CTF 扫雷逆向writeup

原创

yoyo_573 于 2020-10-11 21:59:23 发布 522 收藏 1

分类专栏： ctf

本文链接：https://blog.csdn.net/yoyo_573/article/details/109017642

IDA 打开看Main函数 看到label_52

```
    goto LABEL_27;
  if ( mode & 1 )
    break;
  if ( map[30 * floatx + floaty] == 64 && !flag[0][30i64 * floatx + floaty] )
    goto LABEL_52;
  if ( flag[0][30i64 * floatx + floaty] != 1 )
  {
    Open();
    position(0, 0);
    SetConsoleTextAttribute(handle_out, 2u);
    for ( i = 0; i <= 29; ++i )
    {
      for ( j = 0; j <= 29; ++j )
```



```
108       printf(asc_486016, (unsigned int)(300 - flagnum));
109       goto LABEL_44;
110     }
111 LABEL_52:
112     SetConsoleTextAttribute(handle_out, 4u);
113     position(5, 5);
114     if ( game == 1 )
115     {
116       printf(asc_4861F8);
117     }
118     else
119     {
120       re();
121       Sleep(0x186A0u);
122     }
123     position(5, 8);
124     Sleep(0x3E8u);
125     printf("任意键重玩");
126     scanf("%c%c", spare, spare);
127     system("cls");
128     position(0, 0);
129   }
130 }
```

查看re()函数

```
int k; // [rsp+28h] [rbp-8h]
int i; // [rsp+2Ch] [rbp-4h]

if ( game == 601 )
{
  for ( i = 0; i <= 37; ++i )
  {
    flaga[i] -= j++;
    if ( j == 4 )
      j = 0;
  }
  for ( k = 0; k <= 37; ++k )
    printf("%c", (unsigned int)flaga[k]);
  printf(" ");
}
else
{
  for ( i_0 = 0; i_0 <= 46; ++i_0 )
  {
    flagb[i_0] -= j++;
    if ( j == 4 )
      j = 0;
  }
  for ( k_0 = 0; k_0 <= 46; ++k_0 )
    printf("%c", (unsigned int)flagb[k_0]);
  printf(" ");
```


你可以双击查看flaga[i]的数值，拷贝到数组中，其中du 2表示2个相同值。

这里就知道 是if里的得到flag
直接上脚本

```
j=1
flaga=[0x67,0x6e,0x64,0x67,0x7c,0x67,0x34,0x30,0x62,0x66,0x66,0x33,0x3a,0x36,0x3c,0x62,0x62,0x37,0x3c,0x61,0x63,
0x64,0x68,0x35,0x37,0x67,0x33,0x35,0x38,0x68,0x35,0x30,0x67,0x3a,0x3b,0x33,0x66,0x7f,0x26]
for i in range(38):
    flaga[i]-=j
    j=j+1
    if j==4:
        j=0
        print ( flaga)
flag = ""
for i in range(38):
    flag+=chr(flaga[i])
print (flag)
```

flag{e10adc3949ba59abbe56e057f20f883e}