0ctf – mobile – boomshakalaka writeup

转载

weixin_30539835 于 2016-03-14 19:06:00 发布 241 收藏
文章标签： java 移动开发
原文链接：http://www.cnblogs.com/dliv3/p/5276782.html

作为一个web狗，一道web都没做出来Orz。。。做出来一道apk，纪念一下在ctf中做出的第一道apk。。。

首先在模拟器或者真机中安装一下apk看到是一个cocos2dx的打飞机游戏

根据题目提示，要打游戏打到最高分就会得到flag，首先拉到Jeb中反编译一下，在manifest文件中看到入口类为FirstTest类

```
import android.os.Bundle;
import org.cocos2dx.lib.Cocos2dxActivity;
import org.cocos2dx.lib.Cocos2dxGLSurfaceView;

public class FirstTest extends Cocos2dxActivity {
    static {
        System.loadLibrary("cocos2dcpp");
    }

    public FirstTest() {
        super();
    }

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        new a(((Context)this), "flag").d("YmF6aW5nYWFhYQ==");
        new a(((Context)this), "Cocos2dxPrefsFile").d("NO");
    }

    public Cocos2dxGLSurfaceView onCreateView() {
        Cocos2dxGLSurfaceView v0 = new Cocos2dxGLSurfaceView(((Context)this));
        new a(((Context)this), "Cocos2dxPrefsFile").d("MG");
        v0.setEGLConfigChooser(5, 6, 5, 0, 16, 8);
        return v0;
    }
}
```

FirstTest类的onCreate方法调用了a类对flag和Cocos2dxPrefsFile字符串做了某些操作。

下面看一下a类的实现

```
package com.example.plane;

import android.content.Context;
import android.content.SharedPreferences;

public class a {
    private SharedPreferences editor;

    public a(Context arg1, String arg2) {
        super();
        this.editor = null;
        this.editor = arg1.getSharedPreferences(arg2, 0);
    }

    public void b() {
        this.editor.edit().putString("DATA", "").commit();
    }

    public String c() {
        return this.editor.getString("DATA", "");
    }

    public void d(String arg1) {
        this.editor.edit().putString("DATA", String.valueOf(String.valueOf(this.c())) + arg1).commit();
    }
}
```

a中使用了SharePreferences并向其中写入一些数据，sharePreferences是android的一种数据存储机制，它会在/data/data/com.example.plane/下生成一个xml文件，并将数据存储在其中。

随便玩一下游戏之后，查看/data/data/com.example.plane/Cocos2dxPrefsFile.xml的内容：

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="DATA">MGN0ZntDMGNvUzJkX0FuRHJvMWdz99ZntDMGNvUzJkX0FuRHJvMWMGN0ZntDMGNvUzJkX0FuRHJvMWdz99ZntDMGNvUzJkX0FuRHJvMWRzdz99</string>
    <int name="HighestScore" value="4700" />
    <boolean name="isHaveSaveFileXml" value="true" />
</map>
```

里面有一段base64的字符串，解码之后看到了0ctf{xxx的字符串，但是字符串并不完整，猜测**flag是动态生成的**，多次运行游戏并且获取不同分数后发现该文件中的base64长度随分数高低有所变化，所以flag和游戏分数高低有关

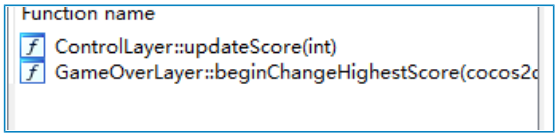
```
0ctf{C0coS2d_AnDro1gs÷Ög´3ACK6õ3&EôSYNäG&óSYN0ctf{C0coS2d_AnDro1gs÷Ög´3ACK6õ3&EôSYNäG&óSYNG7s÷
```

在java层的代码中仅发现FirstTest类中有对SharePreferences的操作。

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    new a(((Context)this), "flag").d("YmF6aW5nYWFhYQ==");
    new a(((Context)this), "Cocos2dxPrefsFile").d("N0");
}

public Cocos2dxGLSurfaceView onCreateView() {
    Cocos2dxGLSurfaceView v0 = new Cocos2dxGLSurfaceView(((Context)this));
    new a(((Context)this), "Cocos2dxPrefsFile").d("MG");
    v0.setEGLConfigChooser(5, 6, 5, 0, 16, 8);
    return v0;
}
```

所以主要操作应该在so中，使用IDA对so进行反编译，发现so中两个与分数有关的函数



看了一下updateScore的代码，感觉已经很接近结果了，（可以动态调试一下以确定分数改变时会调用这个函数），这个程序生成flag的大概流程是，当游戏分数达到一定的分数段，就会输出一部分base64编码后的字符串。

```
else if ( v3 == (const char *)600 )
{
  v8 = cocos2d::CCUserDefault::sharedUserDefault(v5);
  std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v23, &v20, "Rf");
  cocos2d::CCUserDefault::setStringForKey(v8, &v34, &v23);
  v7 = &v23;
}
else if ( v3 == (const char *)700 )
{
  v9 = cocos2d::CCUserDefault::sharedUserDefault(v5);
  std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v24, &v20, "Rz");
  cocos2d::CCUserDefault::setStringForKey(v9, &v34, &v24);
  v7 = &v24;
}
else if ( v3 == (const char *)3000 )
{
  v10 = cocos2d::CCUserDefault::sharedUserDefault(v5);
  std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v25, &v20, "Bt");
  cocos2d::CCUserDefault::setStringForKey(v10, &v34, &v25);
  v7 = &v25;
}
else if ( v3 == (const char *)5600 )
{
  v11 = cocos2d::CCUserDefault::sharedUserDefault(v5);
  std::operator+<char,std::char_traits<char>,std::allocator<char>>(&v26, &v20, "RV");
  cocos2d::CCUserDefault::setStringForKey(v11, &v34, &v26);
  v7 = &v26;
}
```

所以我们只需要按分数的高低顺序将这些base64的字符串拼起来就是flag

之前我们在xml文件中的到的字符串是

0ctf{C0coS2d_AnDro1

在updateScore中得到的base64字符串为：MWRfRzBtRV9Zb1VfS24w

解码后: **1d_G0mE_YoU_Kn0**

卧槽。。。flag不是完整的怎么办!!!

肯定还有其他调用SharePreferences的地方！写文件的API是一样的，使用IDA的交叉引用找到其他调用API的地方，然后得到完整的flag

0ctf{C0coS2d_AnDro1d_G0mE_YoU_Kn0w?}

转载于:https://www.cnblogs.com/dliv3/p/5276782.html