bugku-writeup-Reverse-Easy_vb



示

决: 623

解

提

其

他:



<u>↓</u>下载



01—010 editor 查看

File	Edit	S	ear	ch	Viev	N F	orm	nat	Scri	pts	Ter	npla	ates	De	bug	Тс	ools	Window Help
L 🗋	~ 📂	\sim		.	.		1	‰		7 . I	ຈ (L R	۶	AB I	-	→ 1		👿 । Hex 🚉 ¶ 📳 📐 । 🔜 👰 ।
Start	un a		261/	vh	ovo	,							Ĩ.		Ť			
Start	.up	_ = c	45y_	- 00.	EXE	^	-	-				•				-	-	
1000	b. C	0		2	ے مم	4	5	6 77	/ 0E	ŏ DA	9	A	_В		D CC	CE	11	
1900	n. u	ו טו		00	00	20	AU	77	05	JC AC	40	AD C D	22	99	00		00	W.UN-S ^m II.
1950	11. C) / () / (22	00	60		22	40		02	00	00	22	00	00	· U Labers
190	h . 1	0A 4	46 65	AU 70	55	00	00		00		61	62	AA 65	60	21	00	95	Earm Labol1
1 1 1 0	h · 1		01 61	62	65	60	20	00	00	4C			22		66		11	FOIMLaDelI Labal2 âN 2™fŤ
1420	h · F	27 (01 0C	02	ΔΔ	00	60	50	93	51	40	78	74	31	00	00	00	$-a \hat{0}^{+}T_{0} \times 1$
1430	$h \cdot 4$	ואי	6E	60	60	61	6F	64	32	00	00	00	00	00	00	50	00	Command2
1440	h· 0	0 0	00	00	00	00	00	00	00	F1	4F	AD	33	99	66	CF	11	áN_3™fŤ
1450	h · F	, 0 87 (nc	00	AA	00	60	D3	93	2F	00	00	00	4D	00	43	00	· a `Ó" M C
1A60	h: 5	54 (00	46	00	7B	00	5F	00	4F	00	33	00	74	00	5F	00	T.F.{N.3.t.
1A70	h: 5	52 (00	65	00	76	00	5F	00	31	00	73	00	5F	00	45	00	R.e.v. 1.s. E.
1A80	h: 3	34 (00	61	00	79	00	5F	00	7D	00	00	00	14	00	00	00	4.a.v}
1A90	h: 5	54 (00	72	00	79	00	20	00	61	00	67	00	61	00	69	00	T.r.va.g.a.i.
1AA0	h: 6	5E (00	21	00	00	00	00	00	00	00	00	00	00	00	00	00	n.!
1AB0	h: 0)0 (00	00	00	00	00	00	00	09	4F	AD	33	99	66	CF	11	0-3™fÏ.
1AC0	h:E	37 (0C	00	AA	00	60	D3	93	22	00	00	00	22	6B	CE	8F	·ª.`Ó"""kÎ.
1AD0	h: 6	55 (67	30	52	4D	00	43	00	54	00	46	00	E1	4F	6F	60	egORM.C.T.F.áOo`
1AE0	h: 8	39	5B	68	51	27	59	5B	8D	7E	00	7E	00	7E	00	00	00	‰[hQ'Y[.~.~.~
1AF0	h: F	1 4	4E	AD	33	99	66	CF	11	B7	0C	00	AA	00	60	D3	93	ñN-3™fÏ.•ª.`Ó"
1B00	h: C)9 4	4E	AD	33	99	66	CF	11	B7	0C	00	AA	00	60	D3	93	ÙN-3™fÏ.·ª.`Ó"
1B10	h: 1	8	00	00	00	01	00	92	00	02	00	00	00	00	00	00	00	· · · · · · · · · · · · · · · · · · ·
1B20	h: 0)0 (00	00	00	09	00	00	00	00	00	00	00	56	42	41	36	VBA6
1B30	h: 2	2E 4	44	4C	4C	00	00	00	00	5F	5F	76	62	61	53	74	72	.DLLvbaStr
1B40	h: 4	19	32	00	00	5F	5F	76	62	61	53	74	72	4D	6F	76	65 _h	tta 3://blog.vbaa 5.he May 922597955
Find	Deer	معلي																使用010

editor查看,搜索flag字符无果,搜索{,找到一串字符,将MCTF{}改为Flag{即可。

02—ida查找

File Edit Jump Search View Debugger	r Options Windows Help	
i 🦰 🔚 i 🦛 🗣 🗸 i 🐴 🐂 🐘 🚑 i 🗼 🛵 i i		
		•
Library function 📕 Regular function	Instruction Data Unexplored External symbol	
🗗 Functions window 🛛 🗗 🛪	- IR IDA View-A 🛛 🔟 Hex View-1 🖾 🖪 Structures 🍽 🗄 Enuns 🖾 🕅 Inports 🖾 🕅 Exports 🔍	
Function name	004019A0 5C 56 42 36 2E 4F 4C 42 00 00 00 05 42 00 00 \VB6.0LBVB	^
ThumPTWein	004019B0 80 19 40 00 00 00 00 00 00 00 00 00 00 00 00	
7 IIIdikiwaiii	004019C0 90 19 40 00 AC 19 40 00 D0 42 40 00 00 00 00 00@@@	
	004019D0 00 00 00 00 20 A0 77 05 DA 4E AD 33 99 66 CF 11爛臟檉	
	004019E0 B7 0C 00 AA 00 60 D3 93 4C 61 62 65 6C 33 00 00`計-Label3	
	004019F0 3A 4F AD 33 99 66 CF 11 B7 0C 00 AA 00 60 D3 93 :0檉`計·	
	00401A00 46 6F 72 6D 00 00 00 00 4C 61 62 65 6C 31 00 00 FormLabel1	
	00401A10	
	00401A20 B7 0C 00 AA 00 60 D3 93 54 65 78 74 31 00 00 00許·Text1	
	00401A30 43 6F 6D 6D 61 6E 64 32 00 00 00 00 00 00 5C 00 Command2	
	00401A40 00 00 00 00 00 00 00 00 E1 4E AD 33 99 66 CF 11	
	00401A50 B7 0C 00 AA 00 60 D3 93 2E 00 00 00 4D 00 43 00`許·M.C.	
	00401A60 54 00 46 00 7B 00 5F 00 4E 00 33 00 74 00 5F 00 T.F.{N.3.t	
	00401A70 52 00 65 00 76 00 5F 00 31 00 73 00 5F 00 45 00 R.e.v1.sE.	
	00401A80 34 00 61 00 79 00 5F 00 7D 00 00 00 14 00 00 00 4.a.y}	
	00401A90 54 00 72 00 79 00 20 00 61 00 67 00 61 00 69 00 T.r.ya.g.a.i.	
	00401AA0 6E 00 21 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00401AB0 00 00 00 00 00 00 00 00 00 4F AD 33 99 66 CF 11	
	00401AC0 B7 0C 00 AA 00 60 D3 93 22 00 00 00 22 6B CE 8F`許·""K蝸·	
	00401AD0 65 67 30 52 4D 00 43 00 54 00 46 00 E1 4F 6F 60 eg0RM.C.T.F.問:o`	
	00401AE0 89 5B 68 51 27 59 5B 8D 7E 00 7E 00 7E 00 00 00 塠 hQ'Y[莨·.~	
	00401AF0 F1 4E AD 33 99 66 CF 11 B7 0C 00 AA 00 60 D3 93 藟・檉・`計・	
	00401B00 D9 4E AD 33 99 66 CF 11 B7 0C 00 AA 00 60 D3 93 貼檉許·	
	00401B10 18 00 00 00 01 00 92 00 02 00 00 00 00 00 00 00	
< >	00401B20 00 00 00 00 09 00 00 00 00 00 00 00 05 42 41 36VBA6	
	00001&69 00401&69: .text:dword_401&48+21 (Synchronized with ID& View-&)	~
Output window		0 8 ×
The initial autoanalysis has been fin	nished	^
Duthan	laWaqiin.	og.csan.nel/qq_22597955™

使用ida,在Hex view-1中发现,更容易找到flag,因为大多数为乱码,已排除了很多干扰项。

03—od发现

子愛破解 - easy_vb.exe - [LCG - m主线程, 模块 - easy_vb] ① 文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H) [+] 快速菜单 Toc	备份 复制	>	Folder CMD Exit	- 0 ×
1 em t wh c	二进制	>	11 A 🖲 🞯 🔛 🔜 吾 愛 🕷 Ж	
00402384 .57 push edi 00402385 .880F nov ecx,dword ptr ds:[edi] 00402387 .FF91 A000000 ccll dword ptr ds:[ecx+0xA0] 00402380 .3803 cnp eax,ebx 00402387 .DBE2 cnp eax,ebx 00402387 .0802 cnp eax,ebx 00402393 .08 A00000000000000000000000000000000000	に編(A) 标签 編(報注释 断点(P) HIT 誤踪 PLIN(問覧)	Space : ; >	X < X y_vb. (HoduleEntryPoint> y_vb. (HoduleEntryPoint> u.ut. (HoduleEntryPoint>	< < < < < < < <
0040239D 57 push edi 0040239F 50 push edi 0040239F 50 push eax 0040239F FF15 2410400 edi 00402305 > 8845 E8 nov eax, 40ord ptr ss:[ebp=0x18] 00402369 50 push eax 00402369 68 50:104000 easy_vb.00401A5C	此处为新 EIP 转到 线程 数据窗口中跟随	Ctrl+Gray * > >	y_ob. y_ob. 2.0(FFFFFFF) 2.0(FFFFFFF) 2.0(FFFFFFF)	
0040230HE . FF15 54104000 Call duord ptr ds:[<&NSU00460ubastru 00400230H . 88F8 nou edi,eax 0040823H6 . 8040 E8 lea ecx,dword ptr ss:[ebp-0x18] 0040238H . F7DF neg edi 004023H5 . 102F . 102F 004023H5 . 604-061,e01 . 102F 004023H5 . 102F . 102F 00401A5C . 102F . 102F 004031A5C . 102F . 102F	查找(S) 查找参考(R) 查看 复制到可执行文件 分析	> > > >	2_0(FFFFFFFF) 2_396000(FFF) 2_0(FFFFFFF) OR_SUCCESS (00000000) ,NB,E,BE,NS,PE,GE,LE)	
地比 時間 時間 時間 時間 時間 日本 1	FKVMP IDAFicator StrongOD LoadMapEx	> > > >	<u>419 返回到 kernel32.75C40419</u> 1000 1400 kernel32.BaseThreadInitThunk FDC 12ED 返回到 ntdll.77B872ED 1搜索 ASCII	^
804-04-66 0 69 00 00 00 00 00 00 00 00 00 00 00 00 00	运行脚本(S) Script Functions 用OllyDump脱壳调试进程 Zeus 中文搜索引擎	> >	2 搜索 UNICODE 3 智能搜索 4 帮助 5 关于	ESP EBP NOWS https://biog.csdn.net/ag_225517955

使用od打开,右键选择中文搜索引擎搜索ASCII,然后双击返回主页面就可以看到flag。