XCTF-Reverse：insanity

原创

Waff1ε 于 2020-11-28 20:18:51 发布 48 收藏

分类专栏： # CTF&Reverse

本文链接：https://blog.csdn.net/Waffle666/article/details/110291163

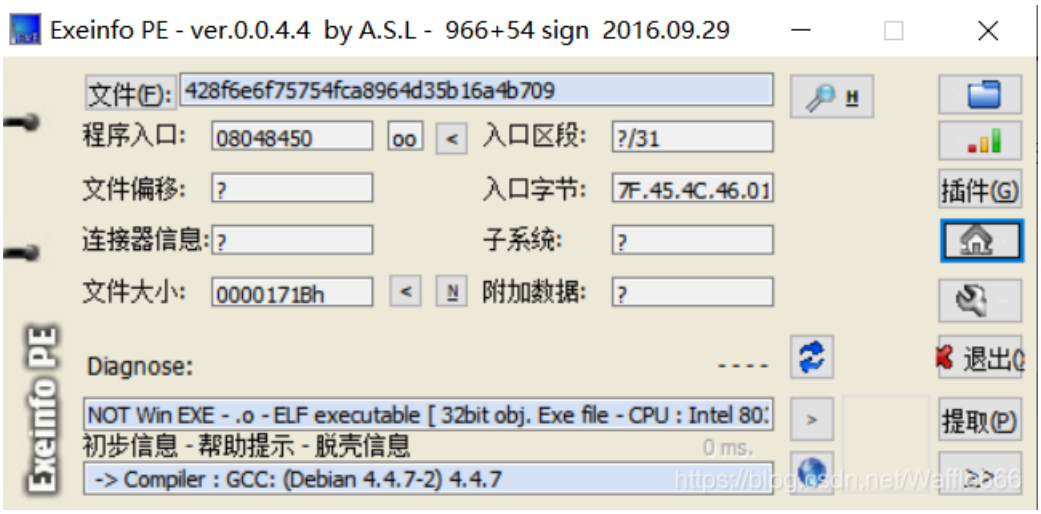
CTF&Reverse 专栏收录该内容

20 篇文章 0 订阅

订阅专栏

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

查壳：



发现是ELF文件格式
在Linux下运行：

得知信息：ELF 32-bit

直接拖进ida32

查看main函数：F5查看伪C代码

IDA View-A | Pseudocode-A | Strings window | Hex View-1 | Structur

```
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 }
```


发现

puts(&strs)，是取这个字符串输出，双击strs进入

```
.data:080499C0 ; char *strs
.data:080499C0 strs            dd offset a9447ThisIsAFla
.data:080499C0                                         ; DATA XREF: main+4D↑r
.data:080499C0                                         ; "9447{This_is_a_flag}"
.data:080499C4                 dd offset aCongratsYo...c ; "Congrats, you hacked me!\n$ "
.data:080499C8                 dd offset aRmRfP...mission ; "rm -rf / : Permission denied"
.data:080499CC                 dd offset a...fineYouMassi ; "#define YOU \"massive failure\""
```

发现flag

9447{This_is_a_flag}