XCTF 攻防世界 app2

原创

pipixia233333 于 2019-04-24 10:25:14 发布 1674 收藏 1
分类专栏： 逆向之旅

本文链接：https://blog.csdn.net/qq_41071646/article/details/89487326

这个题 所实话 好坑爹啊

首先说一下　怎么处理so里面的 (*(*a1 + 680)) 这个讨厌的东西吧

只需要对着a 按下y 键 然后输入 JNIEnv* 就可　效果如下

IDA View-A | Pseudocode-C | Pseudocode-B | Pseudocode-A | Hex View-1 | Stru

```
int __cdecl doRawData(JNIEnv *a1, int a2, int a3, int a4)
{
  char *v4; // esi
  const char *v5; // ST10_4
  int result; // eax
  char *v7; // esi
  jstring (*v8)(JNIEnv *, const jchar *, jsize); // ST10_4
  size_t v9; // eax
  char key[16]; // [esp+4h] [ebp-28h]
  unsigned int v11; // [esp+18h] [ebp-14h]

  v11 = __readgsdword(0x14u);
  if ( checkSignature(a1, a2, a3) == 1 )
  {
    strcpy(key, "thisisatestkey==");
    v4 = (*a1)->GetStringUTFChars(a1, a4, 0);
    v5 = AES_128_ECB_PKCS5Padding_Encrypt(v4, key);
    (*a1)->ReleaseStringUTFChars(a1, a4, v4);
    result = (*a1)->NewStringUTF(a1, v5);
  }
  else
  {
    v7 = UNSIGNATURE[0];
    v8 = (*a1)->NewString;
    v9 = strlen(UNSIGNATURE[0]);
    result = v8(a1, v7, v9);
  }
  return result;
}
```


看的出来 效果还是很不错的

然后这里可以直接看的出来加密类型　然后 java 层的代码 很好理解

```
    {
      Toast.makeText(this, "不能为空", 1).show();
    }
    else
    {
      String str1 = this.c.getText().toString();
      String str2 = this.d.getText().toString();
      Log.e("test", str1 + " test2 = " + str2);
      paramView = new Intent(this, SecondActivity.class);
      paramView.putExtra("ili", str1);
      paramView.putExtra("lil", str2);
      startActivity(paramView);
    }
  }
}

protected void onCreate(Bundle paramBundle)
```

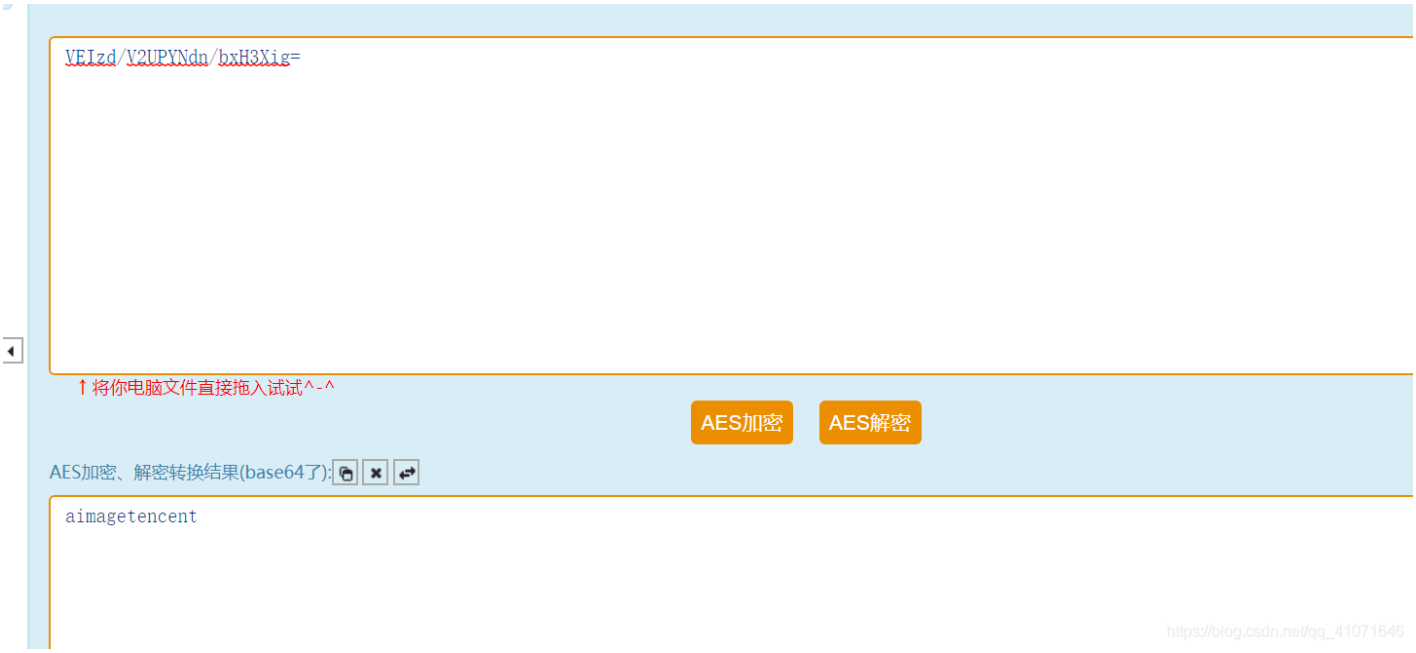

这里是 把我们输入的两个字符串 传播给SecondActivity 这个活动 然后 并跳转到 SecondActivity 活动

然后发现Encryto.doRawData(this, paramBundle + str).equals("VElzd/V2UPYNdn/bxH3Xig==")

doRawData 是so 文件库里面倒进去的 然后我只要 把 so 文件 里面的函数分析出来就好

然后我们发现了 so里面就是一个AES_128_ECB_PKCS5Padding_Encrypt 加密 而且 key 是 thisisatestkey==

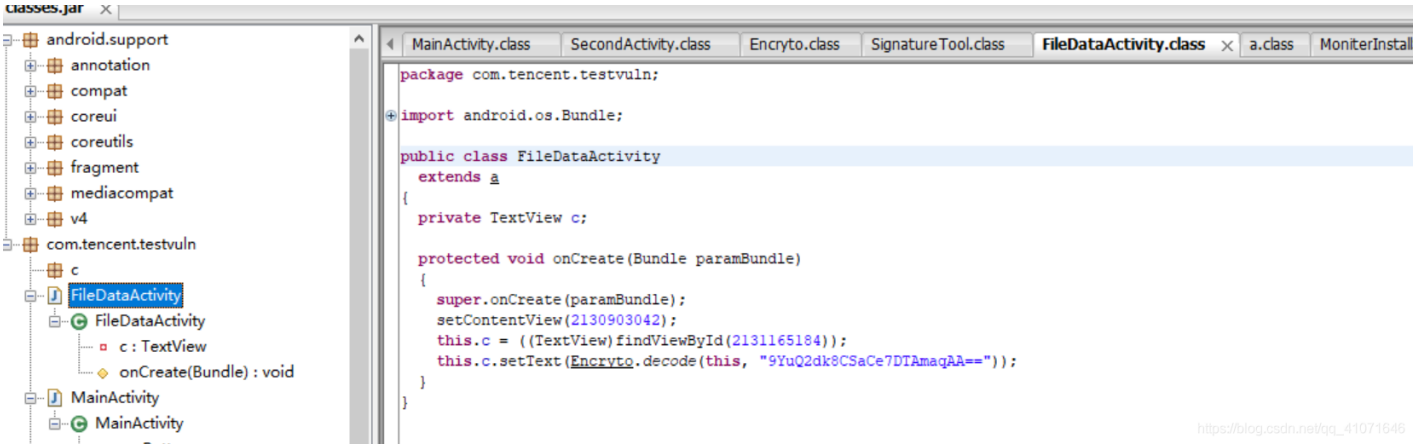
我们只需要解密一下就好



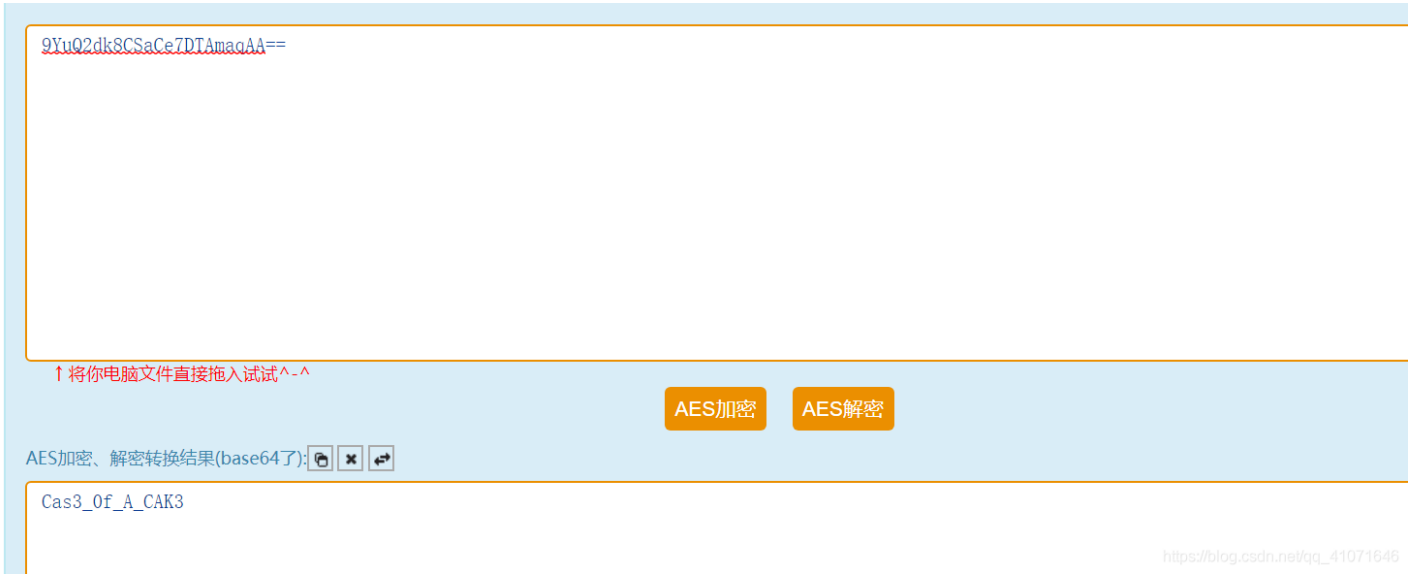
你以为这里结束了 nonono 你会发现 flag 交上去 不对。。。。

我仔细的往后检查了一下 发现并没有哪里不对。

后来 随便翻了翻 发现了这里



我们 暂且试试这个字符串



发现这个字符串 是对的。。。。。

这个题 有点坑啊。