看雪3万课程笔记-FRIDA高级API实用方法：Frida Hook Java（五）访问内部类函数

原创

kfyzjd2008 于 2022-02-16 11:36:17 发布 131 收藏
分类专栏： 安卓 文章标签： 安卓逆向 frida fridahook 看雪三万

本文链接：https://blog.csdn.net/kfyzjd2008/article/details/122959946

本节接上一节课，APP进入第四关。

本节知识点为访问内部类函数：

观察代码可以发现关键判断点为六个内部类函数的返回值是否为true

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

import android.content.Intent;

public class FridaActivity4 extends BaseFridaActivity {
    @Override // com.example.androiddemo.Activity.BaseFridaActivity
    public String getNextCheckTitle() {
        return "当前第4关";
    }

    private static class InnerClasses {
        public static boolean check1() {
            return false;
        }

        public static boolean check2() {
            return false;
        }

        public static boolean check3() {
            return false;
        }

        public static boolean check4() {
            return false;
        }

        public static boolean check5() {
            return false;
        }

        public static boolean check6() {
            return false;
        }

        private InnerClasses() {
        }
    }

    @Override // com.example.androiddemo.Activity.BaseFridaActivity
    public void onCheck() {
        if (!InnerClasses.check1() || !InnerClasses.check2() || !InnerClasses.check3() || !InnerClasses.check4() || !InnerClasses.check5() || !InnerClasses.check6()) {
            super.CheckFailed();
            return;
        }
        CheckSuccess();
        startActivity(new Intent(this, FridaActivity5.class));
        finishActivity(0);
    }
}
```

当前类

内部类

关键判断点

相应hook代码：

```
function hook_InnerClasses(){
    //访问内部类函数
    Java.perform(function(){
        //访问内部类时，在当前类后加$符号，后跟内部类名
        var InnerClasses = Java.use("com.example.androiddemo.Activity.FridaActivity4$InnerClasses");
        console.log(InnerClasses);
        InnerClasses.check1.implementation = function(){
            return true;
        };
        InnerClasses.check2.implementation = function(){
            return true;
        };
        InnerClasses.check3.implementation = function(){
            return true;
        };
        InnerClasses.check4.implementation = function(){
            return true;
        };
        InnerClasses.check5.implementation = function(){
            return true;
        };
        InnerClasses.check6.implementation = function(){
            return true;
        };

    });
}
```

然后在frida命令行中主动调用该函数即可通关。

hook_InnerClasses()