

xctf攻防世界re1 writeup

原创

qq_112419837 于 2020-11-04 11:26:31 发布 96 收藏 1

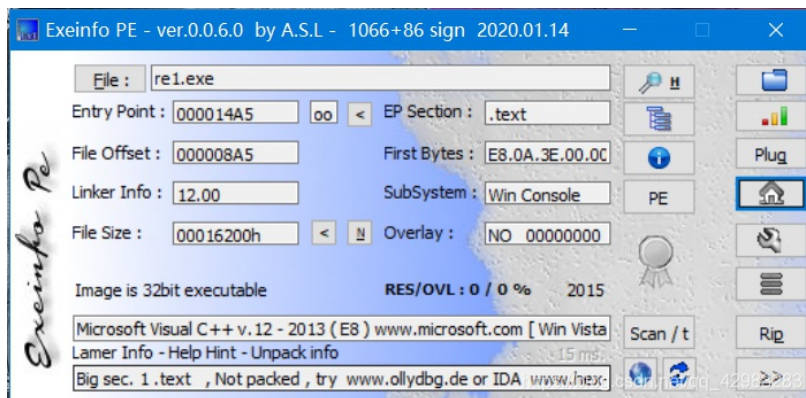
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_42983283/article/details/109486309

版权

The screenshot shows a challenge page for 're1'. It has a difficulty rating of 4.0 stars. The source is 'DUTCTF'. The description says '菜鸡开始学习逆向工程，首先是最简单的题目'. The scene is '暂无'. There is a link to attachments and a URL: https://blog.csdn.net/qq_42983283.

下载查看：



ida打开，注意这个要用7.0打开，6.8分析不出来：

逻辑很简单，输入v9和v5比较：

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int v3; // eax
4     __int128 v5; // [esp+0h] [ebp-44h]
5     __int64 v6; // [esp+10h] [ebp-34h]
6     int v7; // [esp+18h] [ebp-2Ch]
7     __int16 v8; // [esp+1Ch] [ebp-28h]
8     char v9; // [esp+20h] [ebp-24h]
9
10    _mm_storeu_si128((__m128i *)&v5, _mm_loadu_si128((const __m128i *)&v5));
11    v7 = 0;
12    v6 = qword_413E44;
13    v8 = 0;
14    printf("欢迎来到DUTCTF哟\n");
15    printf("这是一道很可爱很简单的逆向题哟\n");
16    printf("输入flag吧:");
17    scanf("%s", &v9);
18    v3 = strcmp((const char *)&v5, &v9);
19    if ( v3 )
20        v3 = -(v3 < 0) | 1;
21    if ( v3 )
22        printf(aFlag_0);
23    else
24        printf((const char *)&unk_413E90);
25    system("pause");
26    return 0;
27 }
```

下断点，动态运行，我这里是记住地址，从od运行，记住只要第10行以后v5赋了值就行：

```

00E51014 - 343EE600 dd re1.00E63E34 ASCII "DUTCTF{Me1c0met0DUTCTF}"
00E51018 33 db 33 CHAR '3'
00E51019 C0 db C0
00E5101A 68 db 68
00E5101B - 4C3EE600 dd re1.00E63E4C
00E5101F F30F7F45 bc movdqu dqword ptr ss:[ebp-0x44],xmm0
00E51024 ? 8945 D4 mov dword ptr ss:[ebp-0x2C],eax
00E51027 ? F30F7E05 443 movq xmm0,qword ptr ds:[0xe63e44]
00E5102F - 660fd645 cc movq qword ptr ss:[ebp-0x34],xmm0
00E51034 - 66:8945 D8 mov word ptr ss:[ebp-0x28],ax
00E51038 - E8 3E020000 call re1.00E5127B
00E5103D - 68 603EE600 push re1.00E63E60
00E51042 - E8 34020000 call re1.00E5127B
00E51047 - 68 803EE600 push re1.00E63E80
00E5104C - E8 2A020000 call re1.00E5127B
00E51051 - 8D45 DC lea eax,dword ptr ss:[ebp-0x24]
00E51054 - 50 push eax
00E51055 - 68 8C3EE600 push re1.00E63E8C %s
00E5105A - E8 72000000 call re1.00E51001
00E5105F 83C4 14 add esp,0x14
00E51062 - 8D45 DC lea eax,dword ptr ss:[ebp-0x24]
00E51065 - 8D4D BC lea ecx,dword ptr ss:[ebp-0x44]
00E51068 > 8011 mov dl,hute ptr ds:[ecx]
00E63E8C=re1.00E63E8C (ASCII "%s")

```

断下以后，智能搜索字符串，找到flag，刚好就是v5赋值的那句：

地址	反汇编	文本字符串
00E51011	db 0F	DUTCTF{we1c0met0DUTCTF}
00E5101A	db 68	欢迎来到DUTCTF哟\n
00E51028	movd dword ptr ds:[0xE63E44],mm0	DUTCTF{
00E5103D	push re1.00E63E60	这是一道很可爱很简单的逆向题哟\n
00E51047	push re1.00E63E80	输入flag吧。
00E51055	push re1.00E63E8C	%s
00E5105F	add esp,0x14	(Initial CPU selection)
00E51091	push re1.00E63E90	flag get./\n
00E51098	push re1.00E63E9C	flag不太对哟，再试试呗，加油哟\n
00E510A5	push re1.00E63EBC	pause
00E51188	push re1.00E60198	COMSPEC
00E511CE	mov [local.4],re1.00E601A0	/c
00E51229	mov ecx,re1.00E601A4	cmd.exe
00E51350	mov eax,dword ptr ds:[0xE5003C]	a
00E517D1	mov ecx,re1.00E65008	\n\n
00E51819	mov eax,re1.00E65008	\n\n
00E51826	mov ecx,re1.00E65008	\n\n
00E51894	mov ecx,re1.00E65008	\n\n
00E52E80	push re1.00E601D4	\
00E52F81	mov eax,re1.00E6540C	.com
00E5312F	push re1.00E601D8	PATH
00E531B9	push re1.00E601E0	~
00E531D2	push re1.00E601E0	~
00E536FF	movsx eax,byte ptr ds:[eax+0xE601E0]	~
00E53A8A	mov esi,dword ptr ds:[0xE65414]	(null)
00E53B77	mov esi,dword ptr ds:[0xE65410]	(null)
00E53ED0	mov esi,dword ptr ds:[0xE65410]	(null)
00E5477B	push re1.00E60300	m
00E5478C	push re1.00E60318	CorExitProcess
00E54AD8	mov dword ptr ds:[0xE67028],edi	
00E54E7B	mov ecx,dword ptr ds:[0xE67028]	

双击：

```

00E51000 $ 55 push ebp
00E51001 - 8BEC mov ebp,esp
00E51003 - 83EC 44 sub esp,0x44
00E51006 - A1 0050E600 mov eax,dword ptr ds:[0xE65000]
00E51008 - 33C5 xor eax,ebp
00E5100D - 8945 FC mov dword ptr ss:[ebp-0x4],eax
00E51010 F30F6F05 343 movdqu xmm0,dqword ptr ds:[0xe63e34]
00E51018 33 db 33 CHAR '3'
00E51019 C0 db C0
00E5101A 68 db 68
00E5101B - 4C3EE600 dd re1.00E63E4C
00E5101F F30F7F45 bc movdqu dqword ptr ss:[ebp-0x44],xmm0
00E51024 ? 8945 D4 mov dword ptr ss:[ebp-0x2C],eax
00E51027 ? F30F7E05 443 movq xmm0,qword ptr ds:[0xe63e44]
00E5102F - 660fd645 cc movq qword ptr ss:[ebp-0x34],xmm0
00E51034 - 66:8945 D8 mov word ptr ss:[ebp-0x28],ax
00E51038 - E8 3E020000 call re1.00E5127B
00E5103D - 68 603EE600 push re1.00E63E60
00E51042 - E8 34020000 call re1.00E5127B
00E51047 - 68 803EE600 push re1.00E63E80
00E5104C - E8 2A020000 call re1.00E5127B
00E51051 - 8D45 DC lea eax,dword ptr ss:[ebp-0x24]
00E51054 - 50 push eax

```

其实010editor直接能搜到：

```

11: 2D 00 7A 00 61 00 00 00 7A 00 68 00 2D 00 63 00 -.z.a...z.h.-c.
11: 68 00 73 00 00 00 00 00 7A 00 68 00 2D 00 63 00 h.s....z.h.-c.
11: 68 00 74 00 00 00 00 00 7A 00 68 00 2D 00 63 00 h.t....z.h.-c.
11: 6E 00 00 00 7A 00 68 00 2D 00 68 00 6B 00 00 00 n...z.h.-h.k...
11: 7A 00 68 00 2D 00 6D 00 6F 00 00 00 7A 00 68 00 z.h.-m.o...z.h.
11: 2D 00 73 00 67 00 00 00 7A 00 68 00 2D 00 74 00 -.s.g...z.h.-t.
11: 77 00 00 00 7A 00 75 00 2D 00 7A 00 61 00 00 00 w...z.u.-z.a...
11: 41 00 00 00 17 00 00 00 43 00 4F 00 4E 00 4F 00 A.....C.O.N.O.
11: 55 00 54 00 24 00 00 00 BA C6 40 00 65 2B 30 30 U.T.$...#E8.e+00
11: 30 00 00 00 31 23 53 4E 41 4E 00 00 31 23 49 4E 0...1#SNAN...1#IN
11: 44 00 00 00 31 23 49 4E 46 00 00 00 31 23 51 4E D...1#INF...1#QN
11: 41 4E 00 00 44 55 54 43 54 46 7B 57 65 31 63 30 AN...DUTCTF(walco
11: 50 65 74 30 44 55 54 43 54 46 7B 00 BB B6 D3 AD mc00DUTCTF...»!G-
11: C0 B4 B5 BD 44 55 54 43 54 46 DF CF 0A 00 00 00 A!mDUTCTFBI...
11: D5 E2 CA C7 D2 BB B5 C0 BA DC BF C9 B0 AE BA DC 0âÊç0»uA®UjF®@U
11: BC F2 B5 A5 B5 C4 C4 E6 CF F2 CC E2 DF CF 0A 00 %0»uA»I0iA!Y...
11: CA E4 C8 EB 66 6C 61 67 B0 C9 3A 00 25 73 00 00 ÈaÈeflag®È...s.s...
11: 66 6C 61 67 20 67 65 74 A1 CC 0A 00 66 6C 61 67 flag getj...flag
11: B2 BB CC AB B6 D4 DF CF A3 AC D4 D9 CA D4 CA D4 ®»i«!00iÈ-00È0È0
11: DF C2 A3 AC BC D3 D3 CD DF CF 0A 00 70 61 75 73 AÀÈ-«00iÈY...paus
11: 65 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 e.....H.....
11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11: 00 00 00 00 00 50 41 00 80 3F 41 00 03 00 00 00 .....PA.E?A.....
11: 52 53 44 53 6B E6 D9 D8 4F 0A D1 44 99 08 44 A7 RSDSk»00.0D®.D$
11: 39 D1 E5 C4 03 00 00 00 45 3A 5C 63 5C 43 6F 6E 9NÀA....E:\c\Con
11: 73 6F 6C 65 41 70 70 6C 69 63 61 74 69 6F 6E 32 soleApplication2
11: 5C 52 65 6C 65 61 73 65 5C 43 6F 6E 73 6F 6C 65 \Release\Console
11: 41 70 70 6C 69 63 61 74 69 6F 6E 32 2E 70 64 62 Application2.pdb
11: 00 00 00 00 00 00 00 00 A4 00 00 00 A4 00 00 00 .....E.....
11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11: 90 2C 00 00 40 75 00 00 D0 AE 00 00 00 00 00 00 ,...@u...D0.....
11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

地址	值
0 出现	flag.
4h	flag
5h	flag
7h	flag

<http://flag.com.net/42983283>