

BUUCTF Reverse(helloworld)

原创

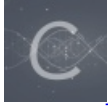
sherlockjobs 于 2020-12-18 10:50:22 发布 698 收藏 2

分类专栏: [Reverse](#) [CTF](#) [网络安全](#) 文章标签: [逆向](#) [安卓逆向](#) [CTF](#) [Reverse](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43456810/article/details/111354853

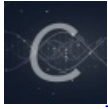
版权



[Reverse](#) 同时被 3 个专栏收录

6 篇文章 0 订阅

订阅专栏



[CTF](#)

19 篇文章 0 订阅

订阅专栏



[网络安全](#)

27 篇文章 0 订阅

订阅专栏

BUUCTF Reverse(helloworld)

题目附件下载下来之后, 是.apk后缀, 所以可能是安卓逆向。

这里我用的工具是Android Killer, 下载地址: https://xiazai.xiazaiba.com/Soft/A/AndroidKiller_1.3.1_XiaZaiBa.zip
filename=AndroidKiller_1.3.1_XiaZaiBa.zip

个人觉得, 此工具使用起来比其他的简单一些。

用Android Killer打开文件之后, 查看MainActivity, 即可看到正确的flag

```
25  invoke-super {p0, p1}, Landroid/support/v7/app/ActionBarActivity;->onCreate(Landroid/os/Bundl
26
27  .line 14
28  const v3, 0x7f030018
29
30  invoke-virtual {p0, v3}, Lcom/example/helloworld/MainActivity;->setContentView(I)V
31
32  .line 15
33  const-string v0, "flag{7631a988259a00816deda84afb29430a}"
34
35  .line 16
36  .local v0, "a":Ljava/lang/String;
37  const-string v1, "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
38
```