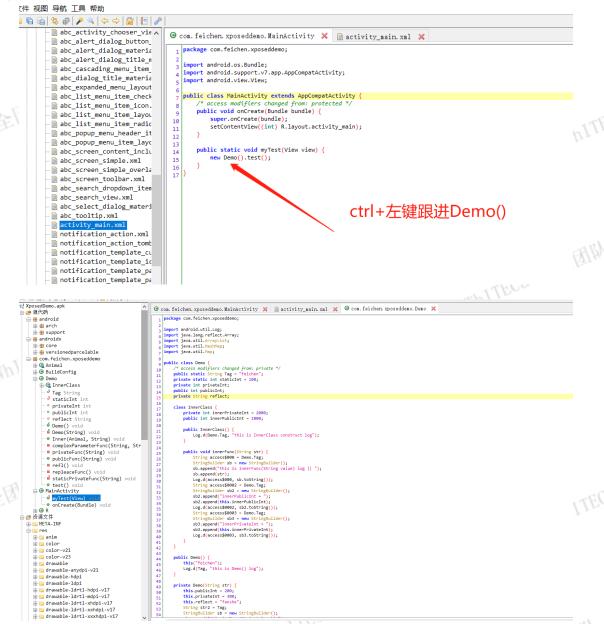


TECat安全国队

WhITECat安全团队

人图图

TECAT



经过分析 test()方法可以发现,当我们点击按钮时会在日志中输出很多对应的日志信息,其中包括静态变量 staticInt = 100,注意静态全局变量 hook 的时候调用的是使用的 XposedHelpers.setStaticIntField() , 若 是 全 局 普 通 变 量 用 XposedHelpers.setIntField()。

```
| public class Demo( /* access modifiers changed from: private */ public static String Tag = 'Feichen'; private static int staticint | 100; private int private int private int private; public int publicint; public int publicint; private String reflect;
```

WhITECat安全团队

ATES

```
public void test() {
         60
61
                     String str = Tag;
StringBuilder sb = new StringBuilder();
sb.append("staticInt");
sb.append(staticInt),
         62
         63
                     Log.d(str, sb.toString());

String str2 = Tag;

StringBuilder sb2 = new StringBuilder();
         65
                                                                                                    staticInt程序默认值是
         66
67
                     sb2.append("publicInt
                                                                                                    100.这里我们修改为
         68
69
                     sb2.append(this.publicInt);
Log.d(str2, sb2.toString());
                     String str3 = Tag;
StringBuilder sb3 = new StringBuilder();
sb3.append("privateInt = ");
sb3.append(this.privateInt);
                                                                                                    520
         72
73
                     Log.d(str3, sb3.toString());

publicFunc("feichen");

String str4 = Tag;

StringBuilder sb4 = new StringBuilder();

sb4.append("publicInt = ");
         75
         76
77
         78
79
                     sb4.append(this.publicInt);
         80
81
                     Log.d(str4, sb4.toString());

String str5 = Tag;

StringBuilder sb5 = new StringBuilder();
         83
                     sb5.append("privateInt
         84
85
                     sb5.append(this.privateInt);
b5.append(this.privateInt);
log.d(str5, sb5.toString());
privateFunc("feichen");
staticPrivateFunc("feichen");
         86
87
         88
89
                     String[][] strArr = (String[][]) Array.newInstance(String.class, new int[]{1, 2});
HashMap hashMap = new HashMap();
hashMap.put("key", "value");
ArrayList arrayList = new ArrayList();
         90
91
92
                     arraylist.add("listValue"):
             我们再次运行 app 点击按钮,不过此次打开我们的 ddms 查看日志输出。
                                      Application
com.feichen.xpos...
com.feichen.xpos...
                           PID
                                 TID
                                                                        this is Demo(String) log || feichen
                                 2336
2336
          09-16 10:36:32.379 2336
     D 09-16 10:36:32.379 2336
                                                                        this is Demo() log
D 09-16 10:36:32.379 2336
                                                                        staticInt = 100
                                 2336 com.feichen.xpos...
2336 com.feichen.xpos...
                                                          feichen
                                                                                                          未hook时, statciInt的值
      D 09-16 10:36:32.379 2336 2336 com.feichen.xpos... feichen
                                                                        privateInt = 300
                                                                         this is publicFunc(String value) log || feichen
        09-16 10:36:32.379 2336 2336 com.feichen.xpos...
09-16 10:36:32.379 2336 2336 com.feichen.xpos...
                                                                        publicInt = 200
                                                          feichen
        09-16 10:36:32.379 2336 2336 com.feichen.xpos...
                                                          feichen
                                                                        privateInt = 300
                                                                        this is privateFunc(String value) log || feichen
         09-16 10:36:32.379 2336
                                 2336
                                       com.feichen.xpos...
                                                          feichen
                                                                        this is staticPrivateFunc(Strin value) log || feichen
        09-16 10:36:32.379 2336
09-16 10:36:32.379 2336
                                       com.feichen.xpos...
                                                                        this is complexParameter(Strin value) log || feichen this is repleaceFunc log
                                 2336
      D 09-16 10:36:32.379 2336
                                 2336
                                       com.feichen.xpos...
                                                          feichen
                                                                        this is Inner log ||feichen
         09-16 10:36:32.379 2336
09-16 10:36:32.379 2336
                                 2336
2336
                                       com.feichen.xpos...
                                                                        this is eatFunc(String value) log || feichen
AnimalInt = 400
                                                          feichen
                                        com.feichen.xpos... feichen
        09-16 10:36:32.379 2336
                                 2336
                                        com.feichen.xpos... feichen
                                                                        this is InnerClass construct log
             然后编写 hook 代码如下:
      package com.xposed;
      import de.robv.android.xposed.lXposedHookLoadPackage;
                                                                                                                               TECat安全团队
      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;
      import android.util.Log;
      public class Hook implements IXposedHookLoadPackage {
             public void handleLoadPackage(final LoadPackageParam lpparam) throws
      Throwable {
                     Log.d("feichen", "hook..."); //日志输出方式一
                XposedBridge.log("Loaded app: " + lpparam.packageName); //日志输出方
                                                                                                                                                 m_TTECat
                     if (lpparam.packageName.equals("com.feichen.xposeddemo")){
                            final
                                                                   Class
```

clazz

XposedHelpers.findClass("com.feichen.xposeddemo.Demo",lpparam.classLoad er);

XposedHelpers.setStaticIntField(clazz,"staticInt",520);

```
安全即以
```

将写好的 xposed 编译安装到 xposed 后,勾选上写好的 xposed 模块,并重启手机,然后运行 app,打开 ddms,点击 button 按钮,查看 ddms 中的 staticInt 初始化值已经被我们 hook 修改为 520,如图:

```
Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit scope
                                      TID
       L... Time
                                              Application
                               PID
                                                                               Tag
                                              com.feichen.xp
                                                                               feichen
                                                                                               this is Demo(String) log || feichen
                                                                                              this is Demo() log
           09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
           09-17 00:19:44.435
                                              com.feichen.xposeddemo
       D 09-17 00:19:44.435 2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              publicInt = 200
                                      2288
           09-17 00:19:44.435
                               2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              privateInt = 300
                                              com.feichen.xposeddemo
                                                                                               this is publicFunc(String value) log || feichen
           09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              publicInt = 200
          09-17 00:19:44.435 2288
                                                                                              privateInt = 300
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
           09-17 00:19:44.435 2288
          09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              this is staticPrivateFunc(Strin value) log || feichen
          09-17 00:19:44.435
                                              com.feichen.xposeddemo
                                                                                              this is complexParameter(Strin value) log || feichen
          09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              this is repleaceFunc log
          09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                              feichen
                                                                                              this is Inner log ||feichen
          09-17 00:19:44.435 2288
                                                                                              this is eatFunc(String value) log || feichen
       D 09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              AnimalInt = 400
D 09-17 00:19:44.435 2288
                                                                                              this is InnerClass construct log
                                              com.feichen.xposeddemo
                                                                                              this is innerFunc(String value) log || feichen
       D 09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
                                                                                              innerPublicInt = 1000
       D 09-17 00:19:44.435 2288
                                      2288
                                              com.feichen.xposeddemo
                                                                               feichen
          09-17 00:19:44.435 2288
                                              com.feichen.xposeddemo
```

然 后 hook 字 符 串 变 量 的 话 使 用 XposedHelpers.setStaticObjectField(clazz,"Tag","Lvmeng");这一条语句,具体的效果这里不再演示,有兴趣的小伙伴下去可以自己尝试。

#### 0x02 Hook 普通方法

Hook 普通方法使用的是 XposedHelpers 下的 findAndHookMethod(类的字节码,方法名,回调函数)方法(用于 Hook 当前类下的所有方法),它有一个重载函数接收四个参数,

findAndHookMethod(类名全路径,类加载器,方法名,回调函数),其中回调函数除了使用

XC\_MethodHook()之外,还有 XC\_MethodReplacement()。对于有参数的函数需要带上参数的字节码。在 0x03 的地方就是四个参数的 findAndHookMethod。

因此, Hook 普通方法的代码如下:

XposedHelpers.findAndHookMethod(clazz, "test", new XC\_MethodHook(){
 public void beforeHookedMethod(MethodHookParam param){

```
Log.d("Lvmeng","Lvmeng========before");
}

public void afterHookedMethod(MethodHookParam param) {
            Log.d("Lvmeng","Lvmeng========after");
```

```
}
}):
```

ECat安生中 其中 beforeHookedMethod 会在调用原方法前执行,如果使用 setResult 则跳过原方法, 并返回 setResult 参数中的值。

afterHookedMethod 会在调用原方法后执行, setResult 可改变返回值。

replaceHookedMethod 会完全替换原方法,即原方法不执行,且返回值可以直接 return, setResult 不生效。

然后将写好的 xposed 编译安装到 xposed 后,勾选上写好的 xposed 模块,并重启手 机,然后运行 app,打开 ddms,点击 button 按钮,查看 ddms 中日志情况如下,可以发现 test()函数已经被成功 hook,并且添加上两条日志信息

```
this is Demo(String) log || feichen
                                                                                                                               this is Demo() log
                 09-17 10:33:18.815 3260
                                                               com.feichen.xposeddemo
                                                                                                          Lymeng
           D 09-17 10:33:18.815 3260
                                                    3260 com.feichen.xposeddemo
                 09-17 10:33:18.816 3260
                                                               com.feichen.xposeddemo
                                                                                                                               privateInt = 300
                09-17 10:33:18.816 3260
                                                     3260
                                                               com.feichen.xposeddemo
                                                                                                          Lymeng
                                                                                                                               this is publicFunc(String value) log || feichen
                09-17 10:33:18.816 3260
                                                               com.feichen.xposeddemo
                                                                                                                               publicInt = 200
                09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
                                                                                                         Lymeng
Lymeng
Lymeng
Lymeng
                                                              com.feichen.xposeddemo
                                                                                                                              privateInt = 300
this is privateFunc(String value) log || feicher
                                                             com.feichen.xposeddemo
                                                                                                                              this is staticPrivateFunc(Strin value) log || feichen this is complexParameter(Strin value) log || feichen
                09-17 10:33:18.816 3260
                                                              com.feichen.xposeddemo
                                                                                                          Lymena
                                                                                                         Lvmeng
Lvmeng
Lvmeng
Lvmeng
                09-17 10:33:18.816 3260
                                                               com.feichen.xposeddemo
                                                                                                                               this is repleaceFunc log
                09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
09-17 10:33:18.816 3260
                                                                                                                              this is Inner log ||feichen
this is eatFunc(String value) log || feicher
                                                               com.feichen.xposeddemo
                                                                                                                               AnimalInt = 400
                                                                                                                              this is InnerClass construct lo
                09-17 10:33:18.816 3260
                                                     3260
                                                               com.feichen.xposeddemo
D 09-17 10:33:18.816 3260
D 09-17 10:33:18.816 3260
D 09-17 10:33:18.816 3260
D 09-17 10:33:18.816 3260
                                                                                                                              this is innerFunc(String value) log || feichen
innerFublicInt = 1000
innerFrivateInt = 2000
                                                               com.feichen.xposeddemo
                                                               com.feichen.xposeddemo
                09-17 10:33:18.816 3260
                                                               com.feichen.xposeddemo
                                                                             WhITECat
```

#### 0x03 Hook 获取参数与返回值

Hook 获取参数是方法中要传入的参数,我们也是可以在 beforeHookedMethod 和 afterHookedMethod 方法中获取我们的参数值,其 hook 代码如下:

XposedHelpers.findAndHookMethod(clazz, "publicFunc", String.class, new XC MethodHook(){

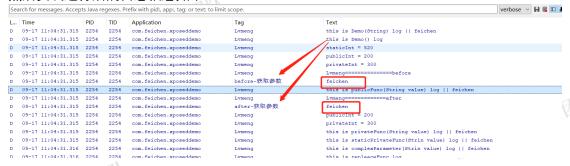
public void beforeHookedMethod(MethodHookParam param){

```
WhITECat安全团队
   Log.d("Lvmeng","Lvmeng======
}
     });
```

其中,我们 hook 的方法是 publicFunc, 查看代码可以发现该方法是接收参数的, 如图所

```
111
       112
                public void publicFunc(String str) {
       113
                   String str2 = Tag;
       114
                   StringBuilder sb = new StringBuilder();
       115
                   sb.append("this is publicFunc(String value) log || ");
       116
                   sb.append(str);
       117
                   Log.d(str2, sb.toString());
       118
       119
五年 120
```

#### 然后安装运行后的日志信息如下:



Hook 获取返回值一般都是在 afterHookedMethod 方法中,Hook 的代码如下:public void afterHookedMethod(MethodHookParam param) {
 Log.d("Lvmeng", ""+param.getResult());
}

在这里不再进行演示获取返回值,有兴趣的小伙伴可以下去自行测试。

Ox04 Hook 构造不坐

# 0x04 Hook 构造函数

Hook 构造函数可分为有参构造函数前、无参构造函数前、有参构造函数后和无参构造函数 后。这里 Hook 构造函数使用的是 XposedHelpers 下的findAndHookConstructor,详细代码如下:

```
XposedHelpers.findAndHookConstructor(clazz, new XC_MethodHook() {
    public void beforeHookedMethod(MethodHookParam param) throws
Throwable {
    Log.d("===============", "这是无参构造函数前");
}
```

```
public void afterHookedMethod(MethodHookParam param) throws
Throwable {
    Log.d("==============", "这是无参构造函数后");
    XposedHelpers.setIntField(param.thisObject, "publicInt", 20000000);
    }
});
```

TTECA

```
XposedHelpers.findAndHookConstructor(clazz,
                                                                                                                                                   String.class,
                                                                                                                                                                                                    new
              XC MethodHook() {
                        public void beforeHookedMethod(MethodHookParam param) throws
              Throwable {
                                 Log.d("===========","这是有参构造函数前");
安全团队
                                 param.args[0] = "= - = ";
                                             void
                                                              afterHookedMethod(MethodHookParam
                                                                                                                                                                     param)
                                                                                                                                                                                              throws
              Throwable {
                                 Log.d("==========","这是有参构造函数后");
                        }
              });
              然后安装运行后的 Hook 日志如下:
                                                         Application
                   09-17 13:21:17.726 2253
                                                                                                                             这是无参构造函数前
                                                 2253
                                                                                                                             这是有参构造函数前
this is Demo(String) 1
这是有参构造函数后
                                                         com.feichen.xposeddemo
                   09-17 13:21:17.726 2253
                                                 2253
                                                         com.feichen.xposeddemo
              D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmena
                                                                                                                            this is Demo() log
这是无参构造函数后
                                                                                                                             staticInt = 520
publicInt = 20000000
                   09-17 13:21:17.726
                                        2253
                                                         com.feichen.xposeddemo
     D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
D 09-17 13:21:17.726 2253
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lymeng
                                                                                                                             privateInt = 300
                                                         com.feichen.xposeddemo
                                                                                             Lymeng
before-获取参数
D 09-17 13:21:17.726 2253

D 09-17 13:21:17.727 2253
                                                                                                                             this is publicFunc(String value) log || feichen
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmeng
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                                                                              ===after
                                                         com.feichen.xposeddemo
com.feichen.xposeddemo
                                                                                             after-获取参数
                                                                                                                             feichen
                                                                                                                            publicInt = 20000000
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lymeng
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lymeno
                                                                                                                             privateInt = 300
                                                         com.feichen.xposeddemo
                                                                                             Lymeng
Lymeng
                                                                                                                             this is privateFunc(String value) log || feichen
this is staticPrivateFunc(Strin value) log || feichen
                                                                                                                             this is complexParameter(Strin value) log || feichen
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmeng
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmeng
                                                                                                                            this is repleaceFunc log
                                                 2253
2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmeng
Lvmeng
                                                                                                                            this is Inner log ||feichen
this is eatFunc(String value) log || feichen
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                             Lvmeng
                                                                                                                            AnimalInt = 400
                                                 2253
                                                         com.feichen.xposeddemo
                                                                                                                            this is InnerClass construct loc
                                                         com.feichen.xposeddemo
                                                                                                                            this is innerFunc(String value) log || feichen innerFublicInt = 1000
                                  WHITECat 安全图M
                  09-17 13:21:17.727 2253
                                                                                            Lymeng
                                                                                                                            innerPrivateInt = 2000
```

WhITECat安全团队

TTECat安全团队

WhITECat安全团队

相图字

TTECat