



[BUUCTF]REVERSE——[ACTF新生赛2020]Universe_final_answer（z3求解）

原创

[Angel~Yan](#)  于 2021-03-05 12:24:01 发布  102  收藏 1

分类专栏: [REVERSE BUUCTF刷题记录](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/mcmuyanga/article/details/114376433>

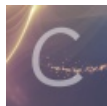
版权



[REVERSE](#) 同时被 2 个专栏收录

75 篇文章 1 订阅

订阅专栏



[BUUCTF刷题记录](#)

198 篇文章 14 订阅

订阅专栏

[\[ACTF新生赛2020\]Universe_final_answer](#)

附件

步骤

1. 无壳儿，一般elf文件都是64位
先在linux中试运行一下看看大概的情况

```
Please give me the key string:123456
False key!
```

2. 64位ida打开，根据运行时候看到的字符串找到关键函数，输入一个字符串，经过sub_860和sub_C50得到flag

```
1 __int64 __fastcall main(int a1, char **a2, char **a3)
2 {
3     __int64 v4; // [rsp+0h] [rbp-A8h] BYREF
4     char v5[104]; // [rsp+20h] [rbp-88h] BYREF
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 ( (unsigned __int8)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 }
```

<https://blog.csdn.net/mcmuyanga>

3. sub_860 ()

```

bool __fastcall sub_860(char *a1)
{
    int v1; // ecx
    int v2; // esi
    int v3; // edx
    int v4; // er9
    int v5; // er11
    int v6; // ebp
    int v7; // ebx
    int v8; // er8
    int v9; // er10
    bool result; // al
    int v11; // [rsp+0h] [rbp-38h]

    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 * v
1 == -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;
}

```

一个算法函数，利用z3库，基本照抄一下就可以解到a1数组，[z3库用法](#)

```

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 * v8
    == -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)

```

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

根据a1数组的顺序，排一下，得到a1数组

a1=[70,48,117,82,84,121,95,55,119,64]

转成字符串看一下

```
>>> a1=[70, 48, 117, 82, 84, 121, 95, 55, 119, 64]  
>>> for i in a1:  
    print(chr(i), end="")
```

F0uRTy_7w@

这题还有一个函数sub_C50 ()，但是参数v4要动调才能知道，估计经过该函数后就能得到最后的flag，但是这题在你解出这个z3后得到key string就可以了，sub_C50根本不用去分析

```
Please give me the key string:F0uRTy_7w@  
Judgement pass! flag is actf{F0uRTy_7w@_42}
```

flag{F0uRTy_7w@_42}