6ctf writeup

team: tx

username:xxw

0x01 Crackeme(Reverse)

这道题首先打开一下，出现字符“Give me your favourite prime number”
所以用IDA打开，查找字符串，然后用Ctrl+X，查找引用字符串的函数，找到了一个函数Check1，发现这个函数判断输入的数字n和他里面一个计算出来的数c是否相等，相等把n给flag，同时返回一个v1=1，不等就返回0，所以再次查一下引用的函数：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _alloca(0x10u);
  __main();
  flag = 0LL;
  pos = 0;
  if ( (unsigned __int8)check1() && (unsigned __int8)check2() && (u
nsigned __int8)check3() && (unsigned __int8)check4() )
  {
    printf("the flag is:%lld", flag);
    while ( flag )
    {
      printf("%c", (unsigned __int64)(flag % 10) + 65, 10, 0);
      printf("%c", (unsigned __int64)(flag % 10) + 106, 10, 0);
      flag /= 10LL;
    }
    puts(&byte_44513D);
    puts("^^^^Good^^^^");
  }
  return 0;
}
```

找到了flag的判定函数了，有4个，一个一个来就是了
第一个我直接用OD运行了一遍，发现c的值是2，所以确定第一个输入为2
第二个，是输入的数和tmp相乘对mod求余等于tmpans，而且这个n不能大于999999，写了个python脚本：

```
for n in range(100,1000000):
    x=123456*n
    if(x%1000000007==779852816):
        print n
```

跑了一下，得到654321（话说那个tmp是123456。。。）
第三个，还是 费了挺大劲，反正代码没有一行行都看懂，加了点推测的因素吧，看到那个MerryChristmas，还有后面有个字符串比较，所以开始想当然输了个一样的，理所当然不对，然后再看，字符串必须有14位，而且还有一个转折，后面有段代码：

```
if ( std::string::length((std::string *)&v19) == '\x0E' )
 {
   for ( i = 0; i <= 13; ++i )
   {
     j = i % 6 + 1;
     v9 = 1;
     v0 = std::string::operator[]((std::string *)&v19, i);
     v6 = *(_BYTE *)v0 + x[j];
     v1 = std::string::operator[]((std::string *)&v18, i);
     if ( v6 != *(_BYTE *)v1 )
     {
       v9 = 3;
       std::string::~string((std::string *)&v18);
       v9 = -1;
       std::string::~string((std::string *)&v19);
       v7 = 0;
       goto LABEL_12;
     }
   }
```

这里面判断了一下v1和v6，其中v1就是MerryChristmas每一位，而v6进行了一个“+”运算，从1到6，倒退过去就是每个字符的ASCII码减一下，所以输入的字符串应该是“Lcont=gpfoog`q”
第四个，发现输入对flag没有影响，直接OD里面把跳转给改掉，不让代码调到else里面就行了，然后运行得到flag：
176455667HqGpGpFoFoEnGpHqBk

0x02 warmup_re (reverse)

这道题用IDA32位打不开，是个64位程序，所以我就只用IDA64查看了静态代码，没有动态调果然吃力多。
还是根据字符串找到函数，发现函数里面出现了21个数，前后有两个输入，然后函数先判定两个输入字符串长度是否一样，然后两个字符串中每一位进行异或运算，然后和那21个数一个一个对比，相等，就输出你的输入是flag，说实话到这了我没看懂，因为不管第一个输入是什么，第二个输入只要保证这个关系就运行报的是对的，然后发现提示里有个“goodgoodstudydaydayup”，刚好21位，而且说是用户名，这样就懂了，flag就是：
1qwer5tyui90op4ertghg

0x03 BASE64？

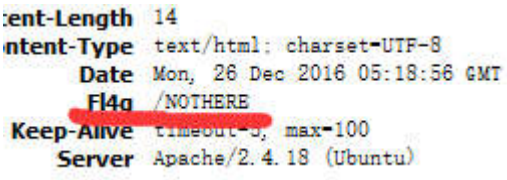
先base32解码，再ASCII解码，得到flag：
PCTF{Just_t3st_h4v3_f4n}

0x04 sign

先ASCII解码，再base32解码，再base64解码，得到flag：
flag{61d_club_welcome}

0x05 warmup——web

打开火狐F12，进入网站，看一下头信息，发现这个：



放到URL后面，ENTER一下:

```
flag{OpenYourHeadHole}
```

0x06 warmup_misc

这道题就是flag每一位字符和那个字符k，也就是本题中的'f'进行异或，在base64编码得到图中的：
UAUSAB1QUFBQUFAbfQ==
所以直接把上面那个base64解码然后再每一位和'f'进行异或运算就得到flag：
6ctf{666666}

0x07 warmup_game

这到题要加群主大人的qq，然后看一下游戏人生，看到无畏先锋区的id是:

还要再猜一下，当然在TGP直接战绩查询，猜的时候方便很多：

（话说中间三个*号我已开始还以为只有3个字母。。。）