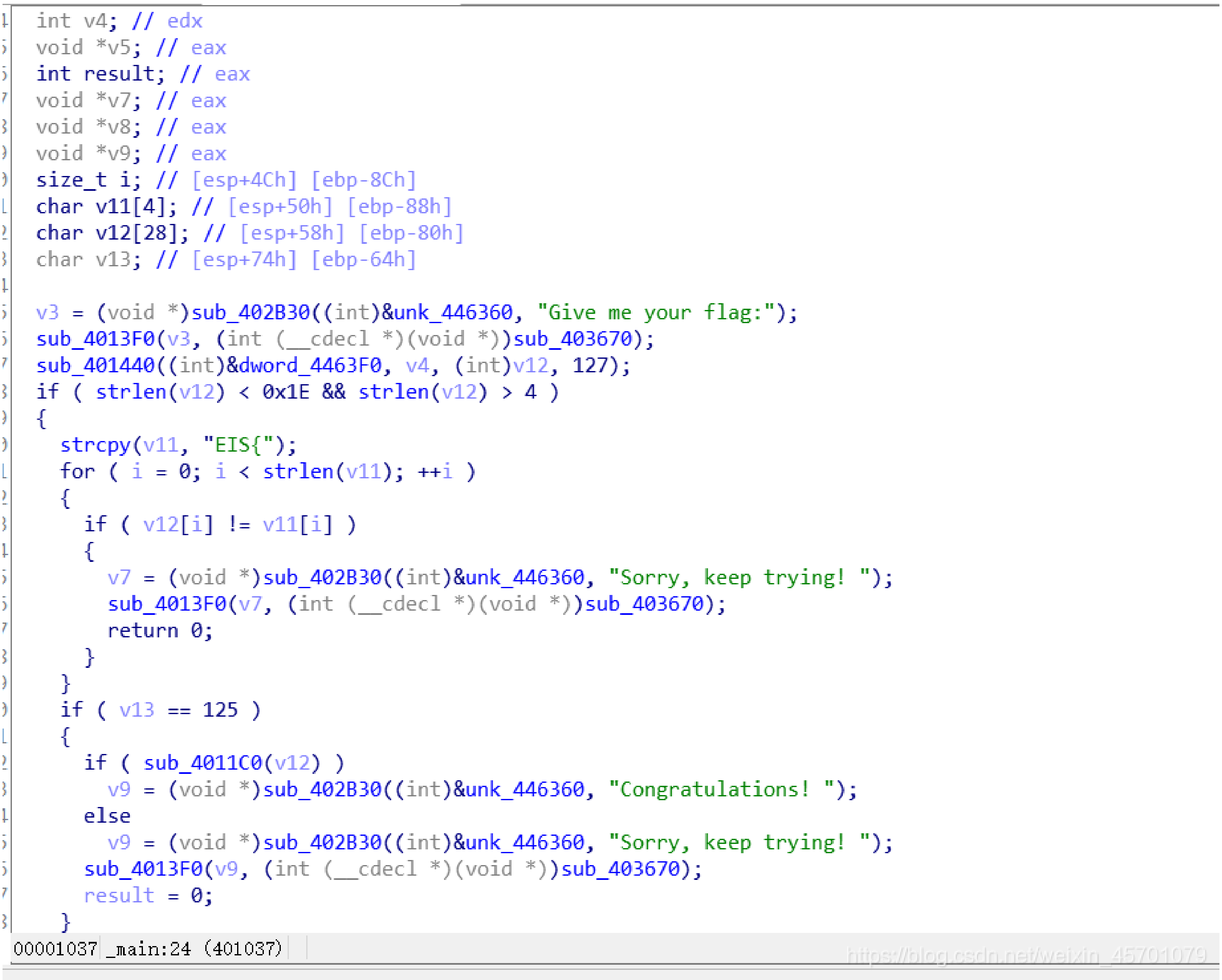
xctf IgniteMe

菜逼的ctf之路 于 2020-10-13 22:23:42 发布 37 收藏 1

xctf IgniteMe

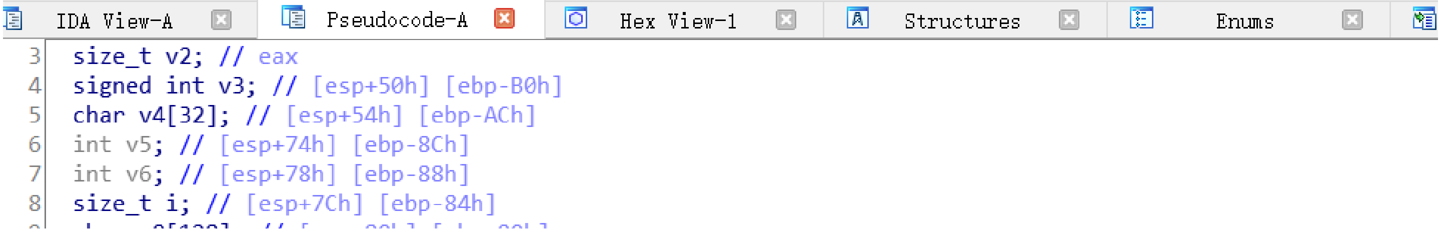
简单题记录一下(本菜鸡也只能记录一下简单题了)
看源代码



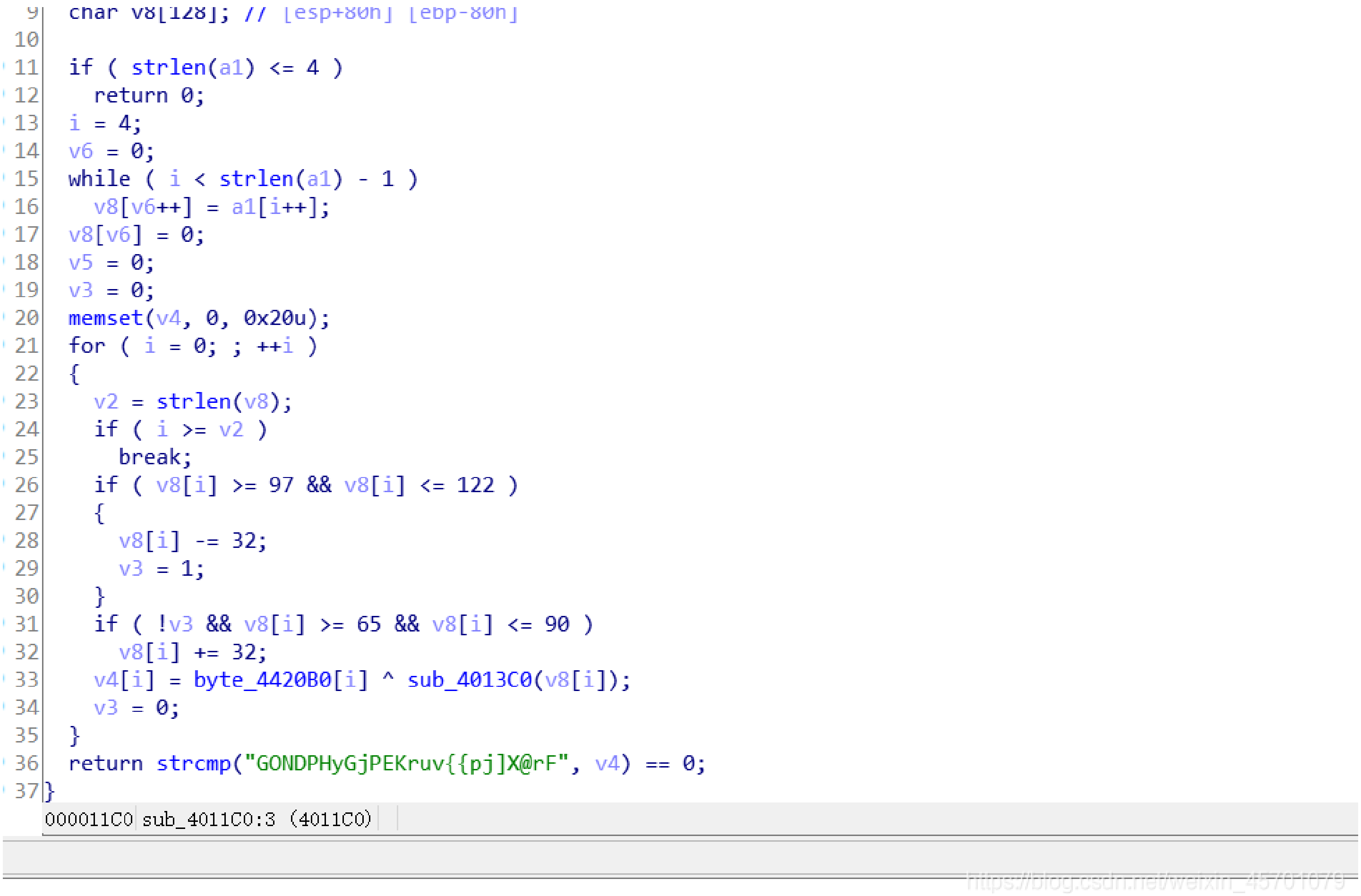
```
  int v4; // edx
  void *v5; // eax
  int result; // eax
  void *v7; // eax
  void *v8; // eax
  void *v9; // eax
  size_t i; // [esp+4Ch] [ebp-8Ch]
  char v11[4]; // [esp+50h] [ebp-88h]
  char v12[28]; // [esp+58h] [ebp-80h]
  char v13; // [esp+74h] [ebp-64h]

  v3 = (void *)sub_402B30((int)&unk_446360, "Give me your flag:");
  sub_4013F0(v3, (int (__cdecl *)(void *))sub_403670);
  sub_401440((int)&dword_4463F0, v4, (int)v12, 127);
  if ( strlen(v12) < 0x1E && strlen(v12) > 4 )
  {
    strcpy(v11, "EIS{");
    for ( i = 0; i < strlen(v11); ++i )
    {
      if ( v12[i] != v11[i] )
      {
        v7 = (void *)sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
        sub_4013F0(v7, (int (__cdecl *)(void *))sub_403670);
        return 0;
      }
    }
    if ( v13 == 125 )
    {
      if ( sub_4011C0(v12) )
        v9 = (void *)sub_402B30((int)&unk_446360, "Congratulations! ");
      else
        v9 = (void *)sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
      sub_4013F0(v9, (int (__cdecl *)(void *))sub_403670);
      result = 0;
    }
00001037 _main:24 (401037)
```

前面的我也没看懂，直接看判断函数sub_4011c0()
打开函数



```
  size_t v2; // eax
  signed int v3; // [esp+50h] [ebp-B0h]
  char v4[32]; // [esp+54h] [ebp-ACh]
  int v5; // [esp+74h] [ebp-8Ch]
  int v6; // [esp+78h] [ebp-88h]
  size_t i; // [esp+7Ch] [ebp-84h]
```

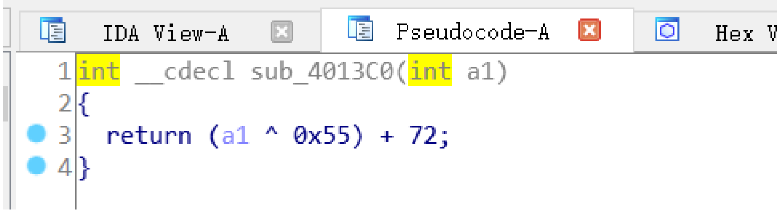


```
char v8[128]; // [esp+80h] [ebp-80h]

if ( strlen(a1) <= 4 )
  return 0;
i = 4;
v6 = 0;
while ( i < strlen(a1) - 1 )
  v8[v6++] = a1[i++];
v8[v6] = 0;
v5 = 0;
v3 = 0;
memset(v4, 0, 0x20u);
for ( i = 0; ; ++i )
{
  v2 = strlen(v8);
  if ( i >= v2 )
    break;
  if ( v8[i] >= 97 && v8[i] <= 122 )
  {
    v8[i] -= 32;
    v3 = 1;
  }
  if ( !v3 && v8[i] >= 65 && v8[i] <= 90 )
    v8[i] += 32;
  v4[i] = byte_4420B0[i] ^ sub_4013C0(v8[i]);
  v3 = 0;
}
return strcmp("GONDPHyGjPEKruv{{pj]X@rF", v4) == 0;
}
```

000011C0 sub_4011C0:3 (4011C0)

逻辑简单先把大小写转换一下(大写转小写，小写转大写)，之后先进入sub_4012c0()函数，然后数据异或，看函数



```
int __cdecl sub_4013C0(int a1)
{
  return (a1 ^ 0x55) + 72;
}
```

简单加密

直接贴出exp

```
a = [
    0x0D, 0x13, 0x17, 0x11, 0x02, 0x01, 0x20, 0x1D, 0x0C, 0x02, 0x19, 0x2F, 0x17, 0x2B, 0x24, 0x1F,
    0x1E, 0x16, 0x09, 0x0F, 0x15, 0x27, 0x13, 0x26, 0x0A, 0x2F, 0x1E, 0x1A, 0x2D, 0x0C, 0x22, 0x4
]
s='GONDPHyGjPEKruv{{pj]X@rF'
flag=''
for i in range(len(s)):
    flag+=chr((((ord(s[i])^a[i])-72)^0x55)^32)
print(flag)
```

最后一个异或32的是大小写转换(看过王爽的汇编的应该懂为啥)，不过因为下划线的存在,异或32之后下划线也变了，所以得到的数据把空格换成下划线就可以了(加上EIS{})。

最近做题有点少，因为社团招新和培训和本地环境出错了，所以书本学习总结可能要向后安排了。