第46天：红帽杯2019-childRE（二）

原创

S1lenc3 于 2019-12-15 22:31:30 发布 215 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/qq_41858371/article/details/103554581

昨天说到处理完输入了，今天把这道题干掉了，一定要有耐心，慢慢调试。

把输入的三个数设为x，y，z。

断到这里，

```
  }
  v16 = (char *)x[0];
  v17 = (_QWORD)(x[1] - x[0]) >> 2;             // 判断x有几位
  v18 = z[0];
  v19 = (_QWORD)(z[1] - z[0]) >> 2;             // 判断z有几位
  v20 = (char *)y[0];
  if ( v17 == v19 )
  {
    v22 = v17 - 1;
    if ( (signed int)v17 - 1 < 0 )
      goto LABEL_47;
    v23 = v22;
    v24 = (char *)z[0] + 4 * v22;               // 从最高位开始，逐位比较
    while ( *(_DWORD *)((char *)v24 + x[0] - z[0]) == *v24 )
    {
      --v22;
      --v24;
      if ( --v23 < 0 )
        goto LABEL_47;
    }
    v21 = *((_DWORD *)x[0] + v22) < *((_DWORD *)z[0] + v22);// 判断x<z?
  }
  else
  {
    v21 = v17 < v19;                            // x<z
  }
  if ( !v21 )
    goto LABEL_47;
  v27 = (_QWORD)(y[1] - y[0]) >> 2;             // 判断y有几位
  if ( v27 != v17 )
  {
    v28 = v27 < v17;
    goto LABEL_62;
```

注释都标注了，自己分析一下。

在这里，发现goto到label_47就直接到运行结束了，没有flag，所以就不让他跳转，就要满足x<z

```
}
v28 = *((_DWORD *)y[0] + v29) < *((_DWORD *)x[0] + v29);// 判断y<x?
```

类似的，也要满足y<x。继续单步，来到一堆计算的地方。

```
v32 = mul(&v136, v125, x);                      // x*3
v33 = mul(&v133, v32, x);                       // x*x*3
v34 = mul(&v130, v33, y);                       // x*x*3*y
v35 = pow(&v127, y, v123);                      // y**2
v36 = mul(&v151, v121, x);                      // x*3
v37 = mul(&v140, v36, v35);                     // x*3*y**2
```

这里是计算位数的。

```
v40 = (_QWORD)(x[1] - x[0]) >> 2;               // x的位数
```

```
v46 = add(Memory, v114, y);
v47 = pow(&v139, v46, v119);                    //  (x+y) **3
v144 = v47;
v48 = sub_7FF6825C1700(&v153, v37);
v49 = sub(v47, v48);
sub_7FF6825C1700(v112, v49);                    // 赋值
v50 = *(_QWORD **)v47;
if ( *(_QWORD *)v47 )
```

这都是一步一步分析的，没什么说的。

```
v65 = mul(&v127, v121, z);                      // z*48
v66 = mul(&v130, v123, z);                      // z*12
v67 = mul(&v133, v66, z);                       // z*z*12
LODWORD(v144) = 4;
_mm_storeu_si128((__m128i *)Memory, (__m128i)0i64);
v118 = 0i64;
sub_7FF6825C4330(Memory, 0i64, &v144);
sub_7FF6825C1270(Memory);
v68 = add(&v136, Memory, z);                    // z+4
v69 = (void **)pow(&v143, v68, v125);           // (z+4)**3
v116 = v69;
v70 = sub_7FF6825C1700(&v139, v67);
v71 = sub(v69, v70);
sub_7FF6825C1700(v112, v71);
```


有很多类似下边这种的判断，刚开始分析了一下，后来发现不影响值的变化，可以忽略。

```
if ( v112[0] )
{
  if ( (unsigned __int64)(4 * ((signed __int64)(v113 - (unsigned __int64)v112[0]) >> 2)) >= 0x1000 )
  {
    v75 = (void *)*((_QWORD *)v112[0] - 1);
    if ( (unsigned __int64)(v112[0] - v75 - 8) > 0x1F )
      invalid_parameter_noinfo_noreturn();
  }
  j_j_free(v75);
  _mm_storeu_si128((__m128i *)v112, (__m128i)0i64);
  v113 = 0i64;
}
```


继续调试，看到了flag字样：

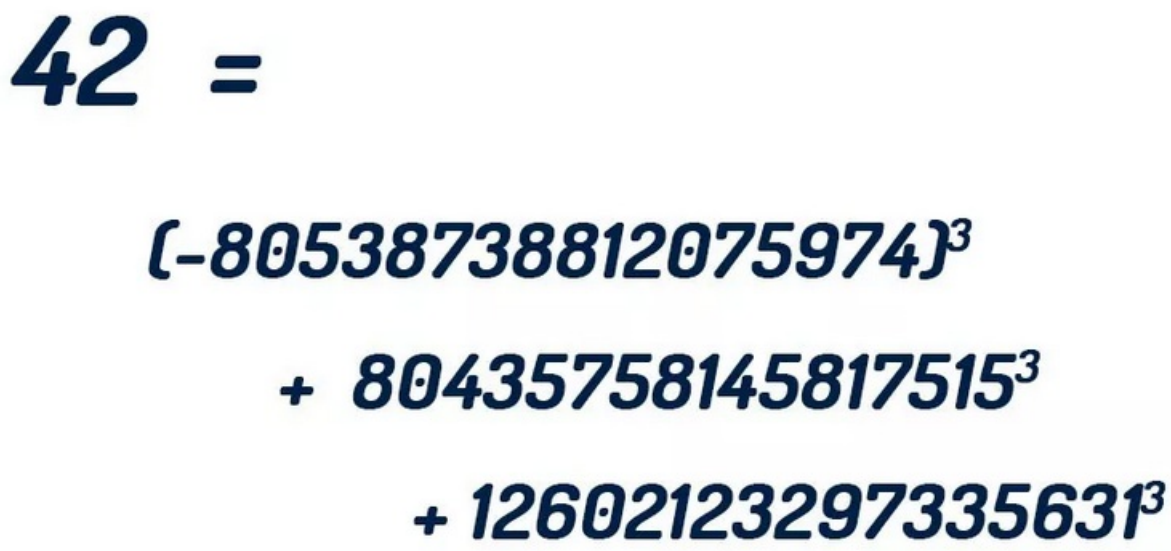
```
v87 = (char *)v153;
v88 = (v154 - (signed __int64)v153) >> 2;
v89 = (char *)v151;
v18 = z[0];
if ( v88 == ((_QWORD)v152 - (_QWORD)v151) >> 2 )
{
  v90 = v88 - 1;
  if ( (signed int)v88 - 1 < 0 )
  {
LABEL_201:
    sub_7FF6825C4120(std::cout, "You win!\nflag{MD5(\"");
    v93 = x[0];
    v94 = x[1];
    if ( x[0] == x[1] )
```


这里只有v88小于等于0时才能执行到You win，然后v88又是某个数的位数，所以只能等于0，然后就需要往上翻找到刚才的一堆计算，最后可以得出如下：

(x+y)**3-(x*3*y**2)-(x**2*3*y)=0
((z+4)**3-z*z*12)-z*48-22=0

可以得出，x**3+y**3-z**3=42

我也算不出来，但是有答案啊，说实话就算我比赛的时候做到这儿，我也不知道有这么三个数。。。。



一定要记住，分析程序的时候，不要太依赖IDA的伪代码，很多代码我都是配合汇编才看懂，这道题需要慢慢分析各个函数的作用，要有耐心。

官方writeup：https://mp.weixin.qq.com/s?__biz=MzU3MzczNDg1OQ==&mid=2247484311&idx=1&sn=5d0276066554008c078e42114301095b&chksm=f