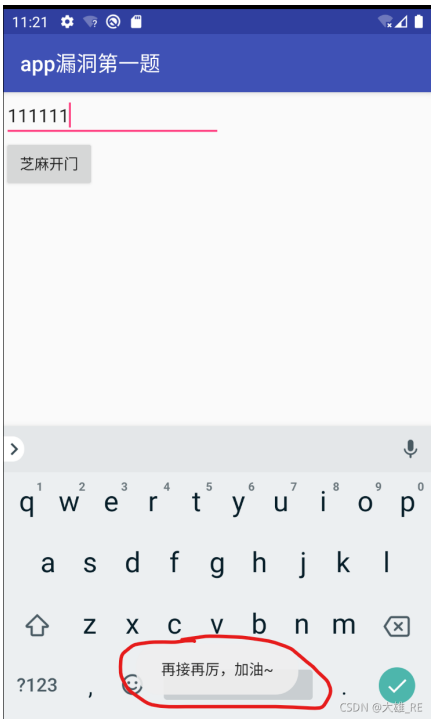
XCTF_MOBILE2_app1

原创

大雄_RE 于 2021-11-17 20:37:40 发布
分类专栏： CTF 文章标签： android 逆向 ctf

题目没有多余提示，直接下载apk。

拖到android模拟器中运行，随便输入一个字符串，点击按钮，弹框“再接再厉，加油~”，如下图：



考虑先反编译看看：

- 修改后缀名为zip
- 解压
- 用dex2jar将解压得到的classes.dex反编译为jar

```
PS C:\Users\leo\Desktop\dex2jar-2.0> .\d2j-dex2jar.bat C:\Users\leo\Desktop\b9af8dfef6b749d2819ef5be16c26a0d\classes.dex

dex2jar C:\Users\leo\Desktop\b9af8dfef6b749d2819ef5be16c26a0d\classes.dex -> .\classes-dex2jar.jar
PS C:\Users\leo\Desktop\dex2jar-2.0>
```

将jar拖到jd-gui中，直接看MainActivity类的代码，在函数成员onCreate中能看到刚才弹框的字符串：

```
String str2 = packageInfo.versionName;
int j = packageInfo.versionCode;
for (int i = 0;; i++) {
  if (i < str1.length() && i < str2.length()) {
    if (str1.charAt(i) != (str2.charAt(i) ^ j)) {
      Toast.makeText((Context)MainActivity.this, "再接再厉，加油~", 1).show();
      return;
    }
  } else {
    if (str1.length() == str2.length()) {
      Toast.makeText((Context)MainActivity.this, "恭喜开启闯关之门！", 1).show();
      return;
    }
    Toast.makeText((Context)MainActivity.this, "年轻人不要耍小聪明噢", 1).show();
  }
}
```


可见这里就是关键代码了。

这里的逻辑很清楚，输入的字符串要满足两个条件：

1. 输入字符串长度等于packageInfo.versionName字符串的长度
2. 输入字符串的每个字符等于packageInfo.versionName字符串的对应字符异或packageInfo.versionCode

异或是可逆运算，也就是将packageInfo.versionName字符串的每个字符异或上packageInfo.versionCode就是我们要输入的内容。

百度一下如何获取apk的versionName和versionCode，得知Android SDK的build-tools中有一个工具aapt可以得到这两个信息：

```
D:\Android\android-sdk\build-tools\30.0.2>aapt dump badging C:\Users\Leo\Desktop\b9af8dfef6b749d2819ef5be16c26a0d.apk
package: name='com.example.yaphetshan.tencentgreat' versionCode='15' versionName='X<cP[?PHNB<P?aj' platformBuildVersionName='7.1.1'
sdkVersion:'19'
targetSdkVersion:'25'
```

versionName为：'X<cP[?PHNB<P?aj'

versionCode为：15

编写python脚本，给字符串'X<cP[?PHNB<P?aj'异或15：

```
version_code = 15
version_name = 'X<cP[?PHNB<P?aj'
flag = ''
for c in version_name:
 flag += chr(ord(c)^version_code)
print(flag)
```

得到结果：

W3l_T0_GAM3_0ne

欢迎关注我的微博：大雄_RE。专注软件逆向，分享最新的好文章、好工具，追踪行业大佬的研究成果。