XPOSED(VXP)/FRIDA Report of PoRE

Student ID　20307130044
Name　徐俊伟

- **Tasks List**

Write down the tasks list you finished and the corresponding score
1.懂球帝 app 跳过开屏广告（xposed）　2 points
2.美食天下 app 跳过开屏广告（frida）　2 points
3.旅法师营地 app 隐藏推广按钮防止误触　3 points
4.哔哩哔哩 app 提醒观看时间，督促　3 points

- **Project Demo Video**

Baidu Netdisk share link (and verify code)
链接：https://pan.baidu.com/s/1RPZPuiClWfAYV_u806p4YA
提取码：60s7

- **Task1**
- **Introduction**

Introduce the task briefly

懂球帝 app 看足球新闻是开屏没广告，不用等待

- **How you find the target function**

Introduce how you reversed the target apk and located the target function you want to hook

1. 第一步先打开夜神模拟器，通过助教给的链接设置其 ro.debuggable == 1，然后就可以被 monitor 监视到
2. 然后打开懂球帝 app，因为这个 app 有时是开屏的小男孩，有时是广告，所以需要反复刷，刷到有广告的时候，并监控到点击“跳过”的 onclick 行为

有启动界面无广告

有启动界面有广告

3. 找到 onclick 后，一层一层往下找，找到最后的新闻页面为：
com.dongqiudi.news.MainActivity

4：其实我的第一解决办法是，如果产生广告页面，就自动点击 onclick，但是不知道为什么，

这条类总是会爆出类不存在的问题，所以只能转换方向

- **How you hooked the function**

  Introduce how you hook the target functions to realize your goal

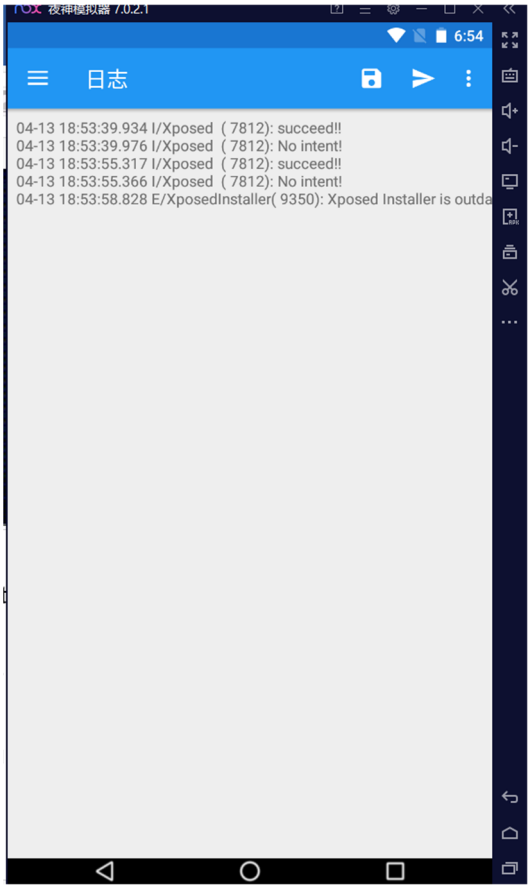
1：我突然想到，虽然开屏的方式可能会变化，但是相同的就是，他们都不是主活动，只要我直接检测当前不是 mainactivity，然后直接跳到 MainActivity，不就没有这个烦恼了吗，

2：于是我选用了 beforehookmethod，在开屏的时候通过 package manager 和 now_activity 的 getLaunchIntentForPackage 和 getintent 两个方法分别拿到启动 activity 和广告 activity，判断如果当前 activity 为广告 activity，则启动主 activity 并结束广告 activity

代码如下

```java
public class Main implements IXposedHookLoadPackage {
    @Override
    public void handleLoadPackage(XC_LoadPackage.LoadPackageParam loadPackageParam) throws Throwable {
        if (loadPackageParam.packageName.equals("com.dongqiudi.news")) {
            XposedBridge.log("hooking!!");
            ClassLoader classLoader = loadPackageParam.classLoader;
            final String main_activity_Name = "com.dongqiudi.news.MainActivity";
            XposedHelpers.findAndHookMethod("android.app.Activity", classLoader, "onStart", new XC_MethodHook() {
                        @Override
                        protected void beforeHookedMethod(MethodHookParam param) throws Throwable {
                            Activity now_activity = (Activity) param.thisObject;
                            Intent launch_intent, ads_intent;
                            PackageManager packageManager = now_activity.getPackageManager();
                            launch_intent = packageManager.getLaunchIntentForPackage(now_activity.getPackageName());
                            ads_intent = now_activity.getIntent();
                            if (launch_intent != null && ads_intent != null)
                                if (launch_intent.getComponent().flattenToString().equals(ads_intent.getComponent().flattenToString())) {
                                    Intent main_intent = new Intent();
                                    main_intent.setClassName(now_activity, main_activity_Name);
                                    now_activity.finish();
                                    now_activity.startActivity(main_intent);
                                    XposedBridge.log(("succeed!!"));
                                }
                            else
                                {
                                    XposedBridge.log("No intent!");
                                }
                        }
                    }
            );
        }
    }
}
```

7：结果



- **Task2**
- **Introduction**

  Introduce the task briefly

  美食天下是一个做饭的 app，也是进去有开屏广告，但是我使用 frida 框架，

  并换一种方式来进行广告的跳过

- **How you find the target function**

  Introduce how you reversed the target apk and located the target function you want to hook

0. 本来我的 frida 不想做同一个的，但是奈何自己有点笨，感觉 frida 很难，所以和助教咨询了，在用不同方法实现两个广告跳过，都给两分，先为每种方法打个基础

1. 第一步先打开夜神模拟器，通过助教给的链接设置其 ro.debuggable == 1，然后就可以被 monitor 监视到

2. 然后打开美食天下 app，有之前的经验，所以先去 onclick，然后找到对应的 activity，这次是 com.meishichina.android.activity.WelcomeActivity，然后找到加载进程的函数。

3. 这次其实比之前更没头绪一点，因为他混杂的很厉害，看一下 oncreate，主要看这里几个函数。

```
protected void onCreate(Bundle arg2) {
    super.onCreate(arg2);
    this.a(0);
    StatService.start(this);
    if(this.m()) {
        this.s();
        return;
    }

    this.b(false);
}
```

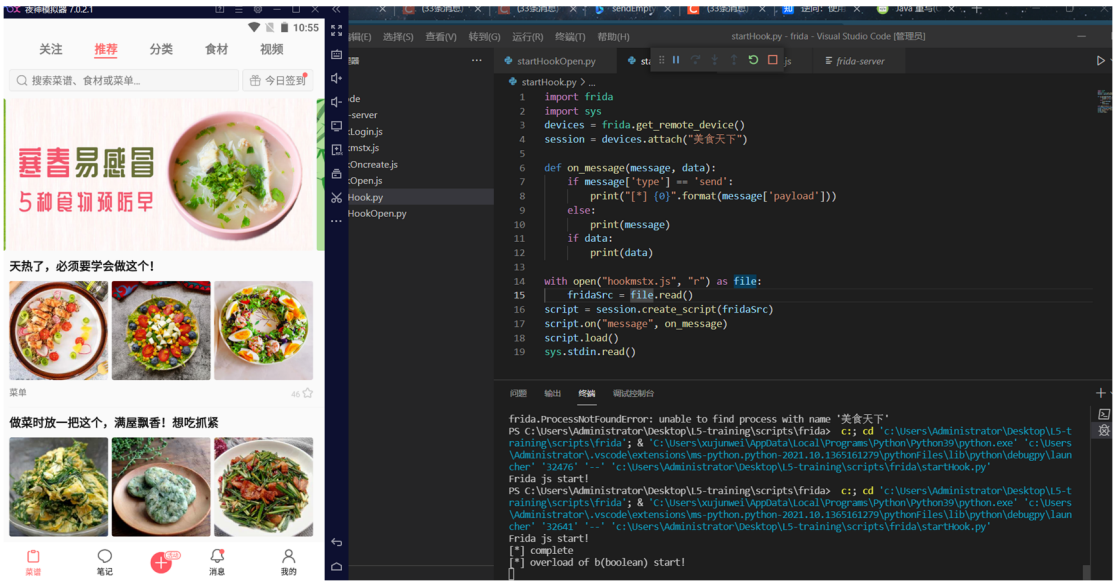
4. 看到 b（boolean arg6）我就很确定了，因为有一个 sendEmptyMessageDelayed 函数，后面还有 home_event_getEventShow 之类的，我能确定就是这个函数控制了广告。

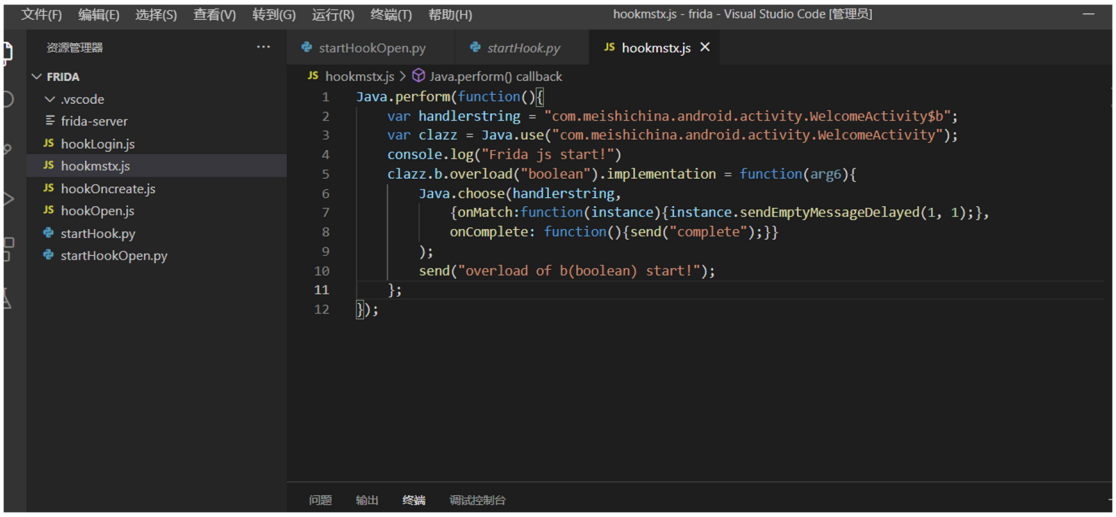
- **How you hooked the function**

  Introduce how you hook the target functions to realize your goal

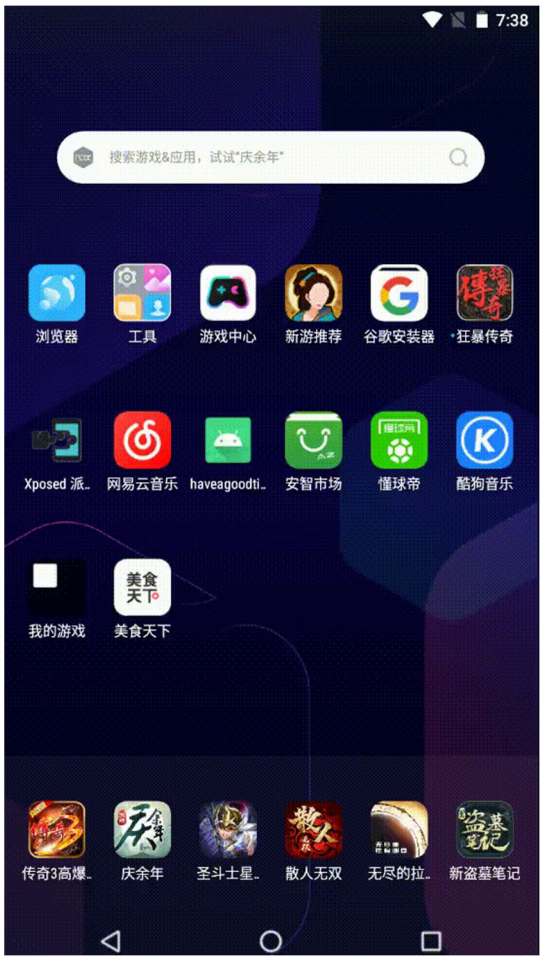
1. 这一段的功能是 5000 毫秒之后会发送一个空消息，若结果为假，就执行。所以我做的是加速。改成（1，1），就只有 1ms 的延迟了，就起到了去广告效果。

```
private void b(boolean arg6) {
    this.n();
    if(a.a(this.getIntent(), this.L)) {
        this.G.sendEmptyMessageDelayed(1, 5000L);
        return;
    }

    this.F = this.getIntent().getStringExtra("umeng_url");
    w0.a(this.d, "home_event_getEventShow", "json", "");
    this.E = this.getIntent().getStringExtra("notify_extras");
    boolean v0 = this.getIntent().getBooleanExtra("reLoad", false);
    this.D = v0;
    if(!v0) {
        RecipeDetailsActivity.p();
        w0.a(this.d, "com.meishichina.android.activity.PaiDetails", "ad_data", "");
    }

    if((n0.a(this.E)) && (n0.a(this.F))) {
        if(x0.b(this.d) == 0) {
            w0.f(this.d);
            this.finish();
            return;
        }

        if(x0.a(this.d) == 0) {
            this.finish();
            return;
        }

        if(!this.D && (this.getIntent().getFlags() & 0x400000) != 0) {
            this.finish();
            return;
        }
    }

    if(arg6) {
        this.G.sendEmptyMessage(1);
        return;
    }

    this.setContentView(0x7F0C0042);  // layout:activity_splash
    this.A = (ImageView)this.findViewById(0x7F0901A4);  // id:activity_splash_image
```


关注
推荐
分类
食材
视频
搜索菜谱、食材或菜单...
今日签到
5种食物预防早
天热了，必须要学会做这个！
菜单
做菜时放一把这个，满屋飘香！想吃抓紧
菜谱
笔记
消息
我的
startHookOpen.py
startHook.py
frida-server
import frida
import sys
devices = frida.get_remote_device()
session = devices.attach("美食天下")
def on_message(message, data):
if message['type'] == 'send':
print("[*] {0}".format(message['payload']))
else:
print(message)
if data:
print(data)
with open("hookmstx.js", "r") as file:
fridaSrc = file.read()
script = session.create_script(fridaSrc)
script.on("message", on_message)
script.load()
sys.stdin.read()
问题
输出
终端
调试控制台
frida.ProcessNotFoundError: unable to find process with name '美食天下'
Frida js start!
[*] complete
[*] overload of b(boolean) start!


文件(F)
编辑(E)
选择(S)
查看(V)
转到(G)
运行(R)
终端(T)
帮助(H)
hookmstx.js - frida - Visual Studio Code [管理员]
资源管理器
FRIDA
.vscode
frida-server
hookLogin.js
hookmstx.js
hookOncreate.js
hookOpen.js
startHook.py
startHookOpen.py
startHookOpen.py
startHook.py
hookmstx.js
hookmstx.js > Java.perform() callback
Java.perform(function(){
var handlerstring = "com.meishichina.android.activity.WelcomeActivity$b";
var clazz = Java.use("com.meishichina.android.activity.WelcomeActivity");
console.log("Frida js start!")
clazz.b.overload("boolean").implementation = function(arg6){
Java.choose(handlerstring,
{onMatch:function(instance){instance.sendEmptyMessageDelayed(1, 1);},
onComplete: function(){send("complete");}}
);
send("overload of b(boolean) start!");
};
});
问题
输出
终端
调试控制台

前后对比：



- **Task3**
- **Introduction**
  Introduce the task briefly

  旅法师营地 app 是一个我用来玩炉石传说的看卡组的软件，但是她会有一些

  推广什么的按钮，我要给他隐藏起来

- **How you find the target function**
  Introduce how you reversed the target apk and located the target function you want to hook

1. 这次是通过截屏的方式寻找的，就不要需要开 ro.debuggable 了，通过标注找的这个控件的 resource id 和所在 package = “com.gonlan.iplaymtg”

首页 炉石传说 万智牌 漫威对决 影:

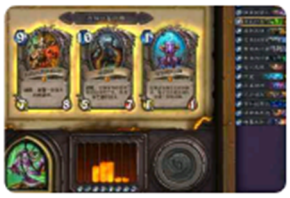
510613
Lv.41

有关现版本德鲁伊强势原因的讨论

截至目前，hsreplay上统计的德鲁伊胜率达到53.7%，位居第二，和战士的56.3%有一定的距离，比新版本第一天高出...

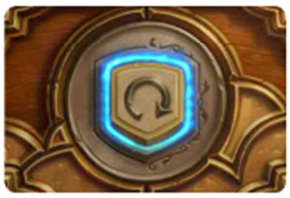
炉石传说 18 34

这是我的jjc橙卡



炉石传说 1

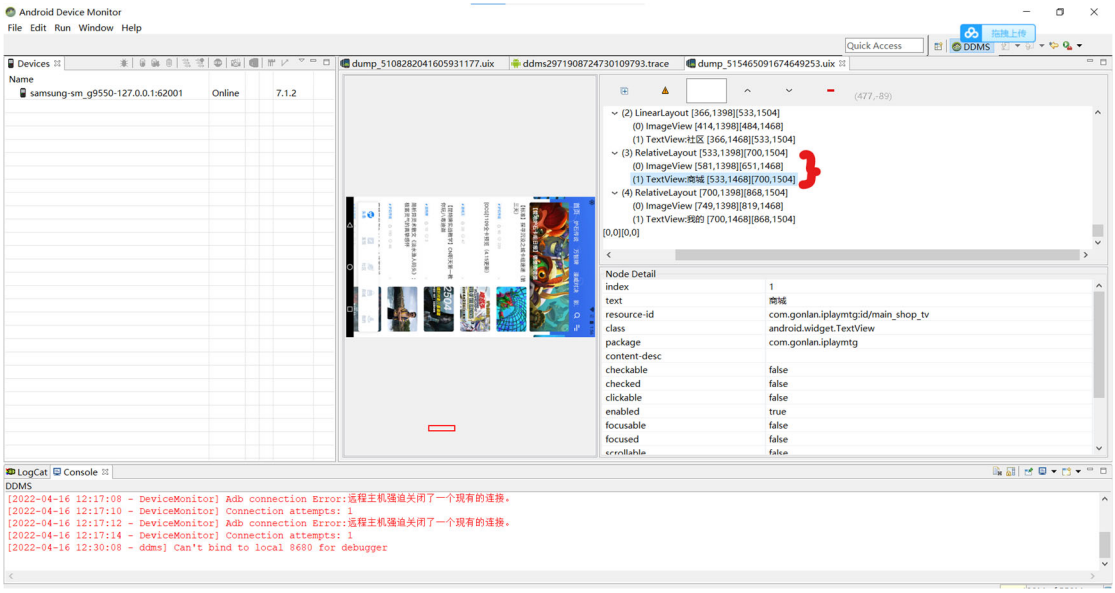
探寻沉没之城正式上线 通行证 竞技场及更多



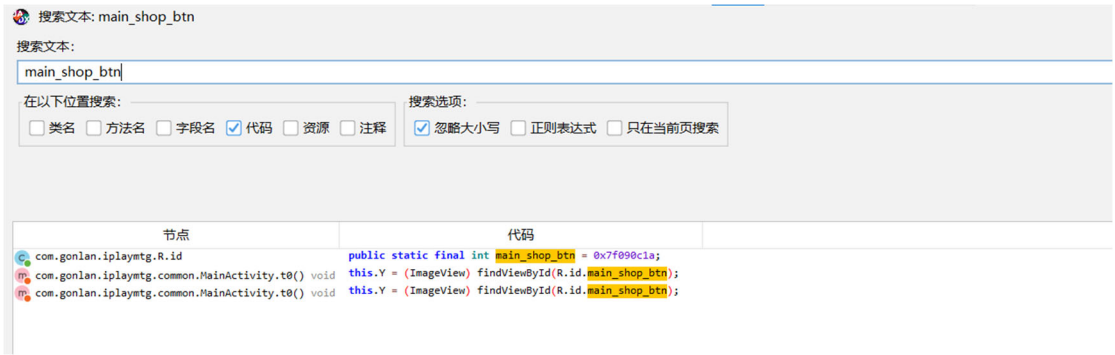
炉石传说 80 307

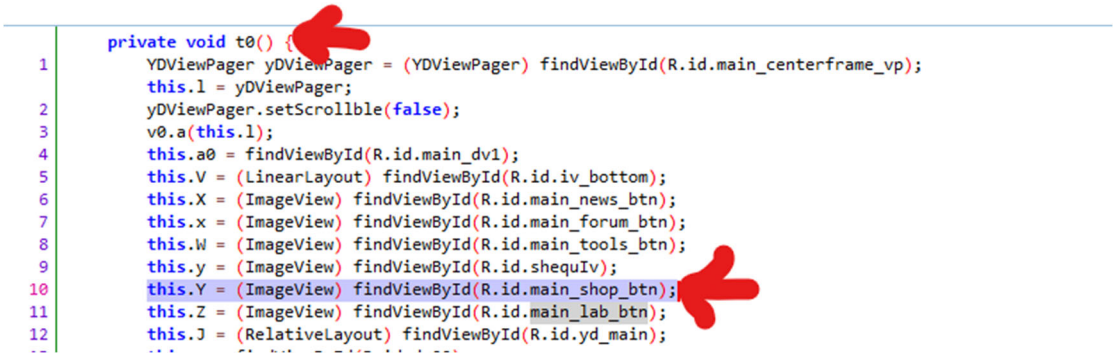
【周报君】一天一个样的高连胜卡组合集（04/12+13）

头条 发现 社区 商城 我的



2. 然后用 jadx 的字符串寻找方式找到这个控件所在 activity = "com.gonlan.iplaymtg.common.MainActivity"、method="t0"和对应的变量 Y



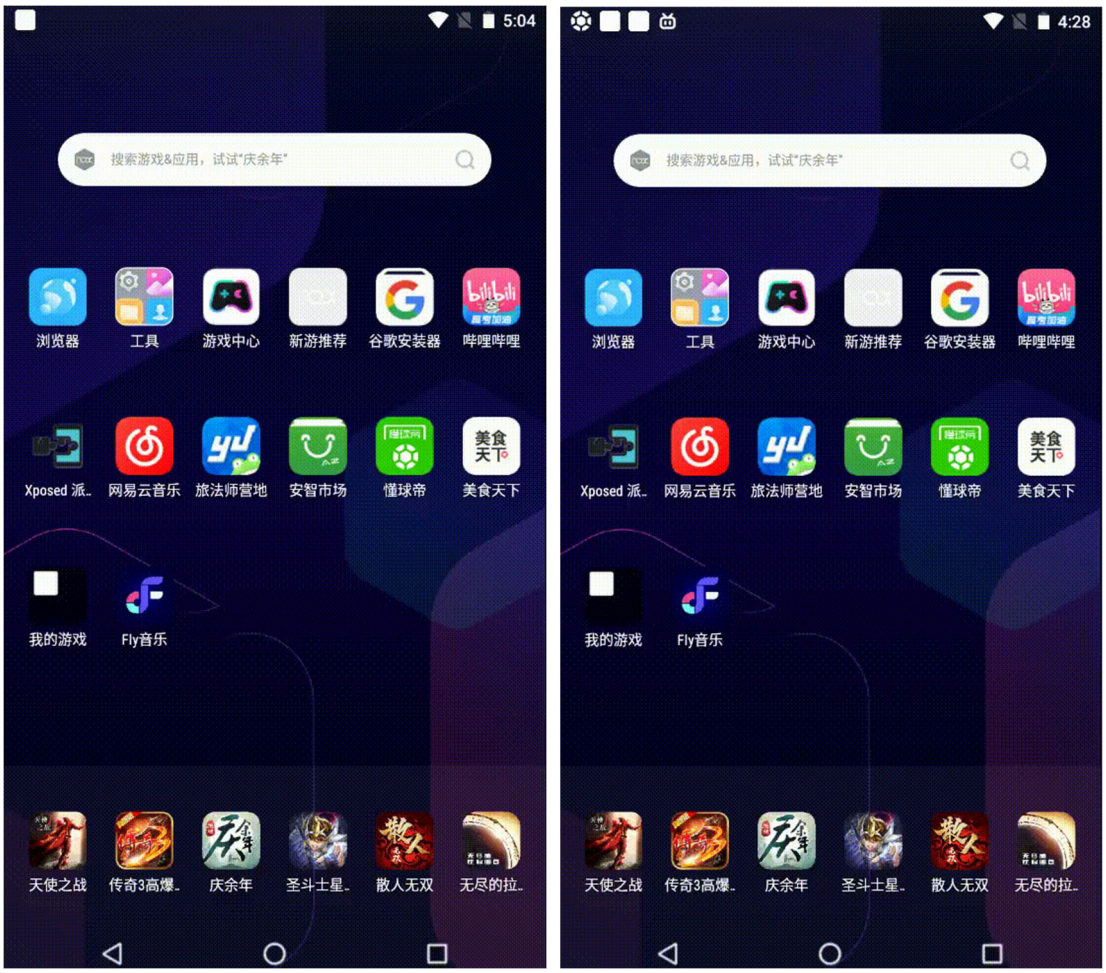


- **How you hooked the function**
  Introduce how you hook the target functions to realize your goal

1. 然后就是代码逻辑，先是判断是否是这个包，然后对于这个函数进行 hook，把这个图标的可见性设为看不见就行了。

```
protected void afterHookedMethod(MethodHookParam param) throws Throwable {
    Class clazz = param.thisObject.getClass();
    Field field = clazz.getDeclaredField( s: "Y");
    field.setAccessible(true);
    ImageView image = (ImageView) field.get(param.thisObject);
    if (image != null) {
        XposedBridge.log( text: "make the shop icon disappear!!!");
        image.setVisibility(View.GONE);
    }
```

2. 这个图标下面还有一个文本，也是同样的方式给他隐藏就成功了。
3. 结果对比展示（请注意底部的 5 个选择控件，结果删去了一个）：



- **Task4**
- **Introduction**
  Introduce the task briefly

  哔哩哔哩 app　希望提示同学们刷了多久 b 站，要好好学习

- **How you find the target function**
  Introduce how you reversed the target apk and located the target function you want to hook

1. 这个 app 主要的想法就是在进入 bilibili 的时刻开始就开始计时，并在前台的情况下不断计时。
2. 但是 xposed 不是重打包 app，无法在 activity 里面自动生成一个方法（也可能是我不太会），我就选择监控无意义的刷视频（就是啥都想看，不断刷的操作）
3. 所以第一目标就是找到主界面的 mainactivity，我找了一种使用 adb 直接寻找的方法，看到了 mainactivity

4. 那么在什么时候提示呢？我的选择是不打扰看视频，但是在视频退出回到主界面时会提示你已经看了多久了。也就是页面的 onStart()方法

```
@Override // com.bilibili.lib.ui.f, androidx.appcompat.app.e, androidx.fragment.app.FragmentActivity, com.bilib
public void onStart() {
    getDelegate().N(h.a(this));
    super.onStart();
    com.bilibili.lib.projection.h.a().q((ViewGroup) getWindow().getDecorView());
}

@Override // com.bilibili.lib.ui.f, androidx.appcompat.app.e, androidx.fragment.app.FragmentActivity, com.bilib
public void onStop() {
    super.onStop();
    if (UserProtocolHelper.l() && !com.bilibili.base.util.b.c()) {
        UserProtocolHelper.B(this);
    }
    com.bilibili.lib.projection.h.a().d();
}
```

- **How you hooked the function**

  Introduce how you hook the target functions to realize your goal

1. 那么第一步就是，一旦有 hook 到类名的"tv.danmaku.bili"启动得到 starttime = new Date()
2. 第二步是找到 tv.danmaku.bili.MainActivityV2 的 onStart()方法，获得当前 activity 并得到 endtime， 然后对于 endtime = new Date()
3. 然后通过判断当前 activity 是否在前台，如果在前台就可以进行消息提醒，否则将 starttime 重置。
3. 然后通过 endtime－starttime 的值进行 toast 类的消息提示，这里可以做很多方法，比如到指定时间就放出不同提示，我这里就做了个满多少时间做出不同的提示。当然因为展示需求，就用了 20s 和 30s 两个短时间。（这个时间包括你在寻找视频的时间）
4. 一旦到达 20s/30s，回到主界面就会显示对应的消息，提示你该干活了。
5. 结果


2:59
登录
俄乌最新局势
直播
推荐
热门
动画
影视
共同抗疫
上B站 看足总杯
曼城
VS
利物浦
切尔西
VS
水晶宫
主队助力官
主擂招募令
参与活动抽大奖，主擂招募等你来
上B站，看足总杯巅峰半决赛！
解压刀法
美味吴川松糕
16.3万
107
0:44
41.6万
336
1:03
诱人的吴川松糕，刀法好解压！
高校封校期间为缓解学生情绪，操场举办"校园版男生女生向前冲"
1万点赞
1万点赞
Vlog.
隔离day30
20.7万
105
4:59
上海某高校大学生
在宿舍隔离的一天
2.7万
18
2:27
首页
动态
会员购
我的


2:58
搜索游戏&应用，试试"庆余年"
浏览器
工具
游戏中心
新游推荐
谷歌安装器
哔哩哔哩
Xposed 派..
网易云音乐
旅法师营地
安智市场
懂球帝
美食天下
我的游戏
Fly音乐
天使之战
传奇3高爆..
庆余年
圣斗士星..
散人无双
无尽的拉..