

# 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

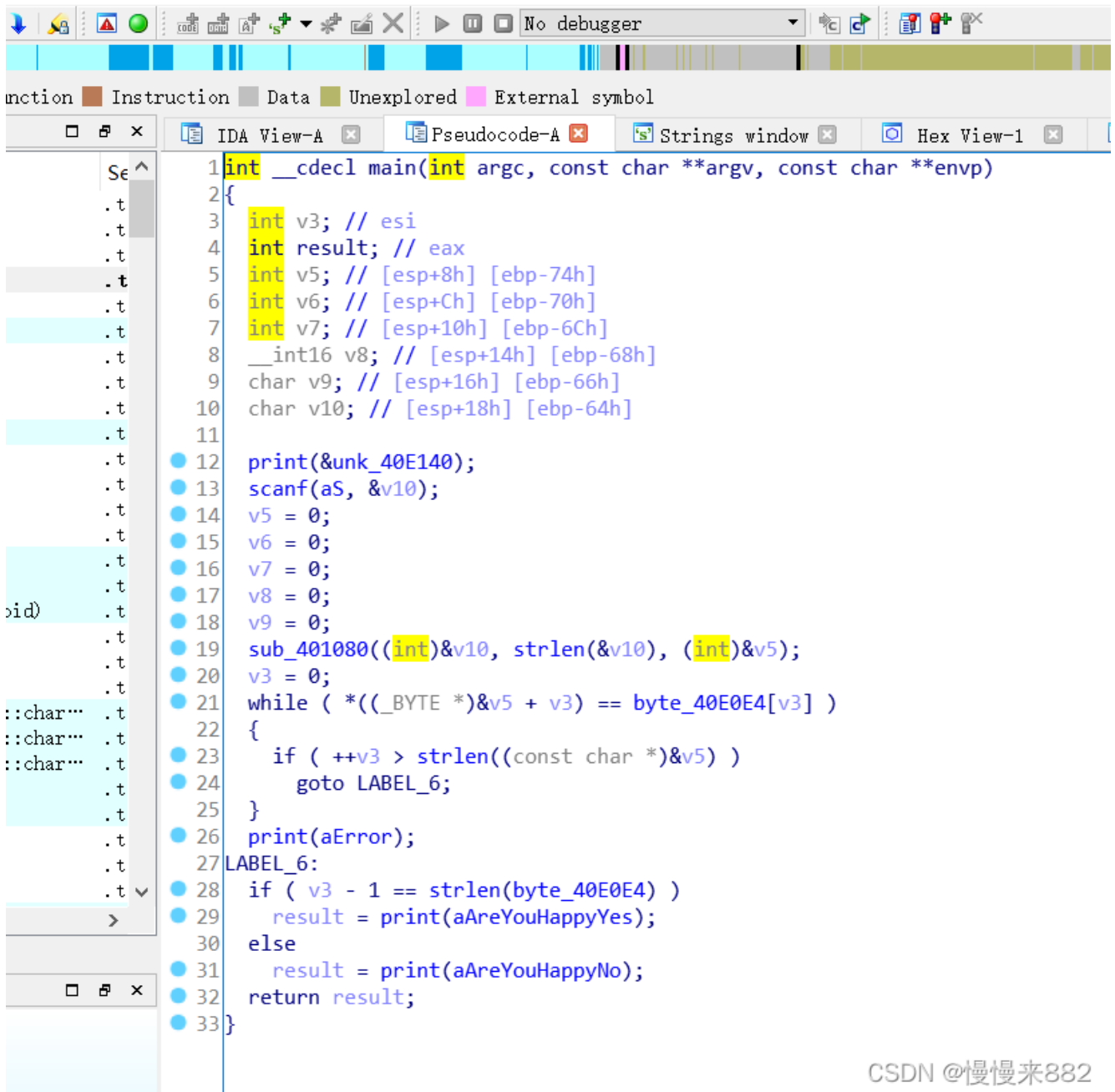
文章标签: 网络安全

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_60553183/article/details/122154512](https://blog.csdn.net/weixin_60553183/article/details/122154512)

版权

查后无壳 32位, 放入ida进入main, 进行小修小改



```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int v3; // esi
4     int result; // eax
5     int v5; // [esp+8h] [ebp-74h]
6     int v6; // [esp+Ch] [ebp-70h]
7     int v7; // [esp+10h] [ebp-6Ch]
8     __int16 v8; // [esp+14h] [ebp-68h]
9     char v9; // [esp+16h] [ebp-66h]
10    char v10; // [esp+18h] [ebp-64h]
11
12    print(&unk_40E140);
13    scanf(aS, &v10);
14    v5 = 0;
15    v6 = 0;
16    v7 = 0;
17    v8 = 0;
18    v9 = 0;
19    sub_401080((int)&v10, strlen(&v10), (int)&v5);
20    v3 = 0;
21    while ( *((_BYTE *)&v5 + v3) == byte_40E0E4[v3] )
22    {
23        if ( ++v3 > strlen((const char *)&v5) )
24            goto LABEL_6;
25    }
26    print(aError);
27 LABEL_6:
28    if ( v3 - 1 == strlen(byte_40E0E4) )
29        result = print(aAreYouHappyYes);
30    else
31        result = print(aAreYouHappyNo);
32    return result;
33 }
```

CSDN @慢慢来882

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)

```

CSDN @慢慢来882

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 }

```

CSDN @慢慢来882

里面是6到15位进行换位。

```

1 int __cdecl sub_401030(const char *a1)
2 {
3     __int64 v1; // rax
4     char v2; // al
5
6     v1 = 0i64;
7     if ( strlen(a1) != 0 )
8     {
9         do
10        {
11            v2 = a1[HIDWORD(v1)];
12            if ( v2 < 97 || v2 > 122 )
13            {
14                if ( v2 < 65 || v2 > 90 )
15                    goto LABEL_9;
16                LOBYTE(v1) = v2 + 32;
17            }
18            else
19            {
20                LOBYTE(v1) = v2 - 32;
21            }
22            a1[HIDWORD(v1)] = v1;
23        LABEL_9:
24            LODWORD(v1) = 0;
25            ++HIDWORD(v1);
26        }
27        while ( HIDWORD(v1) < strlen(a1) );
28    }
29    return v1;
30 }

```

CSDN @慢慢来882

底下还有一个函数是大小写转换。写脚本。

```

import base64

flag = ''; dict = {}; offset = 10
origin = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
for i in range(len(origin)):
    dict[origin[i]] = origin[i]
for i in range(6, 15): #sub_401000()
    dict[origin[i]] , dict[origin[i+offset]] = dict[origin[i+offset]] , dict[origin[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)

```

CSDN @慢慢来882

得flag。

这题主要是变种的base64，还有大小写互换。