

XCTF insanity

原创

这个不是名 于 2020-03-08 13:45:41 发布 806 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/qq_19635147/article/details/104731695

版权

<https://adworld.xctf.org.cn/task/answer?type=reverse&number=4&grade=0&id=5079&page=1>

IDA打开看伪代码

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     unsigned int v3; // eax
4     unsigned int v4; // eax
5
6     puts("Reticulating splines, please wait..");
7     sleep(5u);
8     v3 = time(0);
9     srand(v3);
10    v4 = rand();
11    puts((&strs)[v4 % 0xA]);
12    return 0;
13 }
```

https://blog.csdn.net/qq_19635147

先置随机数再%0xA输出strs里面的一个字符串，双击strs看看里面都有什么

```
.data:080499C0 strs          dd offset a9447ThisIsAFla |
.data:080499C0                ; DATA XREF: main+4Dtr
.data:080499C0                ; "9447{This_is_a_flag}"
.data:080499C4                dd offset aCongratsYouHac ; "Congrats, you hacked me!\n$"
.data:080499C8                dd offset aRmRfPermission ; "rm -rf / : Permission denied"
.data:080499CC                dd offset aDefineYouMassi ; "#define YOU \"massive failure\""
.data:080499D0                dd offset aIfYouRePretend ; "If you're pretending to suck, you just "...
.data:080499D4                dd offset aThereArenTEnou ; "There aren't enough bits in my memory t"...
.data:080499D8                dd offset aYourAbilityToH ; "Your ability to hack is about as good a"...
.data:080499DC                dd offset aHaveYouConside ; "Have you considered becoming a vacuum c"...
.data:080499E0                dd offset aIVeGotAGoodFee ; "I've got a good feeling about this one."...
.data:080499E4                dd offset aKnockKnockWhoS ; "Knock knock, \nwho's there?\nUDP.\nUDP"
.data:080499E4 _data          ends
```

啊，里面有一个flag