2015阿里&看雪移动安全挑战赛-第一题

原创

scoronepion 于 2016-05-07 17:38:22 发布 1508 收藏 2

分类专栏： 安卓逆向 文章标签： 安卓逆向 移动安全 移动安全挑战赛 writeup

本文链接：https://blog.csdn.net/scoronepion/article/details/51339036

2015阿里&看雪移动安全挑战赛-第一题

题目传送门：AliCrackme

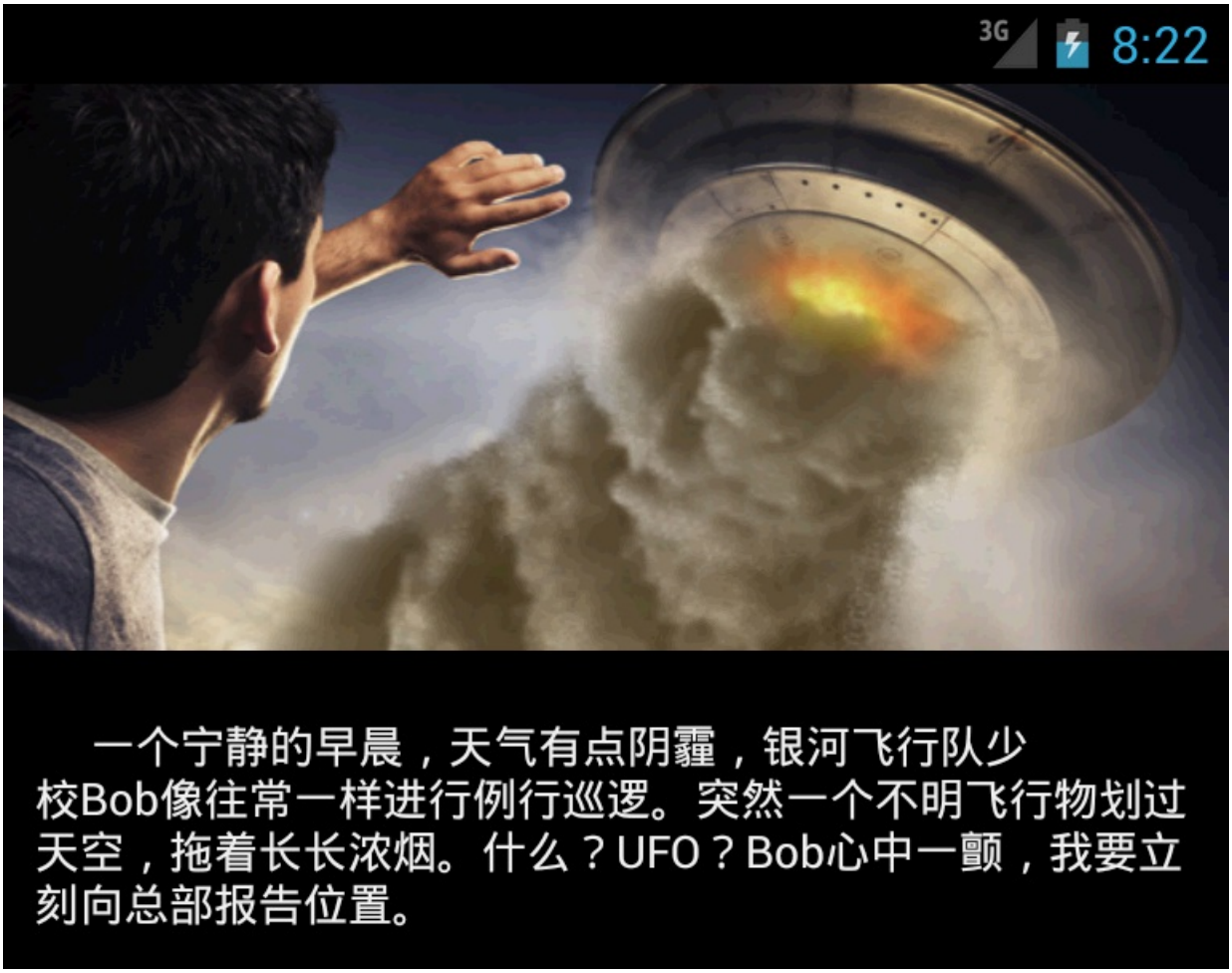
网上已经有很多writeup,我也是按照乌云上的2015移动安全挑战赛（阿里&看雪主办）全程回顾的基本思路来想的。但作为一个新手,就算照着教程来做也会踩到很多坑。所以我想把自己解题过程中遇到的一些细节问题跟大家分享一下。

文章中提到的环境配置是按照看雪论坛非虫的《Android软件安全与逆向分析》（以下简称《逆向》）配置的，这本书很棒，讲的很详细。在这里安利一波。

0x01

[...apk下载安装过程：略...]

apk安装好后，是这个样子的



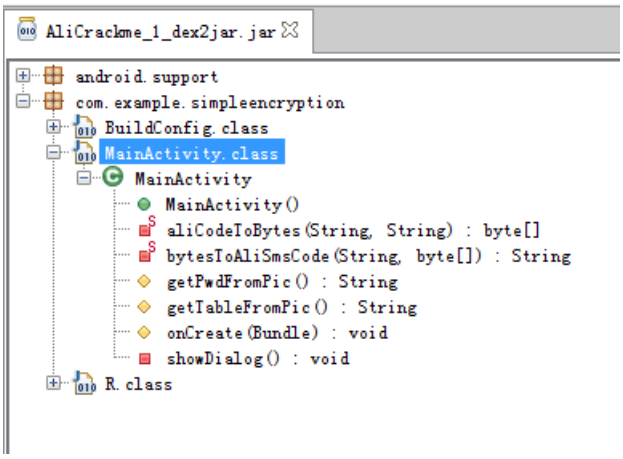
输入密码错误弹出提示，并要求继续。按照《逆向》里的思路，首先我尝试了用apktool将apk反编译成smali的做法。在strings.xml文件中查看是否有可疑字符串。

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="app_name">UFO</string>
    <string name="hello_world">Hello world!</string>
    <string name="action_settings">Settings</string>
    <string name="dialog_title">提示</string>
    <string name="dialog_error_tips">密码不对，请继续破解</string>
    <string name="dialog_good_tips">恭喜！！！破解成功！！！</string>
    <string name="dialog_ok">确定</string>
</resources>
```

结果没有发现。（ps:后来看了很多资料，觉得正确的做法应该是先将dex转jar看代码，然后根据代码来看这里面的东西。）

0x02

第二次尝试用dex2jar把classes.dex转成jar，然后用jd-gui查看。



发现两个方法：`getPwdFromPic()`和`getTableFromPic()`。它们是这样被调用的：

```
String str1 = localEditText.getText().toString();
String str2 = MainActivity.this.getTableFromPic();
String str3 = MainActivity.this.getPwdFromPic();
Log.i("lil", "table:" + str2);
Log.i("lil", "pw:" + str3);
String str4 = "";
try
{
  str4 = MainActivity.bytesToAliSmsCode(str2, str1.getBytes("utf-8"));
  Log.i("lil", "enPassword:" + str4);
  if ((str3 != null) && (!str3.equals("")) && (str3.equals(str4)))
  {
    MainActivity.this.showDialog();
    return;
  }
}
```

这意味着每次输入的时候，程序都会调用日志输出table(映射表)、pw(密码)和enPassword(输入)。那么我们可以在Eclipse中打开LogCat查看它的输出日志。（如何打开LogCat请自行搜索）
比如，我们输入“123”，它的输出了这些东西：

```
com.example.simpleen...  lil  table:一乙二十丁厂七卜人入八九几儿了力乃刀又三于干亏士工土才寸下大丈与万上小口巾山...
                              井开夫天无元专云扎艺木五支厅不太犬区历尤友匹车巨牙屯比互切瓦止少日中冈贝内水见午牛...
                              文六方火为斗忆订计户认心尺引丑巴孔队办以允予劝双书幻玉刊示末未击打巧正扑扒功扔去甘...
                              只央兄叼叫另叨叹四生失禾丘付仗代仙们仪白仔他斥瓜乎丛令用甩印乐
com.example.simpleen...  lil  pw:义弓么丸广之
com.example.simpleen...  lil  enPassword:么广亡
```

输入的`123`变成了`么广亡`，这表明程序内部的映射表将数字转换成了汉字，那么根据pw的输出`义弓么丸广之`，我们可以逆推出它的真实密码为：`581026`
输入`581026`，破解成功

0x03

在乌云上，关于这道题的映射表是这样说的

> 获得正确注册码的代码逻辑为： 1. 从logo.png这张图片的偏移89473处，读取一个映射表，768字节编码成UTF-8，即256个中文表 2. 从偏移91265处读取18个字节编码的UTF-8（即6个中文字符）为最终比较的密码。然后通过输入的字符的转换，转换规则就是ASCII字符编码，去比较是否和最终密码相等。

一开始的时候我以为需要从图片中找出密码来，觉得很头疼。后来发现代码中存在日志输出，倒是直接把答案输出了。