

# CUIT CTF WriteUp-初中数学题

原创

RickGray 于 2014-05-22 16:27:12 发布 1232 收藏

分类专栏: [CTF纪实](#)

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/u013565525/article/details/26600665>

版权



[CTF纪实](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

此题还是比较简单, 就是算出字符串后误以为就是flag, 结果纠结了半天, 才想起把算出的字符串输入到程序里面去, 我去, 坑了我好久, 2B了。

首先多的不说, 直接载进IDA进行分析 (Writeup写得有点累了, 可能写的不怎么详细, 见谅!), 载入IDA

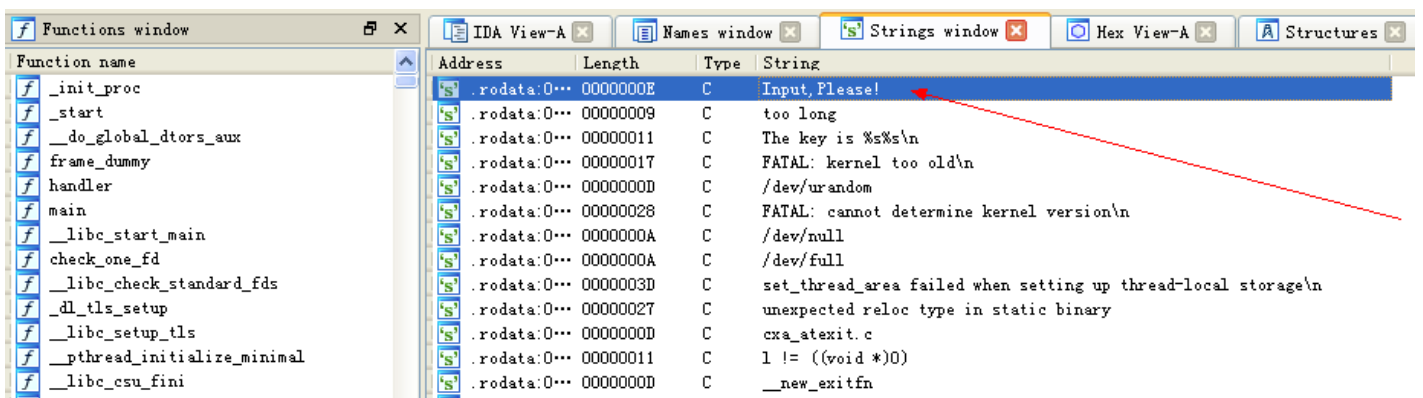
====忘记此题文件被加壳了-upx, So, 使用upx -d后再载入IDA~! ~!

```
root@Meos: ~/Desktop
root@Meos:~/Desktop# upx -d Re300 -o re300
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2011
UPX 3.08      Markus Oberhumer, Laszlo Molnar & John Reiser   Dec 12th 2011

File size      Ratio      Format      Name
-----
584890 <-    267472    45.73%    netbsd/elf386    re300

Unpacked 1 file.
root@Meos:~/Desktop#
```

通过字符串查找, 找到关键字串



跳到字符串调用处F5, 此时可以清晰的看到整个程序的过程

```

puts(0, 64);
_isoc99_scanf("%s", &v10);
if ( strlen(&v10) > 0xBu )
{
    puts("too long");
    exit(-1);
}
v0 = getpid();
v1 = getsid(v0);
if ( v1 != getppid() )
    exit(1);
if ( v11 != v12 || v11 + v12 != 222 )
    exit(-1);
if ( v13 != 2 * (v14 - 1) || v13 != v10 + 29 || v15 != v14 + 31 || v14 + v13 + v10 + v15 != 304 )
    exit(-1);
if ( ptrace(0, 0, (void *)1, 0) < 0 )
    exit(-1);
for ( i = 4; i <= 8; ++i )
{
    if ( v8 + (char)*(&v10 + i) ^ 0x11 != *(&v3 + v8) )
        exit(-1);
    ++v8;
}
printf("The key is %s%s\n", (unsigned int)&v10);
result = *MK_FP(__GS__, 20) ^ v16;
if ( *MK_FP(__GS__, 20) != v16 )
    _stack_chk_fail();
return 0;
}

```

最重要的就是上面那一堆东西了，其实在IDA里面用Graph来看的话更清晰一点，具体的就不多说了，根据上面的代码算一下就可以得到v? 的值，当输入字符串超过12位时，程序会提示“too long”，So，直接猜测输入的字符串就为12位，再根据在IDA中，变量的定义情况也可以确定，经过简单计算后，可以得到当输入的字符串为：GoodCrack3R时会输出flag，下面贴几个关键代码图

```

memset(&v10, 0, 0x100u);
v3 = 82;
v4 = 100;
v5 = 114;
v6 = 117;
v7 = 94;
v8 = 0;

```

```

for ( i = 4; i <= 8; ++i )
{
    if ( v8 + (char)*(&v10 + i) ^ 0x11 != *(&v3 + v8) )
        exit(-1);
    ++v8;
}

```

得到正确的输入后，输入程序即可得到flag: *GoodCrack3R&UnPack3r*