

# 看雪3万课程笔记-FRIDA高级API实用方法: Frida Hook Java (三) 主动调用静态函数和非静态函数

原创

kfyjd2008 于 2022-02-16 10:55:54 发布 235 收藏

分类专栏: [安卓](#) 文章标签: [安卓逆向](#) [frida hook](#) [看雪三万](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/kfyjd2008/article/details/122958764>

版权



[安卓专栏收录该内容](#)

19 篇文章 5 订阅

订阅专栏

本节接上一节课, APP进入第二关。

本节知识点为主动调用静态函数和非静态函数的实现:

观察代码可以发现关键判断点为两个变量的值是否为True, 有两个改变值得函数可以调用。

```
public class FridaActivity2 extends BaseFridaActivity {
    private static boolean static_bool_var = false;
    private boolean bool_var = false;

    @Override // com.example.androiddemo.Activity.BaseFridaActivity
    public String getNextCheckTitle() {
        return "当前第2关";
    }

    private static void setStatic_bool_var() {
        static_bool_var = true;
    }

    private void setBool_var() {
        this.bool_var = true;
    }
}

@Override // com.example.androiddemo.Activity.BaseFridaActivity
public void onCheck() {
    if (!static_bool_var || !this.bool_var) {
        super.CheckFailed();
        return;
    }
    CheckSuccess();
    startActivity(new Intent(this, FridaActivity3.class));
    finishActivity(0);
}
}
```

静态函数调用改变变量值

私有函数调用改变变量值

CSDN @kfyjd2008

hook代码:

```
function call_FridaActivity2() {
  //主动调用函数
  Java.perform(function () {
    var FridaActivity2 = Java.use("com.example.androiddemo.Activity.FridaActivity2");
    FridaActivity2.setStatic_bool_var();    //调用静态函数

    Java.choose("com.example.androiddemo.Activity.FridaActivity2",{
      onMatch:function(instance){
        instance.setBool_var();
      },
      onComplete:function(){

      }
    });
  })
}
```

然后在frida命令行中主动调用该函数即可通关。

call\_FridaActivity2()