

buuoj re逆向33-48题writeup(截图+c++源码+过程)

原创

[weixin_51275728](#) 于 2021-12-07 18:20:35 发布 2898 收藏

分类专栏: [ctfre](#) 文章标签: [c++](#) [安全](#) [信息安全](#) [反编译](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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_51275728/article/details/121773467

版权



[ctfre](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

Re

33-48

[33 xor](#)

[34xor](#)

[35 hello_world_go](#)

[36 igniteme](#)

[37 level3](#)

[38 crossfun](#)

[39 overlong](#)

[41 orgua](#)

[40 BJD hamburger competiton](#)

[42 challenge](#)

[43 base-re](#)

[44 easy strcmp](#)

[45 UniverseFinalAnswer](#)

[46 crackMe](#)

[47 level4](#)

[48 singal](#)

33 xor

33 xor 简单的二重循环，然后比较。记得把数据换成unsigned不然就是不行

The screenshot shows the IDA Pro interface with the following assembly code:

```
1: int64 __fastcall sub_400686(unsigned int *a1, _DWORD *a2)
2: {
3:     int64 result; // rax
4:     unsigned int v3; // [rsp+1Ch] [rbp-24h]
5:     unsigned int v4; // [rsp+20h] [rbp-20h]
6:     int v5; // [rsp+24h] [rbp-1Ch]
7:     unsigned int i; // [rsp+28h] [rbp-18h]
8:
9:     v3 = *a1;
10:    v4 = a1[1];
11:    v5 = 0;
12:    for ( i = 0; i <= 0x3F; ++i )
13:    {
14:        v5 += 0x458BCD42;
15:        v3 += (v4 + v5 + 11) ^ ((v4 << 6) + *a2) ^ ((v4 >> 9) + a2[1]) ^ 0x20;
16:        v4 += (v3 + v5 + 20) ^ ((v3 << 6) + a2[2]) ^ ((v3 >> 9) + a2[3]) ^ 0x10;
17:    }
18:    *a1 = v3;
19:    result = v4;
20:    a1[1] = v4;
21:    return result;
22: }
```

The terminal window shows the following Python code and output:

```
命令提示符 - python
Microsoft Windows [版本 10.0.19043.1348]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\lenovo>python
Python 3.10.0 (tags/v3.10.0:b494f59, Oct 4 2021, 19:00:18) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> from z3 import *
>>> s=Solver()
>>> x1=Int('x1')
>>> x2=Int('x2')
>>> x3=Int('x3')
>>> s.add(x1-x2-2225223423)
>>> File "<stdin>", line 1
>>> s.add(x1-x2-2225223423)
>>> s.add(x1-x3==1121399208)
>>> s.add(x2+x3==4201428739)
>>> s.check()
sat
>>> s.model()
[x1 = 3774025685, x2 = 1548802262, x3 = 2652626477]
>>>
```

```
#include <iostream>
using namespace std;
int main(){
unsigned int a2[4]={2,2,3,4};
unsigned int a1[6]={0xDF48EF7E,0x20CAACF4,3774025685,1548802262,2652626477,0x84F30420};
for(int j=0;j<=4;j+=2){
unsigned int v3 = a1[j];
unsigned int v4 = a1[1+j];
int v5 = 0x458BCD42*64;
for ( int i = 0; i <= 0x3F; ++i )
{ v4 -= (v3 + v5 + 20) ^ ((v3 << 6) + a2[2]) ^ ((v3 >> 9) + a2[3]) ^ 0x10;
v3 -= (v4 + v5 + 11) ^ ((v4 << 6) + a2[0]) ^ ((v4 >> 9) + a2[1]) ^ 0x20;
v5 -= 0x458BCD42;}
a1[j] = v3;
a1[1+j] = v4;
}for(int i=0;i<6;i++)
cout<<hex<<a1[i];
cout<<endl;
for (int i = 0; i < 6; i++)
printf("%c%c%c", *((char*)&a1[i]+2), *((char*)&a1[i] + 1), *((char*)&a1[i]));
}
```

34xor

34 xor 就是简单的异或

IDA - xor.exe C:\Users\lenovo\AppData\Local\Temp\Rar\$DRa12468.1884\xor.exe

File Edit Jump Search View Debugger Options Windows Help

The screenshot shows the IDA Pro interface with the following components:

- Functions window:** Lists various functions such as `sub_401000`, `sub_401010`, `sub_401020`, `sub_401050`, `sub_401090`, `sub_40112F`, `sub_4011DA`, `sub_4011E2`, `start`, `sub_401380`, `sub_4013A8`, `sub_4014A1`, `sub_4014E5`, `sub_401517`, `sub_401550`, `sub_4015D7`, `sub_40166B`, `sub_401688`, `sub_4016B0`, `sub_4016D0`, `sub_4016F2`, `sub_40173F`, `sub_40178A`, `sub_40178D`, `sub_401791`, `sub_401797`, `sub_4017A3`, `sub_4017A6`, `nullsub_1`, `sub_4017C8`, `sub_4017E5`, `sub_4017F1`, `sub_4017F7`, and `sub_4017FD`.
- Instruction window:** Shows assembly instructions and their data references. Key instructions include:
 - `fld_41E9C0` (float) with value `4.2949673e9`
 - `flt_41E9C4` (float) with value `9.223372e18`
 - `flt_41E9C8` (float) with value `-6.8056469e38`
 - `aGiveMeYourFlag` (db) with string `'Give Me Your Flag String:',0Ah,0`
 - `aS` (db) with string `'%',0`
 - `aWrong` (db) with string `'Wrong!',0Ah,0`
 - `aPause` (db) with string `'pause',0`
 - `aRight` (db) with string `'Right!',0Ah,0`
 - `byte_41EA08` (db) with value `4Dh`
 - `aSawbFxzJTqjNBp` (db) with string `'SAWB~FXZ:J:`tQJ`N@ bpdd}8g',0`
- Output window:** Shows messages from the decompiler:

```
409DF3: using guessed type int sub_409DF3(void);
409DF9: using guessed type int sub_409DF9(void);
420BCC: using guessed type int dword_420BCC;
```

```
#include <iostream>
using namespace std;
int main(){
    string a="MSAWB~FXZ:J:`tQJ`N@ bpdd}8g";
    for(int i=0;i<a.length();i++)
    {
        char p=(a[i]^i);
        cout<<p;}
}
```

35 hello_world_go

35 hello_world_go 明码

IDA - hello_world_go C:\Users\lenovo\AppData\Local\Temp\Rar\$DRa15800.32761\hello_world_go

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unexcolored External symbol

Functions window

Function name	Address	Disassembly
fnt_ss_consume	.rodata:0000000004D3C43	db 62h ; b
fnt_ss_peek	.rodata:0000000004D3C44	db 65h ; e
fnt_ss_notEOF	.rodata:0000000004D3C45	db 20h
fnt_ss_okVerb	.rodata:0000000004D3C46	db 74h ; t
fnt_ss_scanBool	.rodata:0000000004D3C47	db 72h ; r
fnt_ss_getBase	.rodata:0000000004D3C48	db 61h ; a
fnt_ss_scanNumber	.rodata:0000000004D3C49	db 63h ; c
fnt_ss_scanRune	.rodata:0000000004D3C4A	db 65h ; e
fnt_ss_scanBasePrefix	.rodata:0000000004D3C4B	db 47h ; G
fnt_ss_scanInt	.rodata:0000000004D3C4C	db 43h ; C
fnt_ss_scanUint	.rodata:0000000004D3C4D	db 53h ; S
fnt_ss_floatToken	.rodata:0000000004D3C4E	db 77h ; w
fnt_ss_complexTokens	.rodata:0000000004D3C4F	db 65h ; e
fnt_hasX	.rodata:0000000004D3C50	db 65h ; e
fnt_ss_convertFloat	.rodata:0000000004D3C51	db 70h ; p
fnt_ss_scanComplex	.rodata:0000000004D3C52	db 53h ; S
fnt_ss_convertString	.rodata:0000000004D3C53	db 74h ; t
fnt_ss_quotedString	.rodata:0000000004D3C54	db 61h ; a
fnt_ss_hexByte	.rodata:0000000004D3C55	db 72h ; r
fnt_ss_hexString	.rodata:0000000004D3C56	db 74h ; t
fnt_ss_scanOne	.rodata:0000000004D3C57	
fnt_errorHandler	.rodata:0000000004D3C58	aFlagHelloWorld db 'flag{hello_world_gogogo}'
fnt_ss_advance	.rodata:0000000004D3C59	; DATA XREF: main_main:loc_49A40A70
fnt_ss_doScanf	.rodata:0000000004D3C5A	; main_main+25Cf0
fnt_glob_func1	.rodata:0000000004D3C5B	
fnt_glob_func2	.rodata:0000000004D3C5C	
fnt_ss_Token_func1	.rodata:0000000004D3C5D	aFunctionNotImp db 'function not implementedgcDrainN phase incorrecth'
fnt_init	.rodata:0000000004D3C5E	db 61h ; a
type_hash_fmt_fmt	.rodata:0000000004D3C5F	db 73h ; s
type_eq_fmt_fmt	.rodata:0000000004D3C60	db 68h ; h
type_hash_fmt_readRune	.rodata:0000000004D3C61	db 20h
type_eq_fmt_readRune	.rodata:0000000004D3C62	db 20h
type_hash_fmt_ssаве	.rodata:0000000004D3C63	db 6Fh ; o
type_eq_fmt_ssаве	.rodata:0000000004D3C64	db 66h ; f
main_main	.rodata:0000000004D3C65	db 20h

Line 1967 of 1967 000D3C70 0000000004D3C70: .rodata:aFunctionNotImp (Synchronized with Hex View-1)

Output window

```
4EBDA0: using guessed type void *go_itab__os_File_io_Writer;
577548: using guessed type __int64 os_Stdin;
577550: using guessed type __int64 os_Stdout;
```

Python

AU: idle Down Disk: 61GB CSDN @weixin_51275728

36 igniteme

36 Igniteme,取了点巧,最后一位为m

IDA - IgniteMe.exe C:\Users\lenovo\AppData\Local\Temp\Rar\$DRa16256.10705\IgniteMe.exe

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unexcolored External symbol

Functions window

Function name	Address	Disassembly
sub_401000		
sub_401020		
sub_401050		
sub_4010F0		
start		

```
1 signed int sub_401050()
2 {
3     int v0; // ST04_4
4     int i; // [esp+4h] [ebp-8h]
5     unsigned int j; // [esp+4h] [ebp-8h]
6     char v4; // [esp+8h] [ebp-1h]
7
8     v0 = sub_401020((int)byte_403078);
9     v4 = sub_401000();
10    for ( i = v0 - 1; i >= 0; --i )
11    {
12        byte_403180[i] = v4 ^ byte_403078[i];
13        v4 = byte_403078[i];
14    }
15    for ( j = 0; j < 0x27; ++j )
16    {
17        if ( byte_403180[j] != (unsigned __int8)byte_403000[j] )
18            return 0;
19    }
20    return 1;
21 }
```

0000045B sub_401050:8 (40105B)

Output window

```
4010F0: using guessed type char Buffer[260];
401050: using guessed type int __cdecl sub_401050(DWORD);
401000: using guessed type int sub_401000(void);
```

Python

AU: idle Down Disk: 61GB CSDN @weixin_51275728

```
#include <iostream>
#include <Windows.h>
using namespace std;
int main(){
int v4=0x69^'m';
unsigned char ida_chars[] =
{
    0x0D, 0x26, 0x49, 0x45, 0x2A, 0x17, 0x78, 0x44, 0x2B, 0x6C,
    0x5D, 0x5E, 0x45, 0x12, 0x2F, 0x17, 0x2B, 0x44, 0x6F, 0x6E,
    0x56, 0x09, 0x5F, 0x45, 0x47, 0x73, 0x26, 0x0A, 0x0D, 0x13,
    0x17, 0x48, 0x42, 0x01, 0x40, 0x4D, 0x0C, 0x02, 0x69
};
for(int i=0x26;i>=0;i--)
{for(int j=1;j<128;j++){
    char p=j^v4;
    {if(p!=ida_chars[i])
    continue;
    }
    char pp=j;
    cout<<pp;
    v4=j;
    break; } }
}
```

37 level3

37 level3 变表的base64,但我先开始没看出来哪里变了。就翻init,然后有发现

The screenshot displays a Windows desktop environment with three main windows:

- IDA Pro (top):** Shows the disassembly of a C++ program. The main function is visible, containing a call to `base64_encode(&v6)`. The output window shows the execution of this function, with the message: `00000BBB main:15 (400BBB)`.
- C++ IDE (middle):** Shows the source code of `base64.cpp`. The `main` function is defined, which reads a string from a file and prints it. The string is: `TSRQPONMLKJIHGFCBAUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-`.
- Base64 Decoder (bottom right):** A tool titled "加密解密小玩具 Ver0.2 by Lucky_789". It has tabs for RSA, AES, Base64, Base32, SHA, MD5, and RC4. The Base64 tab is selected. The input field contains the string: `wotf2020{Base64_is_the_start_of_reverse}`. The output field shows the decoded result: `d2G0ZjLwHjS7Dm0zZAY0X2lX3CoZV9zdNOy09vZl9yZXZlcnG1fd=`.

38 crossfun

38 crossfun 嵌套函数哈哈

IDA Pro interface showing assembly code for a function named `iven_is_handsome`. The code is as follows:

```
1  BOOL8 __fastcall iven_is_handsome(_BYTE *a1)
2  {
3      return a1[10] == 112
4         && a1[13] == 64
5         && a1[3] == 102
6         && a1[26] == 114
7         && a1[20] == 101
8         && (unsigned int)iven_is_c00l(a1);
9  }
```

The output window shows the following warnings:

```
1461: using guessed type __int64 __fastcall check(_QWORD);
13EC: using guessed type __int64 __fastcall iven_is_handsome(_QWORD);
1377: using guessed type __int64 __fastcall iven_is_c00l(_QWORD);
```

```
#include <iostream>
using namespace std;
int main(){
char a1[33];
a1[10] = 'p';
    a1[13] = '@';
    a1[3] = 'f';
    a1[26] = 'r';
    a1[20] = 'e';
a1[7] = 48;
    a1[16] = 95;
    a1[11] = 112;
    a1[23] = 101;
    a1[30] = 117;
    a1[0] = 119 , a1[6] = 50 , a1[22] = 115 , a1[31] = 110 ,a1[12] = 95;
    a1[15] = 100;
    a1[8] = 123;
    a1[18] = 51;
    a1[28] = 95;
    a1[21] = 114;
    a1[2] = 116;
    a1[9] = 99;
a1[32] = 125;
a1[19] = 118;
    a1[5]= 48;
a1[14] = 110;
    a1[4] = 50, a1[17] = 114, a1[29] = 102 , a1[17] = 114 , a1[24] = 95;
    a1[1] = 99, a1[25] = 64;
a1[27] = 101;
cout<<a1;
}
```

39 overlong

39 overlong 直接转成c++,分析发现输出字符短了。答案：我就是死也不会告诉你答案：真香
哈哈

```
#include <iostream>
#include <Windows.h>
using namespace std;
int sub_401000(char *a1,unsigned char * a2){
int v3; // [esp+0h] [ebp-8h]
int v4; // [esp+4h] [ebp-4h]

if ( *a2 >> 3 == 30 )
{
v4 = a2[3] & 0x3F | ((a2[2] & 0x3F) << 6) | ((a2[1] & 0x3F) << 12) | ((*a2 & 7) << 18);
v3 = 4;
}
else if ( *a2 >> 4 == 14 )
{
v4 = a2[2] & 0x3F | ((a2[1] & 0x3F) << 6) | ((*a2 & 0xF) << 12);
v3 = 3;
}
else if ( *a2 >> 5 == 6 )
{
v4 = a2[1] & 0x3F | ((*a2 & 0x1F) << 6);
v3 = 2;
}
else
{
v4 = *a2;
v3 = 1;
}
*a1 = v4;
return v3;}
int sub_401160( char *a1, unsigned char *a2, int a3)
{
int v3; // ST08_4
unsigned int i; // [esp+4h] [ebp-4h]

for ( i = 0; i < a3; ++i )
{
a2 += sub_401000(a1, a2);
v3 = *a1++;
if ( !v3 )
break;
}
return i;}
int main(){
unsigned char ida_chars[] =
{
0xE0, 0x81, 0x89, 0xC0, 0xA0, 0xC1, 0xAE, 0xE0, 0x81, 0xA5,
0xC1, 0xB6, 0xF0, 0x80, 0x81, 0xA5, 0xE0, 0x81, 0xB2, 0xF0,
0x80, 0x80, 0xA0, 0xE0, 0x81, 0xA2, 0x72, 0x6F, 0xC1, 0xAB,
0x65, 0xE0, 0x80, 0xA0, 0xE0, 0x81, 0xB4, 0xE0, 0x81, 0xA8,
0xC1, 0xA5, 0x20, 0xC1, 0xA5, 0xE0, 0x81, 0xAE, 0x63, 0xC1,
0xAF, 0xE0, 0x81, 0xA4, 0xF0, 0x80, 0x81, 0xA9, 0x6E, 0xC1,
0xA7, 0xC0, 0xBA, 0x20, 0x49, 0xF0, 0x80, 0x81, 0x9F, 0xC1,
0xA1, 0xC1, 0x9F, 0xC1, 0x8D, 0xE0, 0x81, 0x9F, 0xC1, 0xB4,
0xF0, 0x80, 0x81, 0x9F, 0xF0, 0x80, 0x81, 0xA8, 0xC1, 0x9F,
```

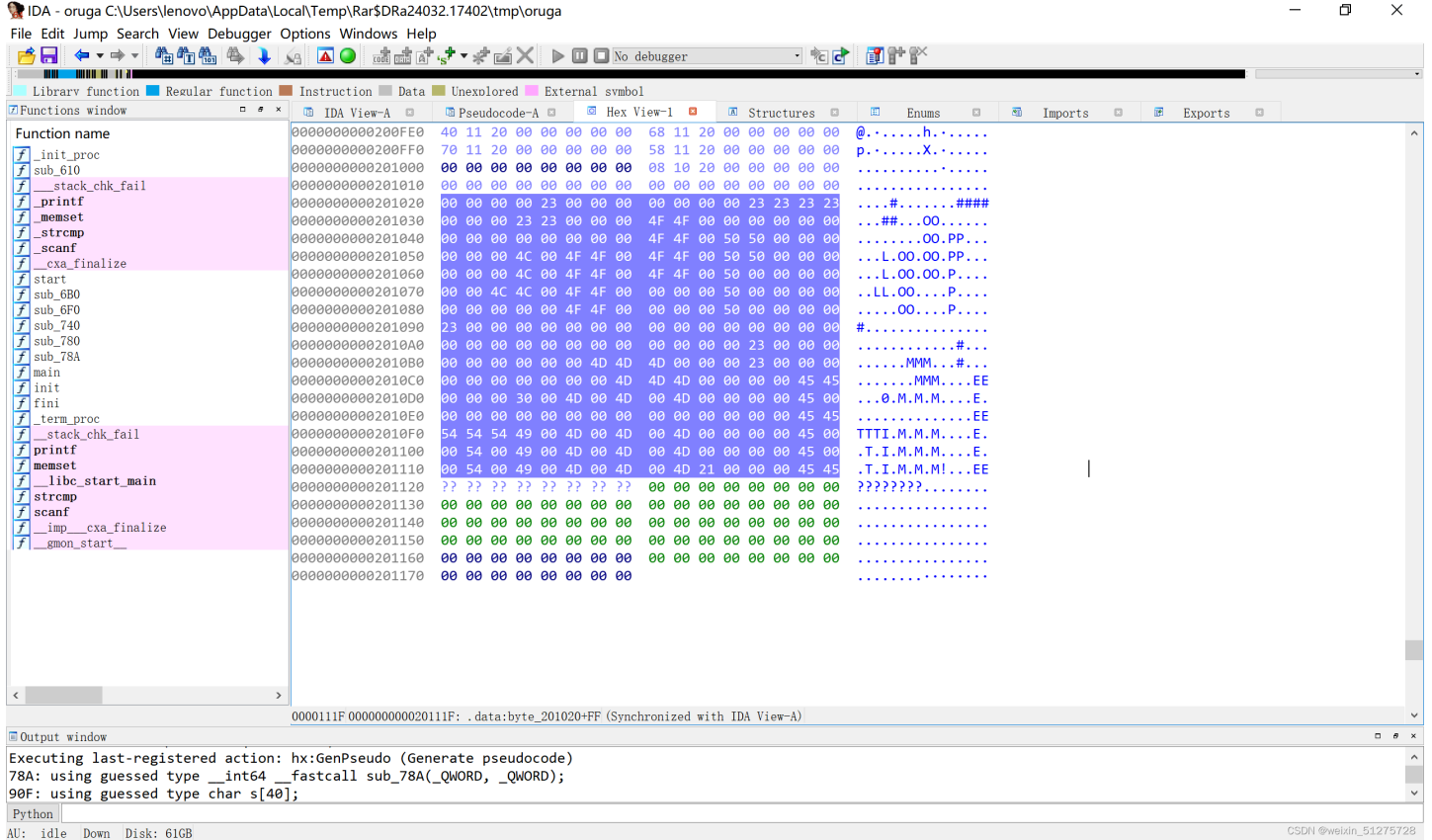
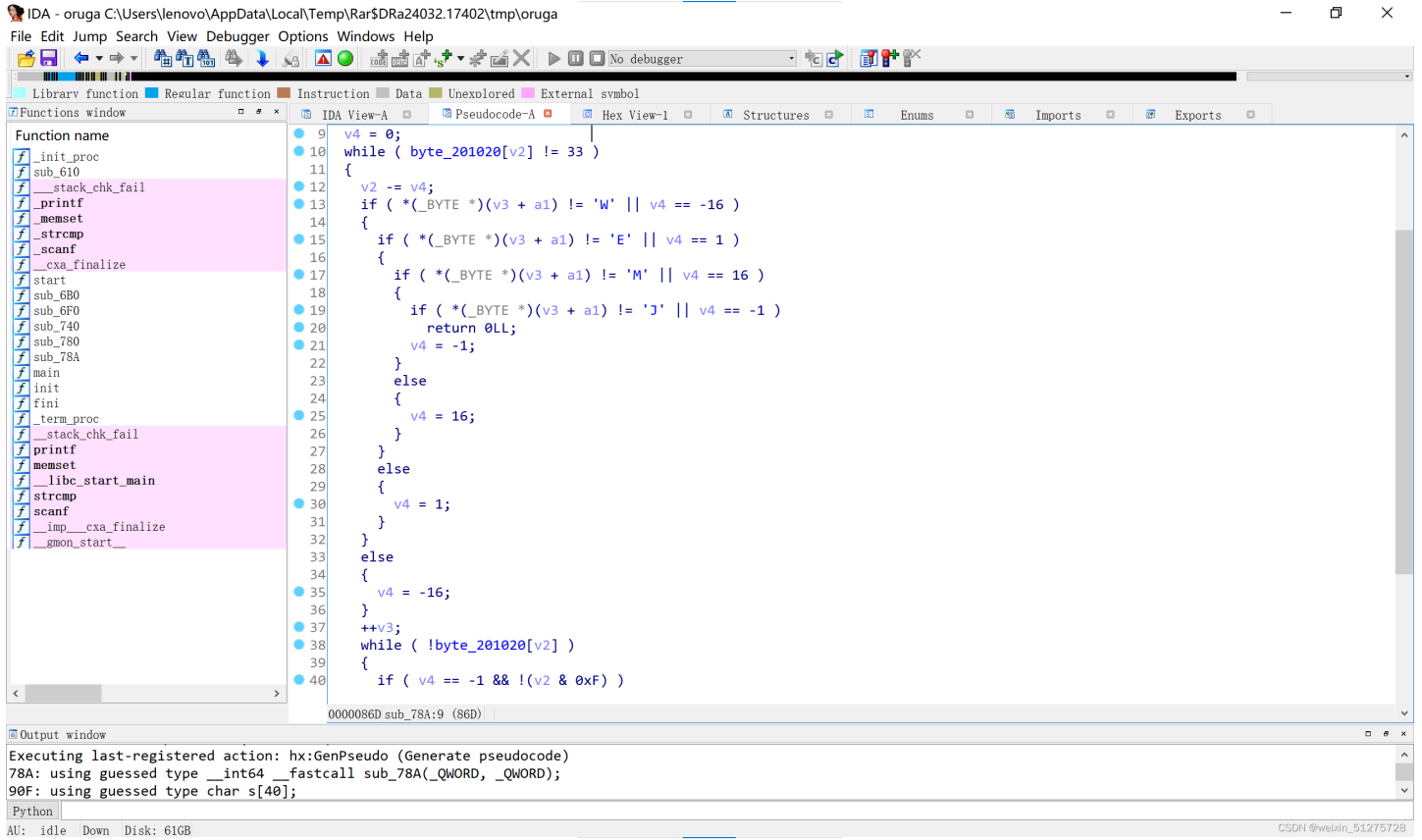


```
0xF0, 0x80, 0x81, 0xA5, 0xE0, 0x81, 0x9F, 0xC1, 0xA5, 0xE0,
0x81, 0x9F, 0xF0, 0x80, 0x81, 0xAE, 0xC1, 0x9F, 0xF0, 0x80,
0x81, 0x83, 0xC1, 0x9F, 0xE0, 0x81, 0xAF, 0xE0, 0x81, 0x9F,
0xC1, 0x84, 0x5F, 0xE0, 0x81, 0xA9, 0xF0, 0x80, 0x81, 0x9F,
0x6E, 0xE0, 0x81, 0x9F, 0xE0, 0x81, 0xA7, 0xE0, 0x81, 0x80,
0xF0, 0x80, 0x81, 0xA6, 0xF0, 0x80, 0x81, 0xAC, 0xE0, 0x81,
0xA1, 0xC1, 0xB2, 0xC1, 0xA5, 0xF0, 0x80, 0x80, 0xAD, 0xF0,
0x80, 0x81, 0xAF, 0x6E, 0xC0, 0xAE, 0xF0, 0x80, 0x81, 0xA3,
0x6F, 0xF0, 0x80, 0x81, 0xAD, 0x00
};

unsigned int v4; // eax
char Text[128]; // [esp+0h] [ebp-84h]
unsigned int v7; // [esp+80h] [ebp-4h]
v4 = sub_401160(Text, ida_chars, 180); //180换成其他数也行
v7 = v4;
Text[v4] = 0;
MessageBoxA(0, Text, "Output", 0);
return 0;
}
```

41 orgua

41 orgua 不知道大家有没有玩过三月之庭，看到图时我感觉很熟悉



就是说走一个方向时在遇到障碍物前不会停，最后到感叹号。最开始在左上角。就一个迷宫，也想难倒我？然后卡了十多分钟。。。血压都上来了。

40 BJD hamburger competition

40 [BJDCTF2020]BJD hamburger competition



www.ttmads.com/nasn.php?type=3

中文 | English | Россия 未登录 首页 在线解密 免费批量解密工具 会员中心

TTMads

广告位长期招租

QQ: 1878399009 定位精准用户 多关键词百度首页

常用哈希加密解密 >> sha1在线加密 | sha1在线解密

DD01903921EA24941C26A48F2CEC24E0BB0E8CC7

在线加密
在线解密

解密成功, 结果是: 1001

备案号: 闽ICP备16008567号-1
 ttmads@yahoo.com QQ:1878399009 md5互助群:303488034
 友情链接: 上班摸鱼神器-单行阅读器 奇乐浓浓小说网 SecSilo 华域联盟 Mrxn's Blog 七行者博客 Arvin's Blog

dnSpy v6.1.8 (32-bit, .NET Framework)

程序集资源管理器

- ButtonEat(): void @06000005
- CancelEat(): void @06000002
- FinalEat(): void @06000003
- PlayAudio(): void @06000004
- TryEat(): void @06000001
- audioSource: AudioSource @04000002
- tryMenu: GameObject @04000001
- ButtonHoldRotate @02000003
- ButtonSpawnFruit @02000004
 - 基类和接口
 - 派生类型
 - ButtonSpawnFruit(): void @0600000D
 - Md5(string): string @0600000A
 - Sha1(string): string @0600000B
 - Spawn(): void @0600000C
 - audioSources: AudioSource[] @04000007
 - result: string @04000008
 - spawnCount: int @04000006
 - toSpawn: GameObject @04000005
- ButtonSwitchMenu @02000005
- CameraZoom @0200000F
- DestroyerBorder @02000006
- FruitSpawner @02000007
- GameControllerScript @02000008
- HoldUIPos @02000009
- IgnoreRb @0200000A
- Init @0200000B

ButtonSpawnFruit X

```

77 Init.secret = 87;
78 }
79 else if (name == "汉堡顶" && Init.spawnCount == 5)
80 {
81     Init.secret = 127;
82     string str = Init.secret.ToString();
83     if (ButtonSpawnFruit.Sha1(str) == "DD01903921EA24941C26A48F2CEC24E0BB0E8CC7")
84     {
85         this.result = "BJDCTF{" + ButtonSpawnFruit.Md5(str) + "}";
86         Debug.Log(this.result);
87     }
88 }
89 Init.spawnCount++;
90 Debug.Log(Init.secret);
91 Debug.Log(Init.spawnCount);
92 }
93 }
94
  
```

局部变量

名称	值	类型

在这里输入你要搜索的内容

22:28 2021/12/6 12:73:08

dnSpy v6.1.8 (32-bit, .NET Framework)

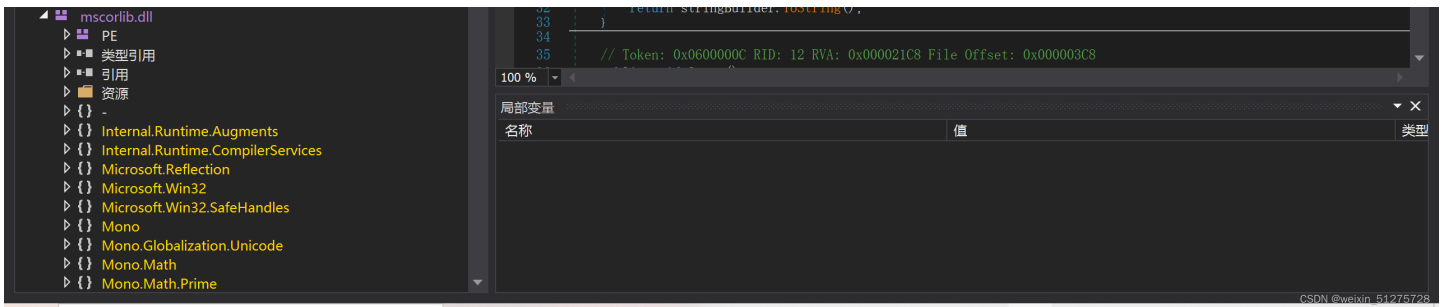
程序集资源管理器

- ButtonSpawnFruit @02000004
 - 基类和接口
 - 派生类型
 - ButtonSpawnFruit(): void @0600000D
 - Md5(string): string @0600000A
 - Sha1(string): string @0600000B
 - Spawn(): void @0600000C
 - audioSources: AudioSource[] @04000007
 - result: string @04000008
 - spawnCount: int @04000006
 - toSpawn: GameObject @04000005
- ButtonSwitchMenu @02000005
- CameraZoom @0200000F
- DestroyerBorder @02000006
- FruitSpawner @02000007
- GameControllerScript @02000008
- HoldUIPos @02000009
- IgnoreRb @0200000A
- Init @0200000B
- InterfaceQuit @0200000C
- MenuSwitch @0200000D
- WorldUI @0200000E
- netstandard (2.0.0.0)
- mscorlib (4.0.0.0)

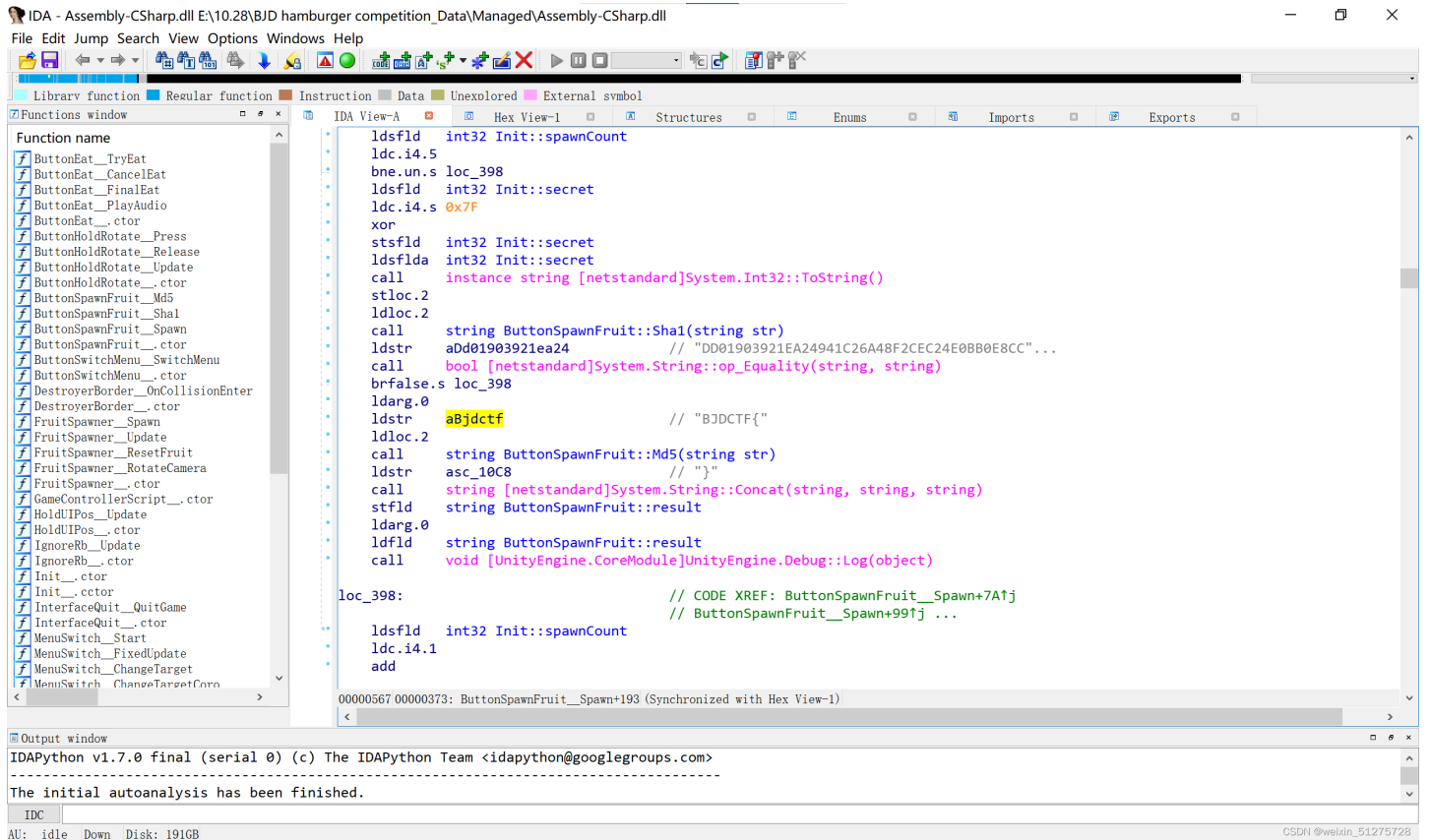
ButtonSpawnFruit X

```

5
6 // Token: 0x02000004 RID: 4
7 public class ButtonSpawnFruit : MonoBehaviour
8 {
9     // Token: 0x0600000A RID: 10 RVA: 0x00002110 File Offset: 0x00000310
10     public static string Md5(string str)
11     {
12         byte[] bytes = Encoding.UTF8.GetBytes(str);
13         byte[] array = MD5.Create().ComputeHash(bytes);
14         StringBuilder stringBuilder = new StringBuilder();
15         foreach (byte b in array)
16         {
17             stringBuilder.Append(b.ToString("X2"));
18         }
19         return stringBuilder.ToString().Substring(0, 20);
20     }
21
22     // Token: 0x0600000B RID: 11 RVA: 0x00002170 File Offset: 0x00000370
23     public static string Sha1(string str)
24     {
25         byte[] bytes = Encoding.UTF8.GetBytes(str);
26         byte[] array = SHA1.Create().ComputeHash(bytes);
27         StringBuilder stringBuilder = new StringBuilder();
28         foreach (byte b in array)
29         {
30             stringBuilder.Append(b.ToString("X2"));
31         }
32         return stringBuilder.ToString();
33     }
34 }
  
```



这道题第一次做时不会，ida不行啊。



看别人题解才知道要用dnspy.而且代码要看全

Sha解密后md5加密

应该是转换大写了,且读取20个字符。

42 challenge

42 challenge base64 变表

The screenshot shows IDA Pro's disassembly window for a function named `main`. The instruction list includes several `db` (data byte) instructions, with the last one being `db 'ZYXABC'`. A dialog box titled "加密解密小玩具 Ver0.2 by Lucky_789" is open, showing encryption options. The "Base64" option is selected. The "字符串" (Strings) tab is active, displaying a list of strings including `ZYXABCDEF...xyzabcdefg...` and `sh00ting_phish_in_a_barrel@flare-on.com`. The "明文" (Plaintext) field is empty, and the "密文" (Ciphertext) field contains `x2dtJE0myjacxDemx2eozT5cVSS9FYUGvWTzWjuexjRgy24rV29q`. The "加密" (Encrypt) button is highlighted.

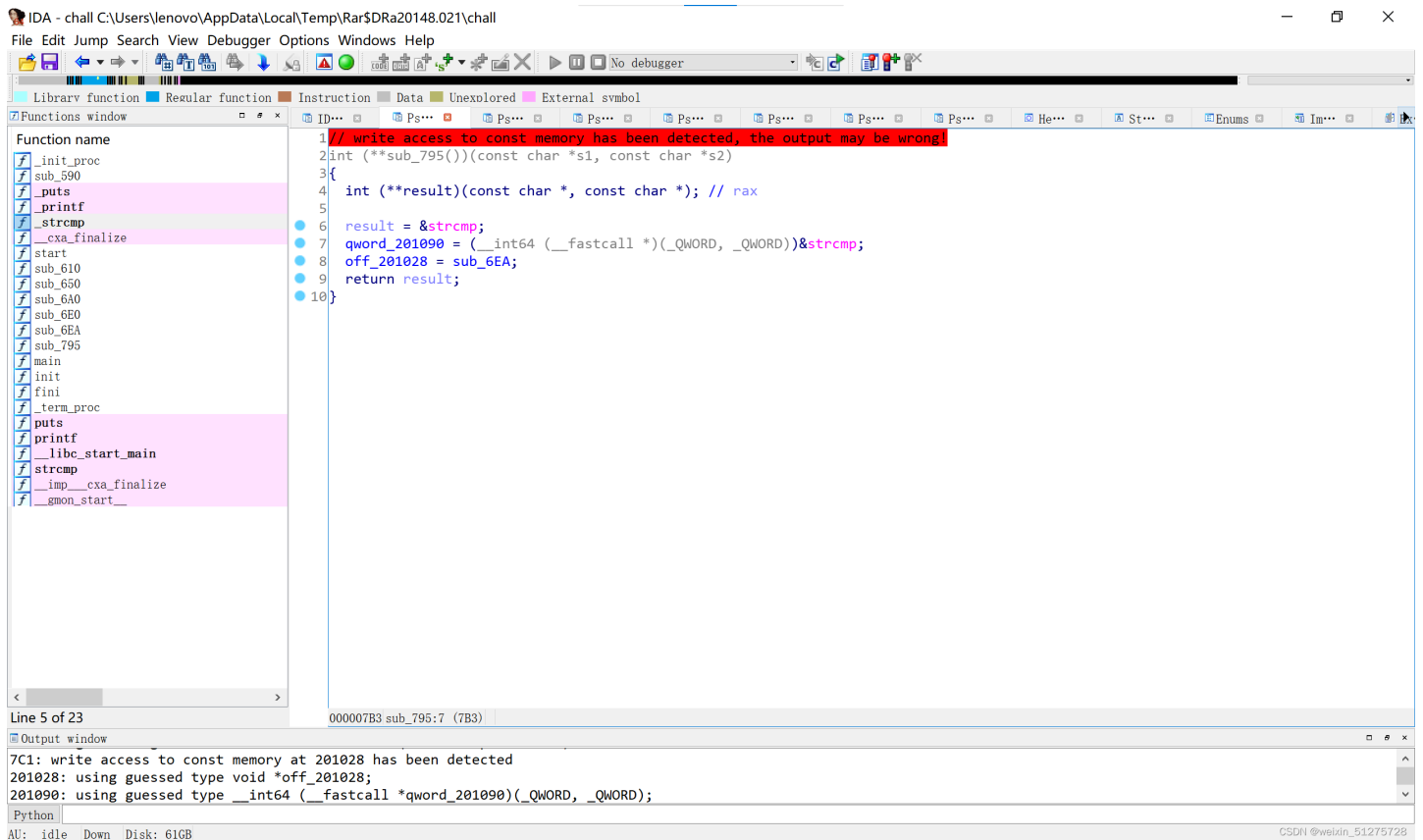
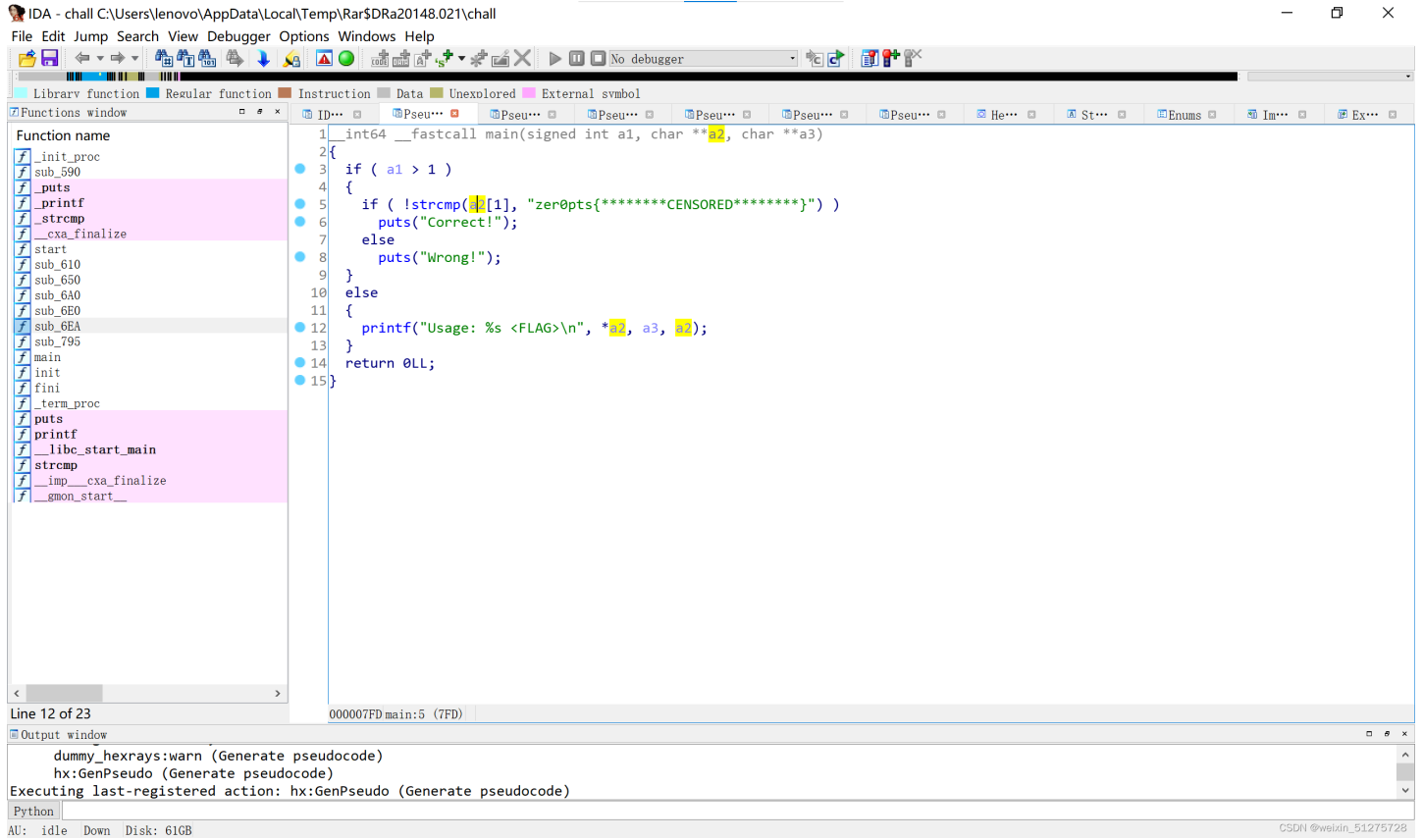
43 base-re

43 base-re 明码

The screenshot shows IDA Pro's disassembly window for a function named `main`. The instruction list includes several `db` (data byte) instructions, with the last one being `db 'ZYXABC'`. A dialog box titled "加密解密小玩具, 仅供娱乐(^_^) by Lucky_789 2014年11月" is open, showing encryption options. The "Base64" option is selected. The "字符串" (Strings) tab is active, displaying a list of strings including `ZYXABCDEF...xyzabcdefg...` and `sh00ting_phish_in_a_barrel@flare-on.com`. The "明文" (Plaintext) field is empty, and the "密文" (Ciphertext) field contains `x2dtJE0myjacxDemx2eozT5cVSS9FYUGvWTzWjuexjRgy24rV29q`. The "加密" (Encrypt) button is highlighted.

44 easy strcmp

44[Zer0pts2020]easy strcmp 一点都不easy 找了半天没找到,我就乱翻函数



201090->795

201028->6ea

```
#include < iostream>
using namespace std;
int main(){
    string p="zer0pts{*****CENSORED*****}";
    char a[24]={ 0x42, 0x09,
        0x4A, 0x49, 0x35, 0x43, 0x0A, 0x41, 0xF0, 0x19, 0xE6, 0x0B,
        0xF5, 0xF2, 0x0E, 0x0B, 0x2B, 0x28, 0x35, 0x4A, 0x06, 0x3A,
        0x0A, 0x4f};
    for(int i=0;i<24;i++){
        p[i+8]+=a[i];
    }
    cout<<p;}

```

45 UniverseFinalAnswer


```

49  *(&v15 + v4++) = v10;
50  a1 = v4;
51  v10 = 0;
52  }
53  }++v7;
54  }
55  while ( v6 < 8 )
56  {
57  v11 += byte_416050[++v12];
58  v13 = byte_416050[v12];
59  v8 = byte_416050[v11];
60  byte_416050[v11] = v13;
61  byte_416050[v12] = v8;
62  if ( *( _DWORD *) ( __readfsdword( 0x30u ) + 104 ) & 0x70 )
63  {
64  v13 = v11 + v12;
65  *(&v17 + v6) = byte_416050[ ( unsigned __int8 ) ( v8 + v13 ) ] ^ *(&v15 + v5);
66  if ( *( _DWORD *) ( __readfsdword( 0x30u ) + 2 ) & 0xFF )
67  {
68  v11 = '+';
69  v12 = '+';
70  }
71  sub_401710( ( int ) &v17, ( const char * ) a2, v6++ );
72  v5 = v6;
73  if ( v6 >= ( unsigned int ) ( &v15 + strlen( &v15 ) + 1 - &v16 ) )
74  v5 = 0;
75  }
76  v14 = 0;
77  sub_401470( a1, &v17, &v14 );
78  return v14 == 0xAB94;
}

```

Line 3 of 276 00000F2F sub_401830:67 (401B2F)

Output window

```

414000: using guessed type void *off_414000;
401251: inconsistent fpu stack
401710: using guessed type _DWORD __cdecl sub_401710( _DWORD, _DWORD, _DWORD );

```

Python

AU: idle Down Disk: 190GB CSDN @weixin_51275728

351a2f05-3848-4de6-9c9d-6e28c946f079.exe - PID: 5772 - 模块: 351a2f05-3848-4de6-9c9d-6e28c946f079.exe - 线程: 主线程 12568 - x32dbg

文件(F) 视图(V) 调试(D) 跟踪(X) 插件(P) 收藏夹(I) 选项(O) 帮助(H) Nov 3 2021 (TitanEngine)

CPU 日志 笔记 断点 跟踪 内存布局 调用堆栈 SEH链 脚本 符号 源代码 线程 句柄 跟踪 MapoAnalyzer

隐藏FPU

```

EAX 00000012
EBX 00000004
ECX 000000C0 'i'
EDX 00000000
EBP 003CF850 '&"剥<'
ESP 003CF80C
ESI 00C32715 "怪M"
EDI 1E8478F8
ETP 00C31B3E 351a2f05-3848-4de6-9c9d-6e28c946f079.00
EFLAGS 00000304
ZF 0 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1

```

ST(0) 00000000000000000000000000000000 x87r0 空 0.00000000000000000000000000000000
ST(1) 00000000000000000000000000000000 x87r1 空 0.00000000000000000000000000000000

默认 (stdcall) 5 解锁

```

1: [esp+4] 00000000
2: [esp+8] 003CF65 "2345678"
3: [esp+C] 00000004
4: [esp+10] 00000008
5: [esp+14] 003CF84D "4vx"

```

内存 1 内存 2 内存 3 内存 4 内存 5 监视 1 |x=|局部变量 结构体

地址	十六进制	ASCII
77801000	16 00 18 00 28 7C 80 77 14 00 16 00 78 74 80 77	... (.w...xt.w
77801010	00 00 02 00 FC 5D 80 77 0E 00 10 00 00 7E 80 77	... ũ.w...-.w
77801020	0C 00 0E 00 F0 7D 80 77 08 00 0A 00 D8 73 80 77	... 0.w...0s.w
77801030	06 00 08 00 00 7D 80 77 06 00 08 00 00 7D 80 77	... 0.w...a].w
77801040	06 00 08 00 08 7D 80 77 06 00 08 00 08 7D 80 77	... 0.w...e].w
77801050	1C 00 1E 00 04 74 80 77 6B 4C 73 45 00 00 00 01	... 0t.wkLse... .w...w.0.w
77801060	00 39 92 77 00 00 00 00 60 17 80 77 90 D8 86 77x.w...0.w
77801070	20 00 22 00 78 80 80 77 84 00 86 00 F0 7E 80 77	... k.w F.w0.waD.w
77801080	90 68 83 77 A0 46 90 77 30 B4 83 77 E0 44 90 77w F.w E.w F.w
77801090	90 1E 83 77 20 69 83 77 60 45 90 77 20 46 90 77	... W.F.wI.W.F.w
778010A0	00 57 83 77 A0 46 90 77 20 25 83 77 20 69 83 77	... W.F.wI.W.F.w
778010B0	80 45 90 77 20 46 90 77 C0 CE 86 77 20 46 90 77	... E.W.F.wI.W.F.w
778010C0	00 00 00 00 57 14 01 E2 46 15 C5 43 A5 FE 00 8D	... W.&F.ACYP..

命令: 默认

运行中 INT3 断点于 351a2f05-3848-4de6-9c9d-6e28c946f079.00C31B3E (00C31B3E)!

已调试时间: 0:10:22:28

IDA - 351a2f05-3848-4de6-9c9d-6e28c946f079.exe E:\下载\351a2f05-3848-4de6-9c9d-6e28c946f079.exe

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unxolored External symbol

Functions window

```

Function name 98 }
sub_401000 99 else
sub_401090 100 {
sub_4011A0 101 {
sub_401470 102     v18 = (char)a3;
sub_401710 103     *a3 ^= 0x1ADu;
sub_401830 104 }
          105     v19 = *a3;
          106     _AL = v18 - v13;
          107     _asm { daa }
          108     if ( a2[6] == 'e' )
          109     {
          110     *a3 |= 0x2310u;
          111     v24 = *a3;
          112     }
          113     else
          114     {
          115     *a3 |= 0x4Au;
          116     }
          v23 = *a3;

```

```
unknown_libname.1
__flush_nolock
__flush
sub_4022DE
__flush
__fsall
__initstdio
__endstdio
sub_4024BE
__lock_file
__lock_file2
__unlock_file
__unlock_file2
__mainCRTStartup
__fast_error_exit
Line 4 of 276      00000A69 sub_401470:98 (401669)
Output window
401710: using guessed type _DWORD __cdecl sub_401710(_DWORD, _DWORD, _DWORD);
401710: using guessed type _DWORD __cdecl sub_401710(_DWORD, _DWORD, _DWORD);
401710: using guessed type _DWORD __cdecl sub_401710(_DWORD, _DWORD, _DWORD);
Python
AU: idle Down Disk: 190GB CSDN @weixin_51275728
```

401830:A3->v9>v10->v15->v17

401000: 检验字符

401090: 对416050处理

4011a0:congraulations /try again

画红圈的地方注意result该在a3异或的下面

dbappsec的来源

```
#include < iostream>
using namespace std;
int main(){
    int result;
    string a2="dbappsec";
    int a3=0;
    if ( a2[0] == 'd' )
    {
        a3 |= 4;
    }
    else
    {
        a3 ^= 3;
    }
    if ( a2[1] == 'b' )
    {
        a3 |= 0x14;
    }
    else
    {
        a3 &= 0x61;
    }
    if ( a2[2] == 'a' )
    {
        a3 |= 0x84;
    }
    else
    {
        a3 &= 0xA;
    }
    if ( a2[3] == 'p' )
    {
        a3 |= 0x114 ;
    }
    else
    {
        a3 >>= 7;
    }
    if ( a2[4] == 'p' )
    {
```

```

    {
        a3 |= 0x380;
    }
    else
    {
        a3 *= 2;
    }
    if ( a2[5] == 'f' )
    {
        a3 |= 0x2DC;

    }
    if ( a2[5] == 's' )
    {
        a3 |= 0xA04;
    }
    else{

        a3 ^= 0x1AD;
    }
    if ( a2[6] == 'e' )
    {
        a3 |= 0x2310;
    }
    else
    {
        a3 |= 0x4A;
    }
    if ( a2[7] == 'c' )
    { a3 |= 0x8A10;
        result = a3;
    }
    else
    {
        a3 &= 0x3A3;
        result = a3;
    }
    cout<<hex<<result<<endl;
    char x[8]={0x2a,0xd7,0x92,0xe9,0x53,0xe2,0xc4,0xcd};
    for(int i=0;i<8;i++){
    x[i]^=a2[i];
    int pp=x[i]&0xff;
    cout<<pp;
    }
}

```

416050太复杂了 用动调发现反调试三个isdebuggerpresent、一个isprocessorfeaturepresent。但strongod就可以不用修改

v15

最后md5

47 level4

a输入 然后进行运算方式及运算的数最后与07后面的数字比较。

IDA - signal.exe C:\Users\lenovo\AppData\Local\Temp\Rar\$DRa5128.26362\signal.exe

```
break;
case 3:
    v5 = v3[v9] - LOBYTE(a1[v10 + 1]);
    v10 += 2;
    break;
case 4:
    v5 = a1[v10 + 1] ^ v3[v9];
    v10 += 2;
    break;
case 5:
    v5 = a1[v10 + 1] * v3[v9];
    v10 += 2;
    break;
case 6:
    ++v10;
    break;
case 7:
    if ( v4[v8] != a1[v10 + 1] )
    {
        printf("what a shame...");
        exit(0);
    }
    ++v8;
    v10 += 2;
    break;
case 8:
    v3[v6] = v5;
    ++v10;
    ++v6;
    break;
case 0xA:
    read(v3);
```

Line 15 of 70 00000AAB_Z9vm_operadPii:45 (4016AB)

Output window

```
401553: using guessed type char var_81[100];
401553: using guessed type char var_E5[100];
401553: using guessed type char var_81[100];
```

Python

AU: idle Down Disk: 74GB

IDA - signal.exe C:\Users\lenovo\AppData\Local\Temp\Rar\$DRa5128.26362\signal.exe

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 04 00 00 00 10 00 00 00 08 00 00 00 .....
03 00 00 00 05 00 00 00 01 00 00 00 04 00 00 00 .....
20 00 00 00 08 00 00 00 05 00 00 00 03 00 00 00 .....
01 00 00 00 03 00 00 00 02 00 00 00 08 00 00 00 .....
08 00 00 00 01 00 00 00 0C 00 00 00 08 00 00 00 .....
04 00 00 00 04 00 00 00 01 00 00 00 05 00 00 00 .....
03 00 00 00 08 00 00 00 03 00 00 00 21 00 00 00 .....!
01 00 00 00 0B 00 00 00 08 00 00 00 0B 00 00 00 .....
01 00 00 00 04 00 00 00 09 00 00 00 08 00 00 00 .....
03 00 00 00 20 00 00 00 01 00 00 00 02 00 00 00 .....
51 00 00 00 08 00 00 00 04 00 00 00 24 00 00 00 .....Q.....$.
01 00 00 00 0C 00 00 00 08 00 00 00 0B 00 00 00 .....
01 00 00 00 05 00 00 00 02 00 00 00 08 00 00 00 .....
02 00 00 00 25 00 00 00 01 00 00 00 02 00 00 00 .....%.
36 00 00 00 08 00 00 00 04 00 00 00 41 00 00 00 .....6.....A...
01 00 00 00 02 00 00 00 20 00 00 00 08 00 00 00 .....
05 00 00 00 01 00 00 00 01 00 00 00 05 00 00 00 .....
03 00 00 00 08 00 00 00 02 00 00 00 25 00 00 00 .....%.
01 00 00 00 04 00 00 00 09 00 00 00 08 00 00 00 .....
03 00 00 00 20 00 00 00 01 00 00 00 02 00 00 00 .....
41 00 00 00 08 00 00 00 0C 00 00 00 01 00 00 00 .....A.....?
07 00 00 00 22 00 00 00 07 00 00 00 3F 00 00 00 .....4.....2...
07 00 00 00 34 00 00 00 07 00 00 00 32 00 00 00 .....P.....3...
07 00 00 00 72 00 00 00 07 00 00 00 33 00 00 00 .....1.....
07 00 00 00 18 00 00 00 07 00 00 00 A7 FF FF FF .....(.
07 00 00 00 31 00 00 00 07 00 00 00 F1 FF FF FF .....Z.....
07 00 00 00 28 00 00 00 07 00 00 00 84 FF FF FF .....
07 00 00 00 C1 FF FF FF 07 00 00 00 1E 00 00 00 .....
07 00 00 00 7A 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Line 15 of 70 0001E40_00403040: .data:byte_403040 (Synchronized with IDA View-A)

Output window

```
401553: using guessed type char var_81[100];
401553: using guessed type char var_E5[100];
401553: using guessed type char var_81[100];
```

Python

AU: idle Down Disk: 74GB

```
#include <iostream>
using namespace std;
int main(){
char a[15];
a[0]^0x10-5=0x22;
a[1]^0x20*3=0x3f;
a[2]-2-1=0x34;
a[3]+1^4=0x32;
a[4]*3-0x21=0x72;
a[5]-2=0x33;
a[6]^9-0x20=0x18;
a[7]+0x51^0x24=0xa7;
a[8]=0x31;
a[9]*2+0x25=0xf1;
a[10]+0x36^0x41=0x28;
a[11]+0x20=0x84;
a[12]*3+0x25=0xc1;
a[13]*9-0x20=0x1e;
a[14]+0x42=0x7a;
cout<<a;
}
```