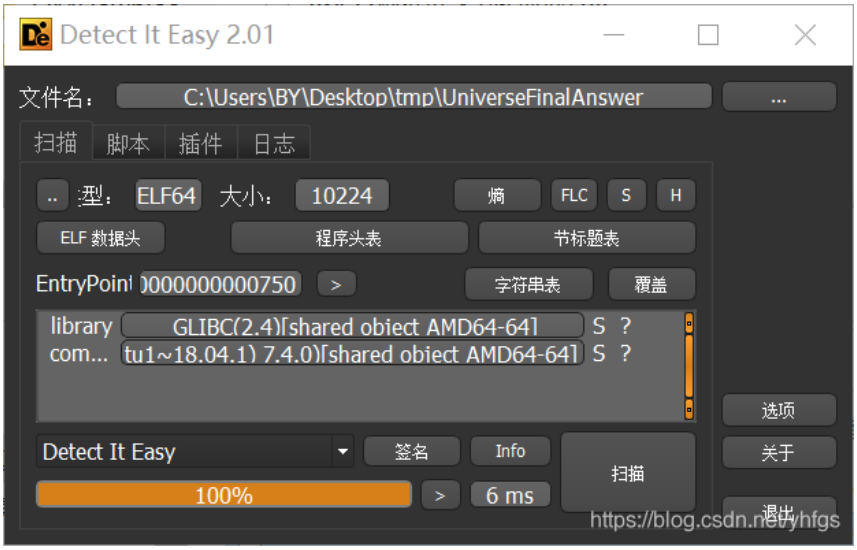
# buuctf——（ACTF新生赛2020）Universe_final_answer

原创

re3sry 于 2021-06-10 20:38:35 发布 62 收藏


1.查壳。

无壳，64位文件。




2.IDA反编译。

```
5  unsigned __int64 v6; // [rsp+88h] [rbp-20h]
6
7  v6 = __readfsqword(0x28u);
8  __printf_chk(1LL, "Please give me the key string:", a3);
9  scanf("%s", v5);
10 if ( sub_860(v5) )
11 {
12   sub_C50(v5, v4);
13   __printf_chk(1LL, "Judgement pass! flag is actf{%s_%s}\n", v5);
14 }
15 else
16 {
17   puts("False key!");
18 }
19 return 0LL;
20}
```



进入sub_860函数

分析代码可知是十元一次方程组，并且a[1]与a[0],a[5]和a[6]互换。

```
  v2 = *a1;
  v3 = a1[2];
  v4 = a1[3];
  v5 = a1[4];
  v6 = a1[6];
  v7 = a1[5];
  v8 = a1[7];
  v9 = a1[8];
  result = 0;
  if ( -85 * v9 + 58 * v8 + 97 * v6 + v7 + -45 * v5 + 84 * v4 + 95 * v2 - 20 * v1 + 12 * v3 == 12613 )
  {
    v11 = a1[9];
    if ( 30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -41 * v3 + -86 * v1 - 15 * v2 - 30 * v8 == -54400
      && -103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 * v2 + 31 * v5 - (v6 << 6) - 120 * v9 == -10283
      && 71 * v6 + (v7 << 7) + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v4 - 119 * v8 + 48 * v9 - 16 * v11 == 22855
      && 5 * v11 + 23 * v9 + 1int v8; // er8 v6 + 99 * v7 + -117 * v5 + -69 * v3 + 22 * v1 - 98 * v2 + 10 * v4 == -2944
      && -54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 * v5 - 60 * v7 + 95 * v6 + 100 * v9 == -2222
      && -83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 * v5 + 16 * v6 + 77 * v8 - 63 * v9 == -13258
      && 81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 * v4 + 60 * v3 + -85 * v2 + 80 * v1 == -1559
      && 101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 * v3 + -28 * v1 + 18 * v2 - v8 == 6308 )
    {
      result = 99 * v11 + -28 * v9 + 5 * v8 + 93 * v6 + -18 * v7 + -127 * v5 + 6 * v4 + -9 * v3 + -93 * v1 + 58 * v2 == -1697;
    }
  }
  return result;
}
```



写脚本：

```
from sympy import *

v1=Symbol('v1')
v2=Symbol('v2')
v3=Symbol('v3')
v4=Symbol('v4')
v5=Symbol('v5')
v6=Symbol('v6')
v7=Symbol('v7')
v8=Symbol('v8')
v9=Symbol('v9')
v11=Symbol('v11')

f1=-85 * v9 + 58 * v8 + 97 * v6 + v7 + -45 * v5 + 84 * v4 + 95 * v2 - 20 * v1 + 12 * v3 - 12613
f2=30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -41 * v3 + -86 * v1 - 15 * v2 - 30 * v8 + 54400
f3=-103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 * v2 + 31 * v5 - v6 * 64 - 120 * v9 + 10283
f4=71 * v6 + v7 * 128 + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v4 - 119 * v8 + 48 * v9 - 16 * v11 - 22855
f5=5 * v11 + 23 * v9 + 122 * v8 + -19 * v6 + 99 * v7 + -117 * v5 + -69 * v3 + 22 * v1 - 98 * v2 + 10 * v4 + 2944
f6=-54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 * v5 - 60 * v7 + 95 * v6 + 100 * v9 + 2222
f7=-83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 * v5 + 16 * v6 + 77 * v8 - 63 * v9 + 13258
f8=81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 * v4 + 60 * v3 + -85 * v2 + 80 * v1 + 1559
f9=101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 * v3 + -28 * v1 + 18 * v2 - v8 - 6308
f11=99 * v11 + -28 * v9 + 5 * v8 + 93 * v6 + -18 * v7 + -127 * v5 + 6 * v4 + -9 * v3 + -93 * v1 + 58 * v2 + 1697

r = solve([f1, f2, f3, f4, f5, f6, f7, f8, f9, f11], [v1, v2, v3, v4, v5, v6, v7, v8, v9, v11])
res=[]
for i, j in r.items():
    res.append(j)

x=res[0]
res[0]=res[1]
res[1]=x

y=res[5]
res[5]=res[6]
res[6]=y

flag=""
for i in range(len(res)):
    flag+=chr(res[i])
print(flag)
```



得到v5==F0uRTy_7w@

3.代入运行sub_C50函数得到flag。

flag{F0uRTy_7w@_42}