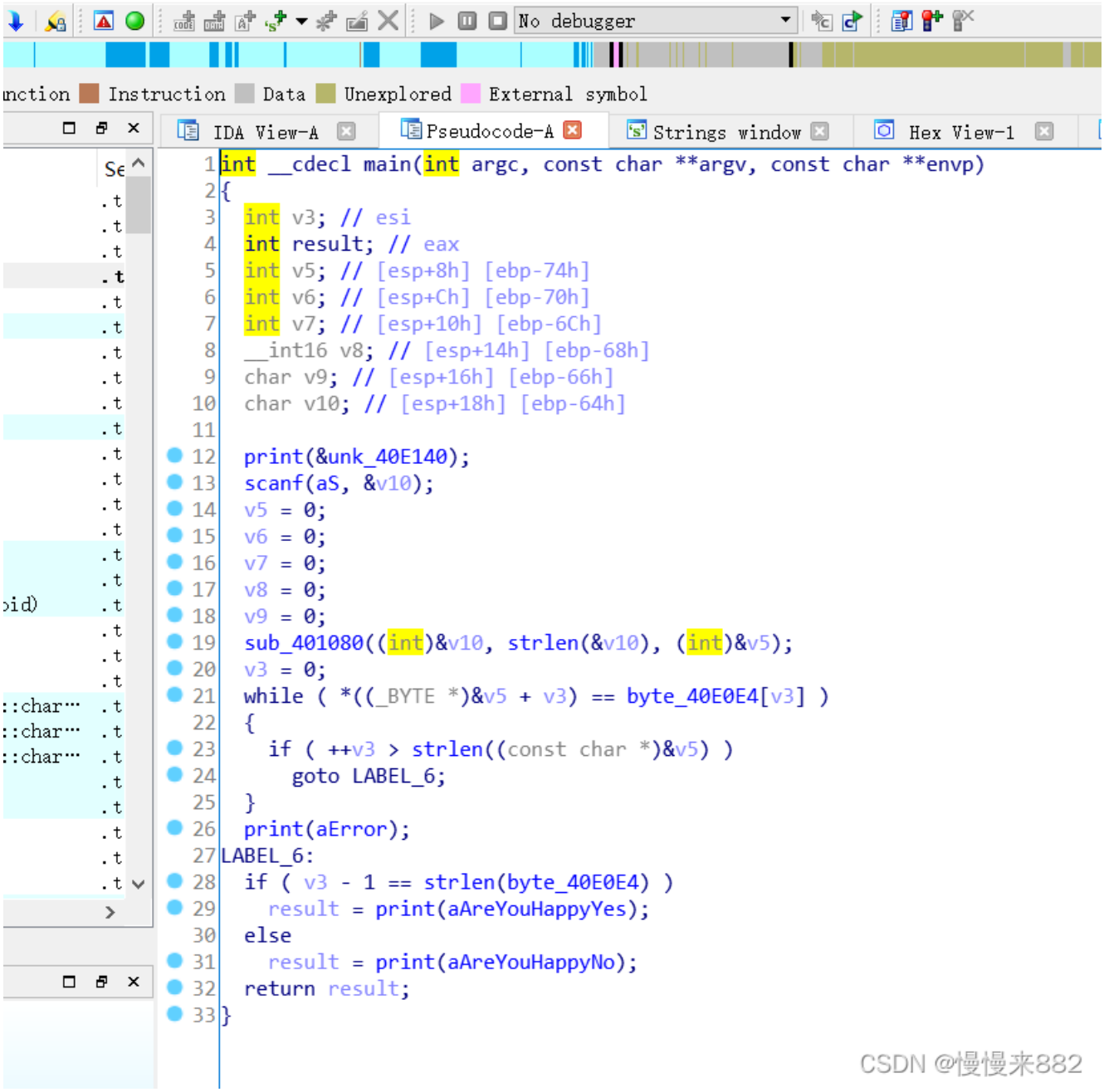
buu:[ACTF新生赛2020]usualCrypt

原创

慢慢来882 于 2021-12-26 13:39:38 发布 1115 收藏
文章标签： 网络安全

查后无壳 32位，放入ida进入main，进行小修小改



BYTE_40E0E4为数组，sub_401080加密方式。后者点进去

```
struction Data Unexplored External symbol
IDA View-A | Pseudocode-A | Strings window | Hex View-1 | Structures | Enums | Imports
```

```
1  int __cdecl sub_401080(int a1, int a2, int a3)
2  {
3    int v3; // edi
4    int v4; // esi
5    int v5; // edx
6    int v6; // eax
7    int v7; // ecx
8    int v8; // esi
9    int v9; // esi
10   int v10; // esi
11   int v11; // esi
12   _BYTE *v12; // ecx
13   int v13; // esi
14   int v15; // [esp+18h] [ebp+8h]
15
16   v3 = 0;
17   v4 = 0;
18   sub_401000();
19   v5 = a2 % 3;
20   v6 = a1;
21   v7 = a2 - a2 % 3;
22   v15 = a2 % 3;
23   if ( v7 > 0 )
24   {
25     do
26     {
27       LOBYTE(v5) = *(_BYTE *)(a1 + v3);
28       v3 += 3;
29       v8 = v4 + 1;
30       *(_BYTE *)(v8++ + a3 - 1) = byte_40E0A0[(v5 >> 2) & 0x3F];
31       *(_BYTE *)(v8++ + a3 - 1) = byte_40E0A0[16 * (*(_BYTE *)(a1 + v3 - 3) & 3)
32                                             + (((signed int)*(unsigned __int8 *)(a1 + v3 - 2) >> 4) & 0xF)];
33       *(_BYTE *)(v8 + a3 - 1) = byte_40E0A0[4 * (*(_BYTE *)(a1 + v3 - 2) & 0xF)
34                                           + (((signed int)*(unsigned __int8 *)(a1 + v3 - 1) >> 6) & 3)];
35       v5 = *(_BYTE *)(a1 + v3 - 1) & 0x3F;
36       v4 = v8 + 1;
```

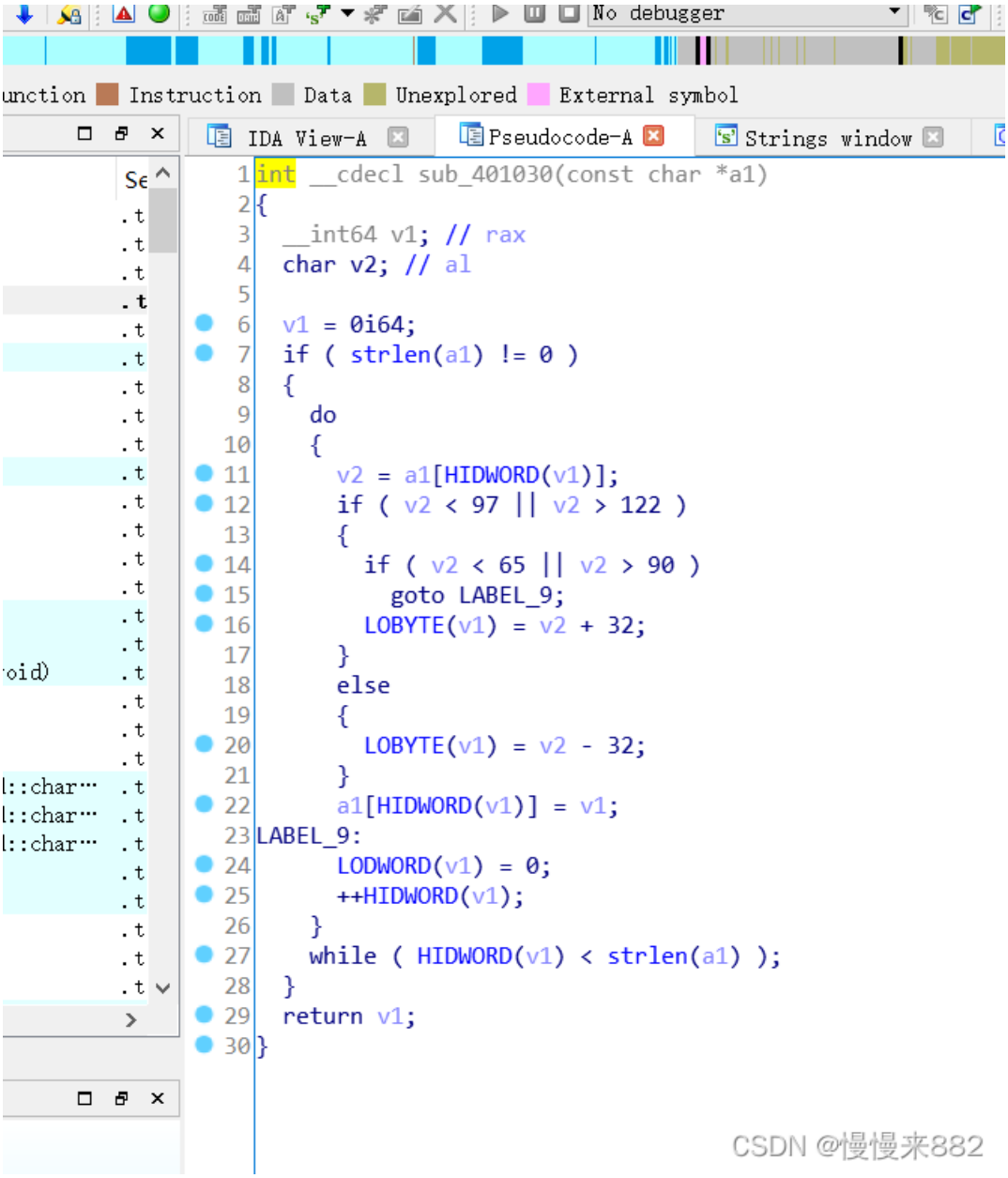
```
00001080 sub_401080:1 (401080)
```


base64但是里面还有一个sub_401000加密。

```
IDA View-A | Pseudocode-A | Strings window
```

```
1  signed int sub_401000()
2  {
3    signed int result; // eax
4    char v1; // cl
5
6    result = 6;
7    do
8    {
9      v1 = byte_40E0AA[result];
10     byte_40E0AA[result] = byte_40E0A0[result];
11     byte_40E0A0[result++] = v1;
12   }
13   while ( result < 15 );
14   return result;
15 }
```


里面是6到15位进行换位。



底下还有一个函数是大小写转换。写脚本。

```python
import base64

flag = ''; dict = {}; offset = 10
orgin = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
for i in range(len(orgin)):
    dict[orgin[i]] = orgin[i]
for i in range(6, 15): #sub_401000()
    dict[orgin[i]] , dict[orgin[i+offset]] = dict[orgin[i+offset]] , dict[orgin[i]] # 恢复base64密钥表
secret = 'zMXHz3TIgnxLxJhFAdtZn2fFk3lYCrtPC2l9'.swapcase() #sub_401030()
for i in range(len(secret)):
    flag += dict[secret[i]]
flag = base64.b64decode(flag)
print(flag)
```


得flag。

这题主要是变种的base64，还有大小写互换。