

# 看雪3万课程笔记-FRIDA高级API实用方法: Frida Hook Java (七) 遍历所有类对类方法hook

原创

kfyjd2008 于 2022-02-16 17:54:19 发布 140 收藏

分类专栏: [安卓](#) 文章标签: [安卓hook](#) [安卓逆向](#) [frida hook](#) [frida](#) [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/122968963>

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进入第六关。

本节知识点为遍历所有已加载类并hook类方法:

本关代码如下:

```
package com.example.androiddemo.Activity;

import android.content.Intent;
import com.example.androiddemo.Activity.Frida6.Frida6Class0;
import com.example.androiddemo.Activity.Frida6.Frida6Class1;
import com.example.androiddemo.Activity.Frida6.Frida6Class2;

public class FridaActivity6 extends BaseFridaActivity {
    @Override // com.example.androiddemo.Activity.BaseFridaActivity
    public String getNextCheckTitle() {
        return "当前第6关";
    }

    @Override // com.example.androiddemo.Activity.BaseFridaActivity
    public void onCheck() {
        if (!Frida6Class0.check() || !Frida6Class1.check() || !Frida6Class2.check()) {
            super.CheckFailed();
            return;
        }
        CheckSuccess();
        startActivity(new Intent(this, FridaActivity7.class));
        finishActivity(0);
    }
}
```

外部类

关键判断点

CSDN @kfyjd2008

有两种方法可以过本关卡:

方法1: 直接hook

```

function hook_FridaActivity6(){
  Java.perform(function(){
    var Frida6Class0 = Java.use("com.example.androiddemo.Activity.Frida6.Frida6Class0");
    Frida6Class0.check.implementation = function(){
      return true;
    };
    var Frida6Class1 = Java.use("com.example.androiddemo.Activity.Frida6.Frida6Class1");
    Frida6Class1.check.implementation = function(){
      return true;
    };
    var Frida6Class2 = Java.use("com.example.androiddemo.Activity.Frida6.Frida6Class2");
    Frida6Class2.check.implementation = function(){
      return true;
    };
  })
}

```

方法二：遍历所有类并hook方法

```

function hook_mul_class(){
  //遍历所有类对类方法hook
  Java.perform(function(){
    Java.enumerateLoadedClasses({//enumerateLoadedClasses()返回数组中的类名。
      onMatch:function(name,handle){
        // console.log(name);
        if(name.indexOf("com.example.androiddemo.Activity.Frida6") >= 0){
          console.log(name);
          var fridaClass6 = Java.use(name);
          fridaClass6.check.implementation = function(){
            console.log("frida 6 check",this);
            return true;
          };
        }
      },onComplete:function(){
    }
  })
})
}

```

第二个方法我测试时不知道为什么只遍历出一个类

com.example.androiddemo.Activity.Frida6.Frida6Class0

其他两个没有遍历出来，望知道的大佬解惑。