

# 2021强网杯 ezmath writeup

原创

一梦不醒 于 2021-06-30 12:55:29 发布 111 收藏

分类专栏: [逆向题解 reverse](#) 文章标签: [reverse](#)

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/qq\\_39153421/article/details/118357222](https://blog.csdn.net/qq_39153421/article/details/118357222)

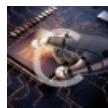
版权



[逆向题解](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[reverse](#)

1 篇文章 0 订阅

订阅专栏

## 前言

题目ida查看后发现有浮点数的运算, 涉及到精度的问题, 本来想的是爆破每一位, 但是发现条件由于精度损失的问题不可能相等, 且数据越来越大, 直到程序inf. 后来听说是math有关的知识, 看了别人的wp, 发现竟是一大堆的数学公式的运算: 积分, 泰勒公式, 辛普森公式. 下面就分析一下题目功能和思路.

## 题目功能

题目逻辑是内置了一个长度为19的数组, 输入的数据经过函数sub\_13F3运算后, 如果相等则输出correct!

```
__isoc99_scanf("%39s", s);
if ( strlen(s) == 38 )
{
    for ( i = 0; i <= 37; i += 2 )
    {
        if ( dbl_4020[i / 2] != sub_13F3(*(unsigned __int16 *)&s[i]) )
            goto LABEL_2;
    }
    puts("correct");
    result = 0LL;
}
```

sub\_13F3函数, 功能是从8225到输入数据的大小循环迭代v3, 如下:

```
double __fastcall sub_13F3(int a1)
{
    int i; // [rsp+8h] [rbp-Ch]
    double v3; // [rsp+Ch] [rbp-8h]

    v3 = qword_2010; // 0x3f3fa5e61d8cedfd 0.00048291080524950886
    for ( i = 0x2021; i < a1; ++i )
        v3 = 2.718281828459045 - (double)i * v3;
    return v3;
}
```

## 尝试

经过调试，得到了qword\_2010的值0.00048291080524950886，然后按照程序的逻辑仿写了代码，对每个字符进行爆破，但是结果发现，得到的数据一正一负且越来越大最后越界inf。发现爆破不太行，陷入了僵局。到底哪里出了问题？后来发现2.718281828459045是自然数e，根据题目名字ezmath猜测是和math有关，函数里面是关于v3的递推，发现类似于

$$I = e^{-\frac{1}{v_3}}$$

## 分析数学算法



## exp

```
import math
import codecs
res = [0.00009794904266317233, 0.00010270456917442, 0.00009194256152777895,
0.0001090322021913372, 0.0001112636336217534, 0.0001007442677411854,
0.0001112636336217534, 0.0001047063607908828, 0.0001112818534005219,
0.0001046861985862495, 0.0001112818534005219, 0.000108992856167966,
0.0001112636336217534, 0.0001090234561758122, 0.0001113183108652088,
0.0001006882924839248, 0.0001112590796092291, 0.0001089841164633298,
0.00008468431512187874]
flag = b''
for i in res:
    flag += codecs.decode(hex(int(math.e/i)-1)[2:], 'hex')[::-1]
print flag
print len(flag)
```

## 总结

题目让我了解了数学知识在程序中的应用，加深了数学从理论到时间的认识，一切源于数学，我是个菜鸡该好好补补数学知识了！！

## 参考

[https://blog.csdn.net/weixin\\_43363675/article/details/118078787](https://blog.csdn.net/weixin_43363675/article/details/118078787)  
<https://blog.csdn.net/SCP000111/article/details/118033127>  
<https://cdcq.github.io/2021/06/15/20210615a/>