攻防世界--Shuffle

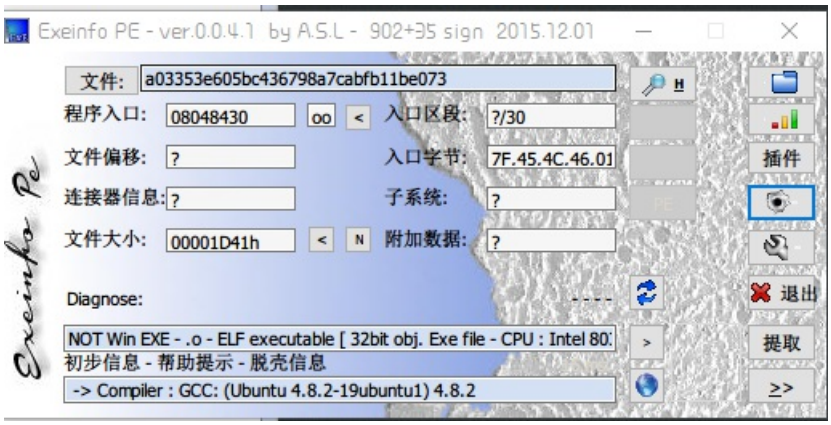
原创

Hk_Mayfly 于 2019-09-09 23:28:00 发布 250 收藏

本文链接：https://blog.csdn.net/qq_39542714/article/details/106835363

测试文件：https://adworld.xctf.org.cn/media/task/attachments/a03353e605bc436798a7cabfb11be073

1.准备



获得信息

1. 32位文件

2.IDA打开

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  time_t v3; // ebx
  __pid_t v4; // eax
  unsigned int v5; // ST18_4
  unsigned int v6; // ST1C_4
  char v7; // ST20_1
  signed int i; // [esp+14h] [ebp-44h]
  char s; // [esp+24h] [ebp-34h]
  char v11; // [esp+25h] [ebp-33h]
  char v12; // [esp+26h] [ebp-32h]
  char v13; // [esp+27h] [ebp-31h]
  char v14; // [esp+28h] [ebp-30h]
  char v15; // [esp+29h] [ebp-2Fh]
  char v16; // [esp+2Ah] [ebp-2Eh]
  char v17; // [esp+2Bh] [ebp-2Dh]
  char v18; // [esp+2Ch] [ebp-2Ch]
  char v19; // [esp+2Dh] [ebp-2Bh]
  char v20; // [esp+2Eh] [ebp-2Ah]
  char v21; // [esp+2Fh] [ebp-29h]
  char v22; // [esp+30h] [ebp-28h]
  char v23; // [esp+31h] [ebp-27h]
```

```
char v24; // [esp+32h] [ebp-26h]
char v25; // [esp+33h] [ebp-25h]
char v26; // [esp+34h] [ebp-24h]
char v27; // [esp+35h] [ebp-23h]
char v28; // [esp+36h] [ebp-22h]
char v29; // [esp+37h] [ebp-21h]
char v30; // [esp+38h] [ebp-20h]
char v31; // [esp+39h] [ebp-1Fh]
char v32; // [esp+3Ah] [ebp-1Eh]
char v33; // [esp+3Bh] [ebp-1Dh]
char v34; // [esp+3Ch] [ebp-1Ch]
char v35; // [esp+3Dh] [ebp-1Bh]
char v36; // [esp+3Eh] [ebp-1Ah]
char v37; // [esp+3Fh] [ebp-19h]
char v38; // [esp+40h] [ebp-18h]
char v39; // [esp+41h] [ebp-17h]
char v40; // [esp+42h] [ebp-16h]
char v41; // [esp+43h] [ebp-15h]
char v42; // [esp+44h] [ebp-14h]
char v43; // [esp+45h] [ebp-13h]
char v44; // [esp+46h] [ebp-12h]
char v45; // [esp+47h] [ebp-11h]
char v46; // [esp+48h] [ebp-10h]
char v47; // [esp+49h] [ebp-Fh]
char v48; // [esp+4Ah] [ebp-Eh]
char v49; // [esp+4Bh] [ebp-Dh]
unsigned int v50; // [esp+4Ch] [ebp-Ch]

v50 = __readgsdword(0x14u);
s = 83;
v11 = 'E';
v12 = 'C';
v13 = 'C';
v14 = 'O';
v15 = 'N';
v16 = '{';
v17 = 'W';
v18 = 'e';
v19 = 'l';
v20 = 'c';
v21 = 'o';
v22 = 'm';
v23 = 'e';
v24 = ' ';
v25 = 't';
v26 = 'o';
v27 = ' ';
v28 = 't';
v29 = 'h';
v30 = 'e';
v31 = ' ';
v32 = 'S';
v33 = 'E';
v34 = 'C';
v35 = 'C';
v36 = 'O';
v37 = 'N';
v38 = ' ';
v39 = '2';
v40 = '0';
```

```
  v41 = '1';
  v42 = '4';
  v43 = ' ';
  v44 = 'C';
  v45 = 'T';
  v46 = 'F';
  v47 = '!';
  v48 = '}';
  v49 = '\0';
  v3 = time(0);
  v4 = getpid();
  srand(v3 + v4);
  for ( i = 0; i <= 99; ++i )
  {
    v5 = rand() % 0x28u;
    v6 = rand() % 0x28u;
    v7 = *(&s + v5);
    *(&s + v5) = *(&s + v6);
    *(&s + v6) = v7;
  }
  puts(&s);
  return 0;
}
```

3.get flag!

> ECCON{Welcome to the SECCON 2014 CTF!}