bugku 不好用的CE WriteUp



不好用的CE

		^
用的ce		
150		
	Submit	1
	[:] 用的ce 150	·用的ce 150

这题有好多种解法,我会一个个解释。

只用OD

只用CE

CE+OD

下载文件

工程1	×
点击一万次	欠有flag
	備定 0510F0博客

S. Form1			×
Label1			
		Command 1	
	@51	сто	博客

点两下试试

S. Form1	- 🗆 ×
3	
	[Command 1
	@51CTO博客

无壳

些 PEID v0	.95			
文件: C:\V	isers\dell\Desktop\工程4	exe		105
λ 0 ₫:	00001128	#P 12:	text	
文件编移:	00001108	首字节:	68, 60, 13, 40	
连接器版本	6.0	子系统	Win32 GM	
PESaiffer:	ticrosoft Visual Basic	v5.0/v6.0		
PEIDOSCAN:	ticrosoft Visual Basic (5.0/6.0		
多文件扫描	単位) 直看进程(T)	alle.	POTO	1500
☑ 总在最新	(3) 违项(0)	1 XFG	ドービジ	E.=L

1.只用OD

只用OD我只想出两种办法,虽然只是下断点的方式不同,但也代表了不同的思路。

一、第一种是最直接的也是最笨的,在搜索字符串里的所有内容都下断点,这里幸好搜索的字符串不是很多, 而且flag凑巧是直接存储在内存里的,所以可以使用。若没这么幸运的话就只能在提示的字符串"点击一万次有 flag"处下断点,一点点的往上翻代码了。



二、我们知道了这个程序使用VB写的,且会弹出一个对话框,对话框在VB理常用的函数为rtcMsgBox,可以用 ODB的插件来自动下断点,

BP P VB Notepa	ed Calc	Folder	CHD	Exit			
Messages and Windows BP rtcMsgBox	(D) 版	1132、使5 年(P) 造	e - 王M 項(T)	至4] 慶□(W)	420	H) [+]	快速期
BP _vbaNew2		<u>•</u>]•	1	1	1	l e m	tw
Comparison BP_vbalvarCat BP_vbalvarCmpEq BP_vbalvarTextCmpEq BP_vbalvarTextCmpEq	FFFFF	call add b add b add b xor b add b cnp b	<pre>sinp yte yte yte yte yte yte</pre>	AHSUBU otr ds: otr ds: otr ds: otr ds: otr ds: otr ds:	360 H60.# [eax] [eax] [eax] [eax] [eax]	ThunRTI ,al ,al ,al ,al ,al	Hain_1
BP_vballarTatEq BP_vballarCat BP_vballarCat BP_vballarCap BP_vballarCanp	B 24CBF	add b add b add b sub d xor c jas si	ute p ute p dx uord ax, 0: hort	ptr ds: ptr ds: ptr ds: c0F4C02 IP4.	[eax] [eax] [eax] [ebx 80 00401	.al .al .al	,ebp
BP_vbaStrCompVar BP_vbaStrCopy BP_vbaStrTextCopp		xor o test add b add b add b add b	6	0510	(eax)	- 8×23] .a1 〇博	.esi 客

只用OD第一种办法:在每一处字符串下断点,这里我们就只在可疑字符串下断点了

即第3、4、5、6、7行

/G/G 1000.00	1天生生物中
0040108 park 1 484, 00401300	Chiefes CPF redections
00401120 push [] H[4 00401200	(35/8/books) (31)
00400005 err +6: 184 00401A20	dilicit addredal
00401100 nov deard ptr an. [shp-0al	10]. THE COMOUNT ALEAL AND A DESCRIPTION OF A DESCRIPTION
004011222 any deard ptr is: [shp=0at	[0]4.00400[eebsflbmslbenegblesblfn
00401843 ere deurd ptr un [ebp-0al	[0] 工程4.00401[142+#IMA/0841441444
100401705 size desed ptr as [shp-0s]	C1)工程4:004011点击—万次有4142
A DESCRIPTION OF THE REAL PROPERTY OF THE REAL PROP	
	<u></u>
	Gererent H

首先断在了最后一条,



看起来是在初始化变量,F9继续运行

工程1	×
点击一万次有fla	g
· · · · · · · · · · · · · · · · · · ·	# 1 0博客

跳出对话框,单击确定继续程序

S. Form1			×
Label1			
		Command 1	
	0	51CTC	博客

点击后触发断点,





这三个可疑的字符串在一起,但是其上并没有大跳转,甚至根本没有跳转,那最后一个可疑字符串就更可疑 了,继续F9运行程序,程序并没有断在最后一个字符串处,说明这个字符串很有可能就是达到条件(点击一万次) 后才会出现的字符串,



这个字符串上面还有一个大跳转,那这个字符串就很有可能是flag了,或者flag相关的字符串,我们把这个大跳转nop掉,看看会出现什么

S Form1	-		×
2			
工程1	×		
De7meMUbDe00		1	
DezmqMUNKCPa	NgJgzLPaxa	mmand 1	
]	補定	LOTC.	lait cite
-	ලා ව.	IC IO	傳答

DeZmqMUhRcP8NgJgzLPdXa

这题最坑的地方也就是这个字符串就出现了,之前做这个题也是断在这里,直到最近出了Writeup才知道,这个 看起来像base64的字符串其实是他的远亲,base58

我们都知道base64的范围是 数字(10)+大小写字母(26*2=52)+两个特殊字符(+,/)

而base58是剔除了容易被人误识别的数字0,L的小写,i的大写和o的大写,还有两个特殊字符(+,/)

0.0=+	- A B 405
9.976 年度去污扰	
立即始的。	
708	
De7moMUNRcP8No.kort.PdX	
	110
	198
150000M	

得到flag

只用OD第二种方法,利用OD的插件,在rtcMsgBox下断点,F9运行程序,被断下



这个地方已经不属于程序的领空了,这里是VB调用的库的领空,在这个位置我们在栈里可以找到程序调用函数 的地址,在其上回车以回到程序领空





然后我们就可以苦哈哈地慢慢往上翻代码了,这个下断点的方式适合在没有明确的提示字符串的时候使用,在 有提示字符串的时候还是用字符串来查找比较方便。

CE+OD

打开程序,CE附加程序,



这里我们不知道这个变化的数字的类型,虽然看起来很像整型



所以我们设置扫描类型为未知的初始值,点击首次扫描

22(A):	
Hex 🗌	
扫描类型未知的	的初始值 🗸 🗌
政道典型 精确类	200
内存扫描值小子	f
开始 值介引	F两者之间
停止	/***************
「可写	■可执行

然后点击按钮,变化一下数值

S. Form1			×
4			
	[Command 1	
	@5	1010	博客

再用CE搜索变化的数值

3 -			00000070-184.exe	
16.92	364	AR B	Repuis Accus	(award)
			10年5日 2002年4 10月1日 2015年5日 10月1日 10月1日	
			. @510	「TO博客

点击再次扫描

地址	治疗谋	先桁谋	^	制的扫描	再次扫描
0002001C	216	216	-		
00020020	113	113			
0002012C	917523	917523			
00020130	12	12		日接角型 京政(and line
000207E0	198	198		-	
00020090	190	198		D202 471	
00020098	20	28		内存归属选项	
00098308	1701764	1701764		7710	000000000
00098380	1701780	1701780		10.1	
00098688	3439400594	343940055		The second	/11111111
00098870	1770942	1770962		- 40 M	
00098884	15293024	15293024		用时用只	
00098894	1702016	1702016		- Carner of	1 2075
00058EA4	1701872	1701872	6	05101	()间空
00040000	1701808	1701858	× 2	30101	117 EL

这样太慢了,我们可以用变动的数值和未变动的数值切换来不断搜索

最后剩了八个结果实在分辨不出来了

3 🛩 🖬		0	0000070-工程4.eve	E
MEAR 002201F5 0003E560 02512600	19.47 (g 2101625013 200425100 200425100	A.R.R. 2019/224012 2014/127400 2014/127400	84208 R708	RMOR 03
0252004 0255800 0200204 02040204 02040204	62 677126400 250 260 132079	42 47710400 250 240 132079	1000 1000 1000 100 1000 100 100 100 100	 Pressent 汀O博客

不过这就够了,我们也不需要知道那么细致,随便选一个,双击,拉到下面的界面里,右键他选择 找出是什么 改写了这个地址

(4) MG1	89428	Del		
0 40 1	教師記録		Silese	
	刘清相关内容区域	Chi+B		
67	反正确此内存区域	Ctrl+D	and Descention	Concession 1
10	面形神符号的		A-703	RANDOW
COT SAL	以十六进制整须			
520000	第次的 色		- torn the	
50004	RENA	Cel+H	a second v	
00204	设置/更改下拉利表录			
00228	和2,%和古中的地址	Space		
HCH	SIG BHINGS		ND.	C MLANG
	21210020100000			口戶自己透明代
	的出版什么这样了这个物理	15	Trenentrerentner	
	我出展什么就写了这个物理	16	× 836.0	
	Walks Walkson		142	
	daman.ca		108 4 205	
	and an an		8008	
	80	CM+X	10.000	
PEAR	84	CMI+C		sind con
	NIM	CH+V	OF JOSTO	lait ette
192	0295		Lenn C C	1111

TRIMINICAL	N 0022C1F0	
计数	推夺	818
	74001947 - C7 01 00000000 - mov Jackj.00000000	27.6CMEF
		Autorian
		1103.0
	@51CT	D博客
	U ,	

注意像这样的,地址特别大的,一定不是程序的代码,这个是程序调用的库的地址



像这样40打头的才是程序的代码,具体要看程序的PE头里定义的基地址,一般为400000。

然后我们就可以记住这个地址,用OD打开程序,到这个地址看看,CE也可以看,但是很多操作不方便

-		-		
Concerning and	Contraction Inc.	-	and all the	
Witness That	0498	Baller		
TRAnsitian	48.00	test.	425 15	
Witness Title	Drief, Michaeler	-	TRiam-WR	
THE CONTRACTOR OF	IN AT ACCOUNTS.	-	dend in the allowed and	
THINK			and in the second of	
THE COLUMN	10.00	-	an late all	
100000000000000000000000000000000000000		-		
Verse- ore	and the second second	-	and the second s	
Tabras - 194	In the Statements	-	week to Distance (0.0 - received)	
TRANS-1062	00.46.94	**	Bend M. Jers (M	
D84##~1048	#3 X0-00304000 00	-	dword ph ([]8.xxx+1001,00 (0000000)	
			accordinates	
SP.R.S. Milania		5-7 Hz		
MAL	1 De 100 De 27 00 100	10.10.1	C 10 18 19 10 11 12 13 18 18 18 17 HILDHARTSHARTSHARTSLEDHERT	
			to be do not be the set on PD AA for the concentration As the set	
		-	IN THE REP OF THE THE PART OF THE PART OF CONTAINED A CONTAINED AND A CONTAINTE AND A CONTAINED AND A CONTAINED AND A CONTAINED AND A CONTAINE	
			IN MA WE WARDLING CONTRACTORS	
Dellacat un en ob el Dellacet un el ob el Dellacet un el ob el			NO DE NE NE DE DE DE NE DE	
		10 10 1		1
				1
				ľ
			の Sel CTC 地 湾 常	
10410108 10 <			oriorobir	

毕竟不是专门用来调试程序的应用。

我们用OD附加到进程上,



ctrl+g 到401D44看看



距离我们第一次找到的关键跳转也很近,



这之间有大量的棕色的浮点数运算,而关键跳转之后再无浮点运算,所以这可能就是算法部分,这次我们仔细 分析下算法部分,



这里可以说是算法部分最重要的四条代码了,从0x4010A8存储的10000就能看出来,在我解释浮点助记符之前,我要先解释一下浮点运算:

在包含浮点运算的处理器里,有8个寄存器,分别是ST0-ST7,他们通过浮点助记符来进行浮点运算,他们的使用方法与栈很类似,存储的顺序从ST0开始到ST7,常用的浮点助记符有:

fld 相当于push fstp 相当于pop fadd 相当于add fsub 相当于sub fdiv 相当于div fmul 相当于mul fstsw 把状态寄存器存入寄存器里 fcomp 相当于cmp

再具体点的用法我会在用的时候解释,现在在最开始的浮点运算处下断点

 CHARTER DESTRICT 	 Marketatetatetatetatetatetatetatetatetateta	
search . and as her deard ply the	eta ministreti	
Realized a state for the found play to	The Book Lots	and a statement
AND A DESCRIPTION OF THE PARTY		1000
		seals, state 1444
statistical sector in the sector descent sector	COLUMN TWO IS NOT THE OWNER.	
name	ALC: NO. OF TAXABLE AND ADDRESS OF TAXABLE ADDRESS	a line of the last in
NAMES OF A DAY OF A D	the boost states	
Respect . Alles		tonit, statutation concernent, shall
many and reversion on deard and	11 (Color & DOI)	
nations	111 map (8-18)	
national . Area representations desired pair and	and month (1998) a sensition of the	and Demokration many Longs (14)
NATION CONTRACTOR AND DESCRIPTION.	100 8/10 /0.0	
REAL PROPERTY AND A DESCRIPTION OF A DES		forest statisting
NAMES OF TAXABLE PARTY OF TAXABLE PARTY.		
station - stational - sound ply the		
MARGINE . MARA		(*. ***E011
NAMES OF THE PARTY OF THE		
rate part in the part ply to		
and the second second		
and an and the second s		
subsection of the state of the		
instantion of the local data and	OF	10TO H
manifer and da lan and hand als	(a)b'	1()))))()))()))())())())()())()())()()
CONTRACT INCOMENT. PROTOCOLS	1000	IUIUHA

因为代码跨度有点大,我就不一一截图了,只把关键代码写下来

fld qword ptr ds:[esi+0x34]

把从[esi+0x34]存入ST0

fadd qword ptr ds:[0x4010B0]

0x4010B0是200.0,即ST0+=200.0

fstp qword ptr ds:[esi+0x34]

即[esi+0x34] = ST0

fstsw ax

把状态寄存器存入ax,周围并没有可以影响到状态寄存器的代码,所以忽略就行

fld qword ptr ds:[esi+0x34]

即ST0=[esi+0x34]

fdiv qword ptr ds:[0x4010B0]

即ST0/=200.0

fstp qword ptr ss:[esp]

即[esp]=ST0,这里存储的就是实际的点击数了

fclex

查了一下是叫做浮点检查错误清除,不会影响结果所以忽略

fld qword ptr ds:[esi+0x34]

即ST0=[esi+0x34],

fdiv qword ptr ds:[0x4010B0]

即ST0/=200.0

fcomp qword ptr ds:[0x4010A8]

即ST0与10000比较

fstsw ax

把状态寄存器存入ax

test ah,0x40

比对状态寄存器,

je 401e97

关键跳转

然后怎么改就看个人喜欢了,可以像上次一样直接nop掉关键跳转,也可以修改0x4010B0里的值来达到点一次 等于数次的效果,也可以直接修改0x4010A8里的值,让一万次变成1次。flag处理部分不再赘述。

后来我查了一下, test ah,0x40 比对的是状态寄存器的cf寄存器,即进位寄存器,所以他只会在从9999进位到 10000时触发,

只用CE:

运行程序,用CE附加上

由于我们已经知道了数值的类型为双浮点(双浮点数占八个字节,有效数字16位,之前的200.0可以数一下有效数字就知道了,即使不知道类型为双浮点也可以一个个试,通常数据存储类型只有4字节,单浮点,双浮点类型,偶尔也有单字节的布尔类型),我们设置扫描类型为未知的初始值,数值类型为双浮点搜索,

18 🕬 🖬 18.0	l .		COURSE TREES	E
16.12	572	A.0.8	RADE RADE	Breat 215
			ISING ASSISTER	*
			DERS EAR	w
			Pta 00000000	OMARKA
			844 844	¥85.9
			CHANNER BRIT	
			Contract Contract	or out in the

然后用 变动的数值/未变动的数值切换搜索,很快就搜索到了一个很扎眼的数值,除了这个2200都是后面跟了很 多个小数的双浮点数,然后用2200/11得到增量200,

3 🛩 🖬		0	0004FC8-IM4	418	
1 11 18					
MAR	当约谋	先町復 二	RECER	再大扫描	
00039180	2.26139	2.24139			
00339170	3.06826	3.04824			
01038054	1.27335	1.27335			
00508410	2200	2200	-		-
00508420	1.79014	1.79014	 Form1 		
02420000	1.44314	1.44314	11		
02420004	1.49759	1.49759			
028431478	4.96804	4.94204			
02843HFC	4.12549	4.03549			
02843800	3.79242	3.79242			
62CF6200	8.09270	5.09278			
02071204	1.18575	1.10575		Con	nand
02CF0224	4.00059	4.00059			
02091228	8.41790	8.40798			
correction .	2.79431	3.74451. Y	Giv	SICTOR	11 227

双击把他加入下面的界面,设置大小为1999800



然后点击程序的按钮

S Form1	-		×
10000			
工程1	×		
DeZmqMUhRcP8NgJg	zLPdXa	mmand 1	
	₩= @\$1	стс	博客

就从11变成了100000,从而得到flag

当然,如果我们知道了增量为200,也可以直接搜索200*X

HTE NEE PECENT RECENT PECENT PECENT				CONSC-TRAN		9
BB Dist	542	352	102	RECORD	#17310#	ROWI26
	1989155	211	200	20		
	 Form 	1	- 0	× INNO NO	AD18	~ ONet
	1			1845	1.7	0.001/00/0
				MIRES	E	0.41,650
			Consel	114		105/7 DRADAWT
OF ICT OF				20082		10000000
CONTROL TO THE STATE				94,8038	4 4000	
N === (000 10 10 円子)				Same	051C	TO博