看雪3万课程笔记-FRIDA高级API实用方法：Frida Hook Java（四）读写静态变量和非静态变量

原创

kfyzjd2008 于 2022-02-16 11:15:44 发布 144 收藏 2
分类专栏： 安卓 文章标签： 安卓逆向 frida frida hook 看雪三万

本文链接：https://blog.csdn.net/kfyzjd2008/article/details/122959348

本节接上一节课，APP进入第三关。

本节知识点为读写静态变量和非静态变量：

观察代码可以发现关键判断点为三个变量的值是否为True，其中一个私有变量名同函数名一样。

```
3  public class FridaActivity3 extends BaseFridaActivity {
       private static boolean static_bool_var = false;
       private boolean bool_var = false;
       private boolean same_name_bool_var = false;

       @Override // com.example.androiddemo.Activity.BaseFridaActivity
       public String getNextCheckTitle() {
           return "当前第3关";
       }

1      private void same_name_bool_var() {
2          Log.d("Frida", static_bool_var + " " + this.bool_var + " " + this.same_name_bool_var);
       }

       @Override // com.example.androiddemo.Activity.BaseFridaActivity
5      public void onCheck() {
7          if (!static_bool_var || !this.bool_var || !this.same_name_bool_var) {
3              super.CheckFailed();
3              return;
           }
8          CheckSuccess();
9          startActivity(new Intent(this, FridaActivity4.class));
1          finishActivity(0);
       }
   }
```

同名

判断点

相应hook代码：

```
function call_FridaActivity3() {
    //读写静态变量和非静态变量
    Java.perform(function(){
        var FridaActivity3 = Java.use("com.example.androiddemo.Activity.FridaActivity3");
        FridaActivity3.static_bool_var.value = true;//访问静态变量
        console.log(FridaActivity3.static_bool_var.value);
        //访问非静态变量
        Java.choose("com.example.androiddemo.Activity.FridaActivity3",{
            onMatch:function(instance){
                instance.bool_var.value = true;
                instance._same_name_bool_var.value = true;//访问有同名函数的变量时应加_
                console.log(instance.bool_var.value,instance._same_name_bool_var.value);
            },
            onComplete:function(){

            }
        });
    })
}
```

然后在frida命令行中主动调用该函数即可通关。

call_FridaActivity3()