crash

发表于 2021-01-07 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， HarmonyOS和HMS专场， Reverse
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | HarmonyOS和HMS专场 | Reverse | crash

点击此处获得更好的阅读体验

WriteUp来源

来自Venom战队官方发布

题目描述

> *crash文件逆向*

题目考点

- *函数符号表恢复*

解题思路

题目给的是一个coredump文件，从coredump文件中提取出binary文件，并恢复出库函数符号，最终得到的文件用ida打开后保存得到test.idb，即可开始逆向

把md5字符串解完得到字符串`bo&tn&o#~{c|vut.yb&y|''s.v|gg ``，对其进行异或0x17得到字符串ux1cy1x4iltkahbc9nu1nk00d9akpp7w`，盲猜这是flag

Flag

```
1 flag{ux1cy1x4iltkahbc9nu1nk00d9akpp7w}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/HarmonyOS和HMS专场/Reverse/oDoXBDig52yVtJtCnEeMzo.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Reverse # XCTF高校网络安全专题挑战赛 # HarmonyOS和HMS专场
puzzle
华为HCIE的第一课