BugKu Re 部分 Writeup

原创

疯疯芸 于 2019-07-08 12:56:00 发布

分类专栏： CTF 文章标签： CTF Re

本文链接：https://blog.csdn.net/qq_45262739/article/details/95054133

入门逆向

拖进 IDA 发现初始化了一推变量，直接全部 R 得到 flag

easy_vb

拖进 IDA 看起来有壳，但是，往下看看，发现了 `MCTF{_N3t_Rev_1s_E4ay_}` 大喜，赶紧提交，然后错了。。。

回看题目，提交格式为 `flag{}` ，心想，哎呀**，入门题还要搞点坑让人跳，CTF 套路深，我还是溜了吧。

然后试了各种方法，啥都没发现。然后看了一篇题解，说是要把 `MCTF` 替换成 `flag`。

.....

啥也别说了，CTF 套路深。

提交 flag： `flag{_N3t_Rev_1s_E4ay_}`

Easy_Re

拖进 IDA，F5 反编译

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v3; // eax
  __int128 v5; // [esp+0h] [ebp-44h]
  __int64 v6; // [esp+10h] [ebp-34h]
  int v7; // [esp+18h] [ebp-2Ch]
  __int16 v8; // [esp+1Ch] [ebp-28h]
  char v9; // [esp+20h] [ebp-24h]

  _mm_storeu_si128((__m128i *)&v5, _mm_loadu_si128((const __m128i *)&xmmword_413E34));
  v7 = 0;
  v6 = qword_413E44;
  v8 = 0;
  printf("欢迎来到DUTCTF呦\n");
  printf("这是一道很可爱很简单的逆向题呦\n");
  printf("输入flag吧:");
  scanf("%s", &v9);
  v3 = strcmp((const char *)&v5, &v9);
  if ( v3 )
    v3 = -(v3 < 0) | 1;
  if ( v3 )
    printf(aFlag_0);
  else
    printf((const char *)&unk_413E90);
  system("pause");
  return 0;
}
```

就是输入一个字符串 v9 与 v5 比较
拖进 OD，在输入时加一个断点，观察寄存器的值得到 flag：`DUTCTF{We1c0met0DUTCTF}`

```
EAX 00000001
ECX 00A9115D re1.00A9115D
EDX 02C36BC0
EBX 00000000
ESP 006FFE54 ASCII "DUTCTF{We1c0met0DUTCTF}"
EBP 006FFE98 ASCII "帼o"
ESI 00A914A5 re1.<ModuleEntryPoint>
EDI 00A914A5 re1.<ModuleEntryPoint>
EIP 00A91062 re1.00A91062
C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 5D1000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```