BUUCTF-RE-[ACTF新生赛2020]Universe_final_answer

原创

Persistent_s 于 2021-05-08 16:33:32 发布 40 收藏

分类专栏： RE CTF 逆向

本文链接：https://blog.csdn.net/Henlenl/article/details/116531098


RE 同时被 3 个专栏收录

20 篇文章 0 订阅

订阅专栏


CTF

28 篇文章 1 订阅

订阅专栏

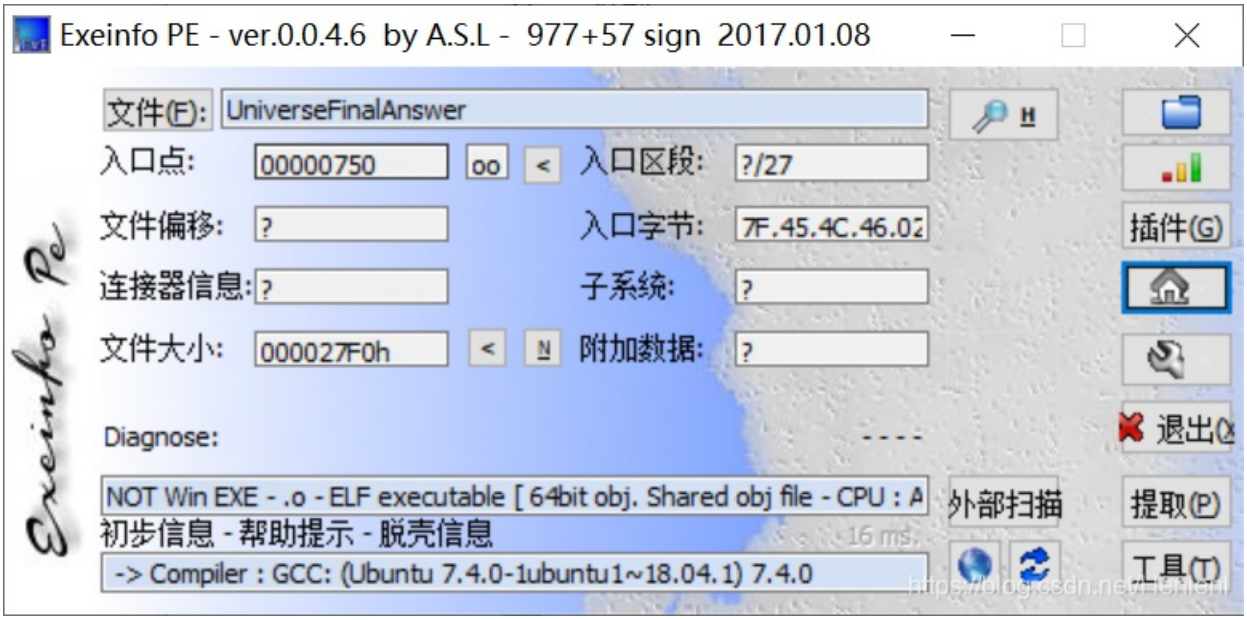

逆向

18 篇文章 0 订阅

订阅专栏

[ACTF新生赛2020]Universe_final_answer

查壳


Exeinfo PE - ver.0.0.4.6 by A.S.L - 977+57 sign 2017.01.08
文件(F):
UniverseFinalAnswer
入口点:
00000750
入口区段:
?/27
文件偏移:
?
入口字节:
连接器信息:
?
子系统:
?
文件大小:
000027F0h
附加数据:
?
Diagnose:
NOT Win EXE - .o - ELF executable [64bit obj. Shared obj file - CPU : A
初步信息 - 帮助提示 - 脱壳信息
-> Compiler : GCC: (Ubuntu 7.4.0-1ubuntu1~18.04.1) 7.4.0
外部扫描
插件(G)
退出(X
提取(P)
工具(T)

无壳程序

IDA 分析

进入main函数

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 v4; // [rsp+0h] [rbp-A8h]
  char v5; // [rsp+20h] [rbp-88h]
  unsigned __int64 v6; // [rsp+88h] [rbp-20h]

  v6 = __readfsqword(0x28u);
  __printf_chk(1LL, "Please give me the key string:", a3);
  scanf("%s", &v5);
  if ( sub_860(&v5) )
  {
    sub_C50((__int64)&v5, &v5, &v4);
    __printf_chk(1LL, "Judgement pass! flag is actf{%s_%s}\n", &v5);
  }
  else
  {
    puts("False key!");
  }
  return 0LL;
}
```


我们进入主要的函数(sub_860)看看

```
  v1 = a1[1];
  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 + 122 * v8 + -19 * 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;
}
```


这种题目一看就知道是z3求解器

z3学习与安装

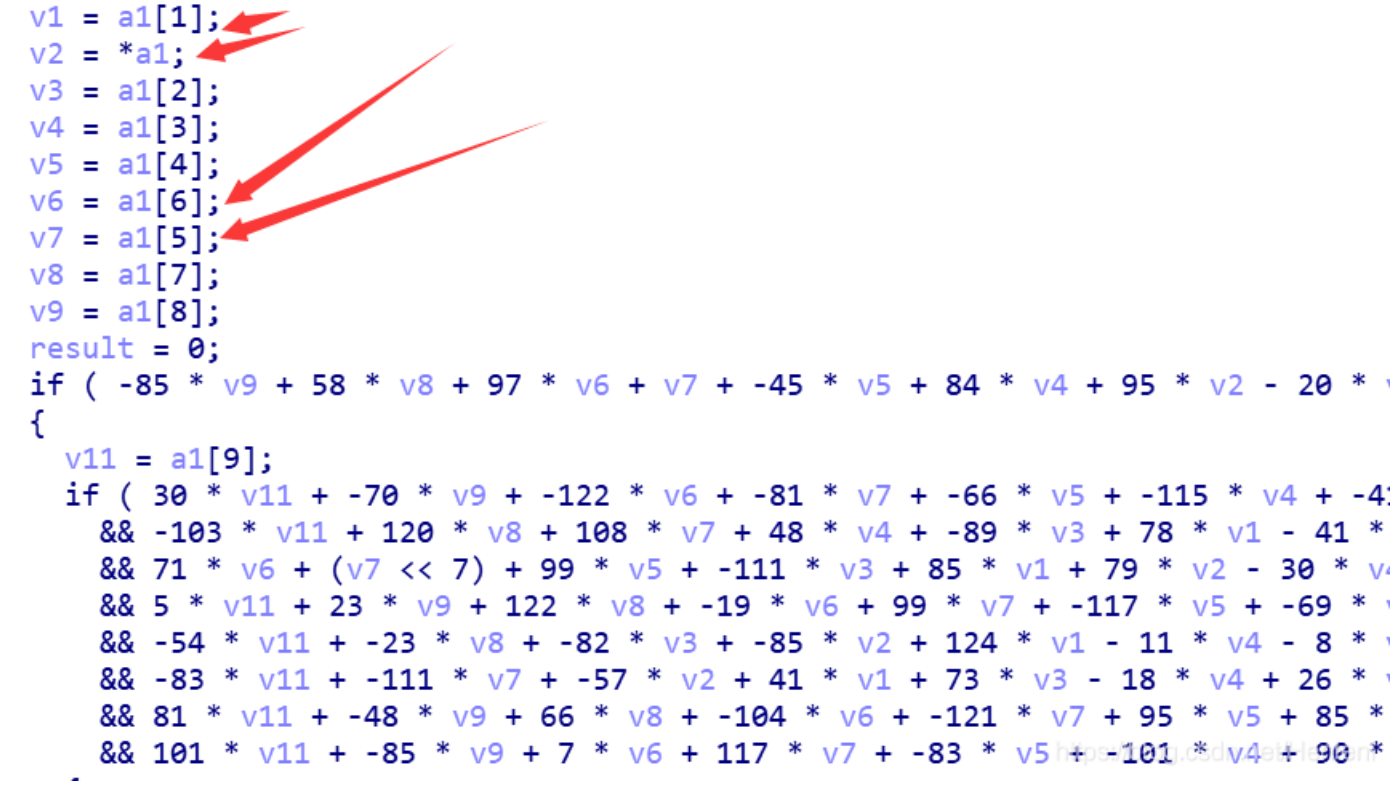
脚本

```
from z3 import *
s = Solver()
v1 = Int('v1')
v2 = Int('v2')
v3 = Int('v3')
v4 = Int('v4')
v5 = Int('v5')
v6 = Int('v6')
v7 = Int('v7')
v8 = Int('v8')
v9 = Int('v9')
v11 = Int('v11')

s.add(-85 * v9 + 58 * v8 + 97 * v6 + v7 + -45 * v5 + 84 * v4 + 95 * v2 - 20 * v1 + 12 * v3 == 12613)
s.add(30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -41 * v3 + -86 * v1 - 15 * v2 - 30 * v
8 == -54400)
s.add(-103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 * v2 + 31 * v5 - (v6 * 64) - 120 * v9
 == -10283)
s.add(71 * v6 + (v7 * 128) + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v4 - 119 * v8 + 48 * v9 - 16 * v11 =
= 22855)
s.add(5 * v11 + 23 * v9 + 122 * v8 + -19 * v6 + 99 * v7 + -117 * v5 + -69 * v3 + 22 * v1 - 98 * v2 + 10 * v4 ==
-2944)
s.add(-54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 * v5 - 60 * v7 + 95 * v6 + 100 * v9 ==
 -2222)
s.add(-83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 * v5 + 16 * v6 + 77 * v8 - 63 * v9 ==
-13258)
s.add(81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 * v4 + 60 * v3 + -85 * v2 + 80 * v1 =
= -1559)
s.add(101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 * v3 + -28 * v1 + 18 * v2 - v8 == 630
8)
s.add(99 * v11 + -28 * v9 + 5 * v8 + 93 * v6 + -18 * v7 + -127 * v5 + 6 * v4 + -9 * v3 + -93 * v1 + 58 * v2 == -
1697)

if s.check() == sat:
    result = s.model()

print(result)
```

然后我们得到结果

```
[v6 = 95,
 v9 = 119,
 v11 = 64,
 v7 = 121,
 v2 = 70,
 v4 = 82,
 v3 = 117,
 v1 = 48,
 v5 = 84,
 v8 = 55]
```

但是要值得注意的是(v1 与 v2的位置要互换,v6 与 v7的位置要互换)



```
v1 = a1[1];
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 *
{
  v11 = a1[9];
  if ( 30 * v11 + -70 * v9 + -122 * v6 + -81 * v7 + -66 * v5 + -115 * v4 + -4
    && -103 * v11 + 120 * v8 + 108 * v7 + 48 * v4 + -89 * v3 + 78 * v1 - 41 *
    && 71 * v6 + (v7 << 7) + 99 * v5 + -111 * v3 + 85 * v1 + 79 * v2 - 30 * v
    && 5 * v11 + 23 * v9 + 122 * v8 + -19 * v6 + 99 * v7 + -117 * v5 + -69 *
    && -54 * v11 + -23 * v8 + -82 * v3 + -85 * v2 + 124 * v1 - 11 * v4 - 8 *
    && -83 * v11 + -111 * v7 + -57 * v2 + 41 * v1 + 73 * v3 - 18 * v4 + 26 *
    && 81 * v11 + -48 * v9 + 66 * v8 + -104 * v6 + -121 * v7 + 95 * v5 + 85 *
    && 101 * v11 + -85 * v9 + 7 * v6 + 117 * v7 + -83 * v5 + -101 * v4 + 90 *
```

那么我们可以进行变换

get flag

> flag{F0uRTy_7w@_42}