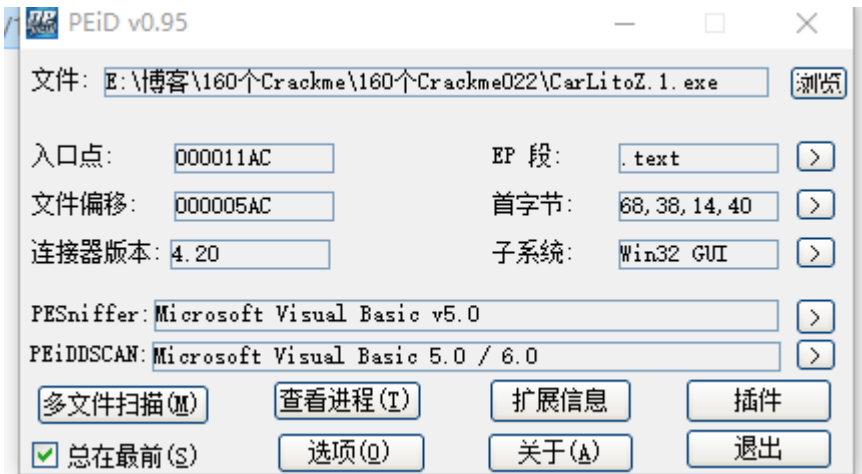
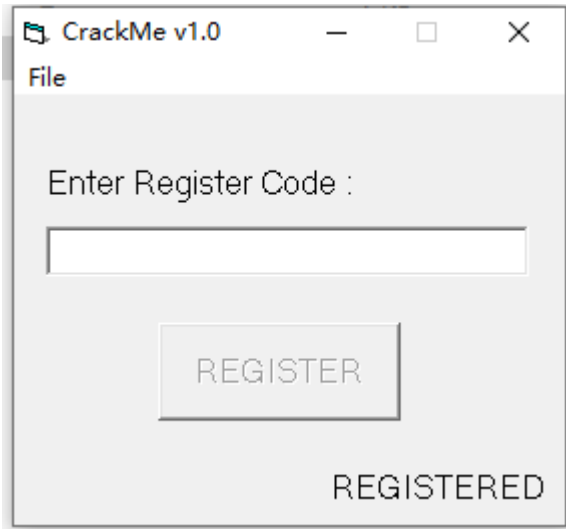


查壳



这个Crackme是用VB写的，没有加壳，也不是P-Code，那就直接上OD吧

分析程序



这个Crackme只有一个序列号保护，一般来说序列号的保护程序大多数只需要追踪正确的Key就能达到目的，少部分是通过算法校验的

追踪序列号

地址	HEX	数据	反汇编	注释		
00402F38	.	50	push eax			
00402F39	.	FF15 34614000	call dword ptr ds:[<MSVBVM50. __vbaHresultCheckObj	MSVBVM50. __vbaHresultCheckObj		
00402F3F	>	8D4D E4	lea ecx, dword ptr ss:[ebp-0x1C]			
00402F42	.	FFD7	call edi			
00402F44	.	E9 8C000000	jmp CarLitoZ.00402FD5			
00402F49	>	FFD7	call edi			
00402F4B	.	8D55 94	lea edx, dword ptr ss:[ebp-0x6C]			
00402F4E	.	8D4D D4	lea ecx, dword ptr ss:[ebp-0x2C]			
00402F51	.	C745 9C 28234	mov dword ptr ss:[ebp-0x64], CarLitoZ.00402328	Wrong Code! Try Again		
00402F58	.	C745 94 08000	mov dword ptr ss:[ebp-0x6C], 0x8			
00402F5F	.	FFD7	call edi			
00402F61	.	8D45 A4	lea eax, dword ptr ss:[ebp-0x5C]			
00402F64	.	8D4D B4	lea ecx, dword ptr ss:[ebp-0x4C]			
00402F67	.	50	push eax			
00402F68	.	8D55 C4	lea edx, dword ptr ss:[ebp-0x3C]			
00402F6B	.	51	push ecx			
00402F6C	.	52	push edx			
edi=00000000						
跳转来自 00402DE9						
地址	HEX	数据	UNICODE	地址	数值	注释

首先根据错误的字符串提示，找到跳转到这个位置的地方，直接转到402DE9的位置

地址	HEX 数据	反汇编	注释
00402DC9	. 894D AC	mov dword ptr ss:[ebp-0x54], ecx	
00402DCC	. 894D BC	mov dword ptr ss:[ebp-0x44], ecx	
00402DCF	. 8945 A4	mov dword ptr ss:[ebp-0x5C], eax	
00402DD2	. 8945 B4	mov dword ptr ss:[ebp-0x4C], eax	
00402DD5	. C745 8C 08234	mov dword ptr ss:[ebp-0x74], CarLitoZ.00402308	CrackMe v1.0
00402DDC	. C745 84 08000	mov dword ptr ss:[ebp-0x7C], 0x8	
00402DE3	. 8D55 84	lea edx, dword ptr ss:[ebp-0x7C]	
00402DE6	. 8D4D C4	lea ecx, dword ptr ss:[ebp-0x3C]	
00402DE9	. 0F84 5A010000	ja CarLitoZ.00402F49	
00402DEF	. FFD7	call edi	<MSVBVM50. __vbaVarDup>
00402DF1	. 8D55 94	lea edx, dword ptr ss:[ebp-0x6C]	
00402DF4	. 8D4D D4	lea ecx, dword ptr ss:[ebp-0x2C]	
00402DF7	. C745 9C D4224	mov dword ptr ss:[ebp-0x64], CarLitoZ.004022D4	Registration Successful
00402DFE	. C745 94 08000	mov dword ptr ss:[ebp-0x6C], 0x8	
00402E05	. FFD7	call edi	
00402E07	. 8D45 A4	lea eax, dword ptr ss:[ebp-0x5C]	
00402E0A	. 8D4D B4	lea ecx, dword ptr ss:[ebp-0x4C]	
edi=00000000			

下面就是注册成功的提示，我们直接往上翻

地址	HEX 数据	反汇编	注释	寄存器 (FPU)	
00402D92	. 56	push esi		SP 0019F110	
00402D93	. 50	push eax		BP 0019F1D0	
00402D94	. FF15 34614000	call dword ptr ds:[<MSVBVM50. __vbaHresultCheckObj	MSVBVM50. __vbaHresultCheckObj	SI 00423290	
00402D9A	> 8D4E 34	lea ecx,dword ptr ds:[esi+0x34]		DI 00000000	
00402D9D	. 8D55 94	lea edx,dword ptr ss:[ebp-0x6C]		IP 00402DB0	
00402DA0	. 51	push ecx	var18 = 004232C4		
00402DA1	. 52	push edx	var28 = 0019F164	0 ES 002B	
00402DA2	. C745 9C 01000	mov dword ptr ss:[ebp-0x64],0x1		1 CS 0023	
00402DA9	. C745 94 02800	mov dword ptr ss:[ebp-0x6C],0x8002		0 SS 002B	
00402DB0	. FF15 6C614000	call dword ptr ds:[<MSVBVM50. __vbaVarTstEq>]	__vbaVarTstEq	1 DS 002B	
00402DB6	. 8B3D C4614000	mov edi,dword ptr ds:[<MSVBVM50. __vbaVarDup>]	MSVBVM50. __vbaVarDup	0 FS 0053	
00402DBC	. B9 04000280	mov ecx,0x80020004		0 GS 002B	
00402DC1	. 66:85C0	test ax,ax		0	
00402DC4	. B8 0A000000	mov eax,0xA		0 LastErr	
00402DC9	. 894D AC	mov dword ptr ss:[ebp-0x54],ecx			
00402DCC	. 894D BC	mov dword ptr ss:[ebp-0x44],ecx		FL 00000246	
ds:[0040616C]=741CB99E (MSVBVM50. __vbaVarTstEq)					
地址	HEX 数据	UNICODE	地址	数值	注释
00404000	00 00 00 00	00 00 00 00	008 4B 42 00	00 00 00 00 爬B...
00404010	90 32 42 00	00 00 00 00	000 36 42 00	58 36 42 00	@B... 爬
00404020	00 00 00 00	08 0A 45 00	00 00 00 00	00 00 00 00	... 爬...
00404030	00 00 00 00	00 00 00 00	00 00 40 00	F8 9F 42 00 @□
00404040	4B 1C 0B 74	00 00 00 00	00 00 00 00	18 1F 42 00	... 爬...
00404050	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404060	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404070	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404080	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404090	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004040F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404100	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404110	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404120	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404130	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404140	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404150	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404160	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404170	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404180	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404190	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004041F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404200	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404210	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404220	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404230	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404240	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404250	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404260	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404270	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404280	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404290	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004042F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404300	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404310	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404320	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404330	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404340	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404350	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404360	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404370	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404380	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404390	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004043F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404400	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404410	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404420	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404430	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404440	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404450	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404460	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404470	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404480	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404490	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004044F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404500	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404510	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404520	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404530	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404540	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404550	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404560	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404570	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404580	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404590	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004045F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404600	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404610	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404620	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404630	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404640	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404650	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404660	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404670	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404680	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404690	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046E0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004046F0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404700	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404710	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404720	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404730	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404740	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404750	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404760	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404770	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404780	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
00404790	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004047A0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004047B0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004047C0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	... 爬...
004047D0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	

ds:[0040616C]=741CB99E (MSVBVM50.__vbaVarTstEq)										0 empty 0.0 1 empty 0.0 0 empty 0.0	
地址		HEX 数据				UNICODE			地址	数值	注释
0019F164	02 80 00 00	00 00 00 00	01 00 00 00	15 00 00 00	步...□			0019F110	0019F164	var28 = 0019F164	
0019F174	00 00 00 00	BA 15 01 97	BC F1 19 00	FC 31 D9 75	...零			0019F114	004232C4	var18 = 004232C4	
0019F184	00 00 00 00	BA 15 01 97	49 00 5A 00	18 F2 19 00	...零IZ			0019F118	0019F1DC		
0019F194	00 00 00 00	00 00 00 00	01 00 00 00	8E 00 10 00	...□			0019F11C	0019F2B8		
0019F1A4	00 00 00 00	BA 15 97 FF	FF FF FF FF	44 30 00 00	...7...			0019F120	005CD5A4		
0019F1B4	00 00 00 00	00 00 00 00	88 F7 19 00	66 10 40 00	...□9			0019F124	00000001		
0019F1C4	18 F1 19 00	20 10 40 00	01 00 00 00	DC F1 19 00	□@□			0019F128	00000001		
0019F1D4	A9 E5 0D 74	90 32 42 00	EC F1 19 00	EF 1E 40 00	琳@B			0019F12C	00000014		
0019F1E4	14 22 42 00	00 00 00 00	00 00 00 00	00 00 00 00				0019F130	00D94E30		
ds:[0040616C]=741CB99E (MSVBVM50.__vbaVarTstEq)										0 empty 0.0 1 empty 0.0 0 empty 0.0	
地址		HEX 数据				UNICODE			地址	数值	注释
004232C4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00			0019F110	0019F164	var28 = 0019F164	
004232D4	02 00 00 00	8C D6 5C 00	01 00 2F 00	62 34 0E 74	...□/倍			0019F114	004232C4	var18 = 004232C4	
004232E4	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00			0019F118	0019F1DC		
004232F4	00 00 00 00	24 1C 40 00	84 1C 40 00	F8 1C 40 00	...@□@			0019F11C	0019F2B8		
00423304	8C 1D 40 00	A8 1D 40 00	C4 1D 40 00	E0 1D 40 00	...@			0019F120	005CD5A4		
00423314	40 1E 40 00	9C 1E 40 00	B8 1E 40 00	00 00 00 00	...@			0019F124	00000001		
00423324	00 00 00 00	80 A5 7F 23	62 4F 00 08	38 37 42 00	...巨斐B			0019F128	00000001		
00423334	A0 31 41 00	40 37 42 00	A8 31 41 00	70 55 42 00	...好B			0019F12C	00000014		
00423344	00 52 42 00	00 00 0C 74	E7 1B 0C 74	00 D0 14 00	刀B.珠			0019F130	00D94E30		
00423354	40 00 42 00	E8 36 42 00	18 00 1A 00	10 37 42 00	...B			0019F134	00000000		
M1 M2 M3 M4 M5 Command:											

其中var28的值为1，var18的值为0，说明在这个比较函数之前已经有过一次校验，继续往上追

地址	HEX 数据	反汇编	注释
00402D69	. 897D E4	mov dword ptr ss:[ebp-0x1C],edi	
00402D6C	. 897D D4	mov dword ptr ss:[ebp-0x2C],edi	
00402D6F	. 897D C4	mov dword ptr ss:[ebp-0x3C],edi	
00402D72	. 897D B4	mov dword ptr ss:[ebp-0x4C],edi	
00402D75	. 897D A4	mov dword ptr ss:[ebp-0x5C],edi	
00402D78	. 897D 94	mov dword ptr ss:[ebp-0x6C],edi	
00402D7B	. 897D 84	mov dword ptr ss:[ebp-0x7C],edi	
00402D7E	. FF93 F8060000	call dword ptr ds:[ebx+0x6F8]	CarLitoZ.00401F11
00402D84	. 3BC7	cmp eax,edi	
00402D86	. 7D 12	jge short CarLitoZ.00402D9A	
00402D88	. 68 F8060000	push 0x6F8	
00402D8D	. 68 0C224000	push CarLitoZ.0040220C	
00402D92	. 56	push esi	
00402D93	. 50	push eax	
00402D94	. FF15 34614000	call dword ptr ds:[<&MSVBVM50.__vbaHresultCheck]	MSVBVM50.__vbaHresultCheck
00402D9A	> 8D4E 34	lea ecx,dword ptr ds:[esi+0x34]	

这里有一个来历不明的call，既没有函数名，也没有注释，很可能就是在这个函数里面对于序列号进行比较，回车跟进去

地址	HEX 数据	反汇编	注释
00401F11	. E9 1A130000	jmp CarLitoZ.00403230	
00401F16	. 00	db 00	
00401F17	. 00	db 00	
00401F18	. 00	db 00	
00401F19	. 00	db 00	
00401F1A	. 00	db 00	
00401F1B	. 00	db 00	
00401F1C	. 40404000	dd CarLitoZ.00404040	
00401F20	. 44294000	dd CarLitoZ.00402944	
00401F24	. FF	db FF	
00401F25	. FF	db FF	
00401F26	. FF	db FF	
00401F27	. FF	db FF	
00401F28	. 00	db 00	
00401F29	. 00	db 00	
00401F2A	. 00	db 00	
00401F2B	. 00	db 00	

进去之后有一个远跳，

地址	HEX 数据	反汇编	注释
00403230	> 55	push ebp	
00403231	. 8BEC	mov ebp, esp	
00403233	. 83EC 0C	sub esp, 0xC	
00403236	. 68 66104000	push <jmp.&MSVBVM50. __vbaExceptionHandler>	SE 处理程序安装
0040323B	. 64:A1 00000000	mov eax, dword ptr fs:[0]	
00403241	. 50	push eax	
00403242	. 64:8925 00000000	mov dword ptr fs:[0], esp	
00403249	. 81EC 54030000	sub esp, 0x354	
0040324F	. 8B45 08	mov eax, dword ptr ss:[ebp+0x8]	
00403252	. 53	push ebx	CarLitoZ. 00404A68
00403253	. 56	push esi	
00403254	. 57	push edi	
00403255	. 8B08	mov ecx, dword ptr ds:[eax]	
00403257	. 8965 F4	mov dword ptr ss:[ebp-0xC], esp	
0040325A	. 33F6	xor esi, esi	
0040325C	. C745 F8 4010	mov dword ptr ss:[ebp-0x8], CarLitoZ. 00401040	
00403262	. 50	push eax	

跳到这个函数，这个才是真正的校验序列号的函数，看来这个作者跟我们玩了一个捉迷藏

地址	HEX 数据	反汇编	注释
0040365B	. C745 94 0800	mov dword ptr ss:[ebp-0x6C], 0x8	
00403662	. FFD7	call edi	rtcMidCharVar
00403664	. 8B45 E0	mov eax, dword ptr ss:[ebp-0x20]	
00403667	. 8D95 54FFFFFF	lea edx, dword ptr ss:[ebp-0xAC]	
0040366D	. 8985 6CFFFFFF	mov dword ptr ss:[ebp-0x94], eax	
00403673	. 52	push edx	Length8 = 0x0
00403674	. 8D85 64FFFFFF	lea eax, dword ptr ss:[ebp-0x9C]	
0040367A	. 6A 09	push 0x9	Start = 0x9
0040367C	. 8D8D 44FFFFFF	lea ecx, dword ptr ss:[ebp-0xBC]	
00403682	. 50	push eax	dString8 = 00000004
00403683	. 51	push ecx	RetBUFFER = 00423290
00403684	. C785 5CFFFFFF	mov dword ptr ss:[ebp-0xA4], 0x1	
0040368E	. 899D 54FFFFFF	mov dword ptr ss:[ebp-0xAC], ebx	
00403694	. 8975 E0	mov dword ptr ss:[ebp-0x20], esi	CarLitoZ. 00404A68
00403697	. C785 64FFFFFF	mov dword ptr ss:[ebp-0x9C], 0x8	
004036A1	. FFD7	call edi	rtcMidCharVar
004036A2	. 8B45 DC	mov eax, dword ptr ss:[ebp-0x24]	

地址	HEX 数据	反汇编	注释
00403846	. 8D95 34FFFFFF	lea edx, dword ptr ss:[ebp-0xCC]	
0040384C	. 51	push ecx	var28 = 00423290
0040384D	. 52	push edx	saveto8 = NULL
0040384E	. FFD7	call edi	__vbaVarAdd
00403850	. 50	push eax	var18 = 00000004
00403851	. 8D85 04FFFFFF	lea eax, dword ptr ss:[ebp-0xFC]	
00403857	. 8D8D F4FEFFFF	lea ecx, dword ptr ss:[ebp-0x10C]	
0040385D	. 50	push eax	var28 = 00000004
0040385E	. 51	push ecx	saveto8 = 00423290
0040385F	. FFD7	call edi	__vbaVarAdd
00403861	. 50	push eax	var18 = 00000004
00403862	. 8D95 C4FEFFFF	lea edx, dword ptr ss:[ebp-0x13C]	
00403868	. 8D85 B4FEFFFF	lea eax, dword ptr ss:[ebp-0x14C]	
0040386E	. 52	push edx	var28 = NULL
0040386F	. 50	push eax	saveto8 = 00000004
00403870	. FFD7	call edi	__vbaVarAdd

这个函数一直往下拉，你会看到有很多重复的代码和一些疑似在计算序列号的函数，如果你从函数头开始一步一步分析，那你就上当了，因为这些函数根本没有任何作用，关键的代码只有一处

地址	HEX 数据	反汇编	注释	寄存器 (FPU)	
004038A1	. 52	push edx	var28 = NULL	SP 0019ED90	
004038A2	. 50	push eax	saveto8 = 0019EEC0	BP 0019F10C	
004038A3	. FFD7	call edi	__vbaVarAdd	SI 00000000	
004038A5	. 8D8D C4FDF	lea ecx,dword ptr ss:[ebp-0x23C]		DI 741C0ECC MSVB	
004038AB	. 50	push eax	var18 = 0019EEC0	IP 004038B7 CarL	
004038AC	. 51	push ecx	var28 = 00425BE0		
004038AD	. 8D95 B4FDF	lea edx,dword ptr ss:[ebp-0x24C]			
004038B3	. 52	push edx	saveto8 = NULL	0 ES 002B 32位	
004038B4	. FFD7	call edi	__vbaVarAdd	1 CS 0023 32位	
004038B6	. 50	push eax	var28 = 0019EEC0	0 SS 002B 32位	
004038B7	. FF15 6C61400	call dword ptr ds:[&MSVBVM50.__vbaVarTstEq]	__vbaVarTstEq	1 DS 002B 32位	
004038BD	. 8BF8	mov edi,ecx		0 FS 0053 32位	
004038BF	. 8D45 A4	lea eax,dword ptr ss:[ebp-0x5C]		0 GS 002B 32位	
004038C2	. 8D4D A8	lea ecx,dword ptr ss:[ebp-0x58]		0 LastErr ERRO	
004038C5	. 50	push eax		FL 00000246 (NO,	
004038C6	. 8D55 AC	lea edx,dword ptr ss:[ebp-0x54]		0 empty 0.0	
004038C9	. 51	push ecx		1 empty 0.0	
ds:[0040616C]=741C899E (MSVBVM50.__vbaVarTstEq)					
地址	HEX 数据	UNICODE	地址	数值	注释
0019EEC0	08 00 00 00 54 F0 19 00 4C 28 48 00 4D 38 01 1C	□. □.!	0019ED90	0019EEC0	var28 = 0019EEC0
0019EED0	08 00 00 00 E0 D8 5C 00 FC 30 48 00 C5 A5 11 74	□. \-H*	0019ED94	0019EEB0	var18 = 0019EEB0
0019FEE0	02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00	...□.□.	0019ED98	00000000	

找到这个比较的函数，下断点，查看参数

地址	HEX 数据	UNICODE
00482694	31 00 31 00 31 00 31 00 31 00 31 00 31 00	11111111
004826A4	31 00 31 00 31 00 31 00 31 00 41 01 1B E3	11111.七
004826B4	00 1A 00 8C 3C 13 68 6C 00 00 00 00 02 00 00 00	错误&泪..
004826C4	20 29 46 00 00 00 00 00 00 00 00 00 03 00 00 00	...F....□.
004826D4	00 00 00 00 4C 01 10 E3 00 1B 00 8C 3C 13 68 6C	..ō 错误
004826E4	00 00 00 00 02 00 00 00 20 29 46 00 00 00 00 00	...F..
004826F4	00 00 00 00 03 00 00 00 70 00 00 00 77 01 0D E3	...□.p.ý
00482704	00 1C 00 88 B4 DE 78 6C C8 0C 79 6C 00 00 00 00	错误 汚&洒
00482714	01 00 00 00 C0 84 49 00 40 7B 76 6C 00 00 00 00	□. 捺I笔
00482724	00 00 00 00 72 01 0A E3 00 1D 00 8C 3C 13 68 6C	...□. 错误

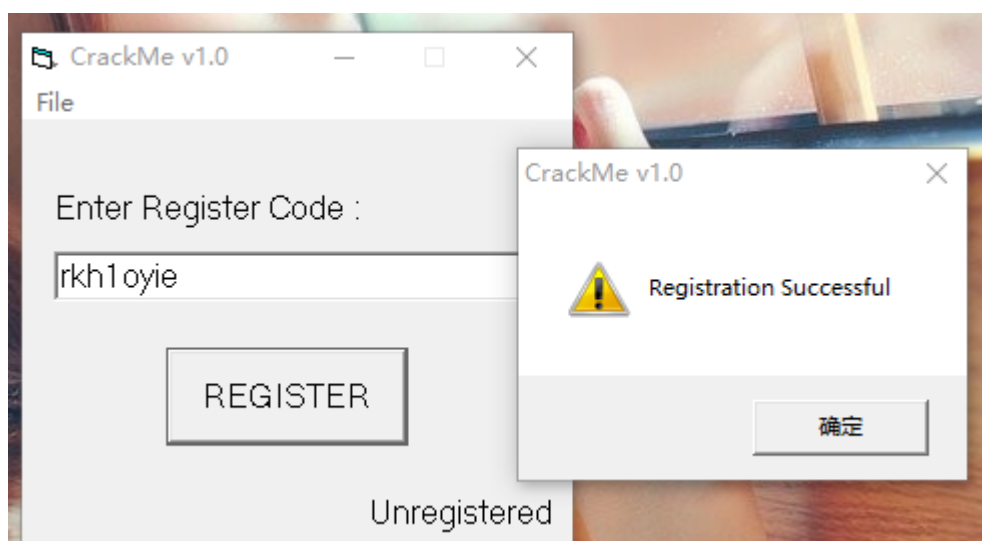
var18是我随便输入的序列号11111111

地址	HEX 数据	UNICODE
0048284C	72 00 6B 00 68 00 31 00 6F 00 79 00 69 00 65 00	rkhloyie
0048285C	00 00 5B 4A 9A F6 59 2A 59 5C 77 8D 9A 00 22 E3	. 靴 ✕ 厠
0048286C	00 25 00 80 60 1C 1A 77 00 10 1A 77 00 00 00 00	-耀b告の告
0048287C	48 60 44 00 5A DD 13 17 E7 68 5B 4A 9A F6 59 2A	忤D 厠棧靴
0048288C	59 5C 77 8D 85 00 5F E3 00 26 00 88 60 1C 1A 77	厠起 厠
0048289C	00 10 1A 77 01 00 00 00 48 60 44 00 5A DD 13 17	の告□. 忤
004828AC	E7 68 5B 4A 9A F6 59 2A 59 5C 77 8D 80 00 54 E3	棧靴 ✕ 厠
004828BC	00 27 00 80 5A DD 13 17 E7 68 5B 4A 9A F6 59 2A	✕耀 厠棧靴
004828CC	59 5C 77 8D 00 00 19 00 70 F3 19 00 00 00 00 00	厠起. □
004828DC	01 00 00 00 8B 00 51 E3 00 28 00 80 60 1C 1A 77	□. 耀

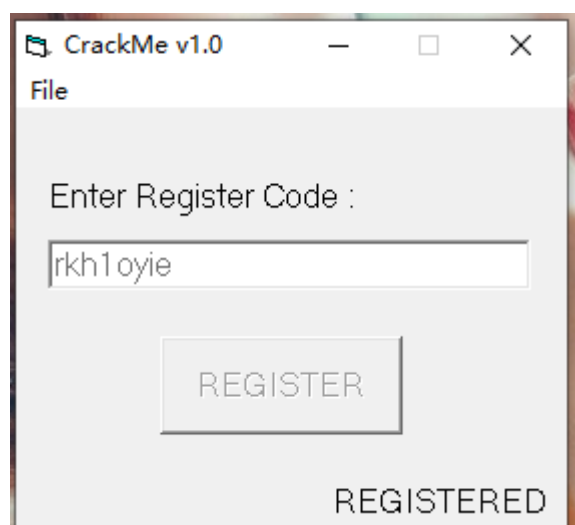
var28就是正确的序列号rkhl0yie，看到了吗？这个就是作者给我们下的套，城里人套路深我要回农村

验证结果

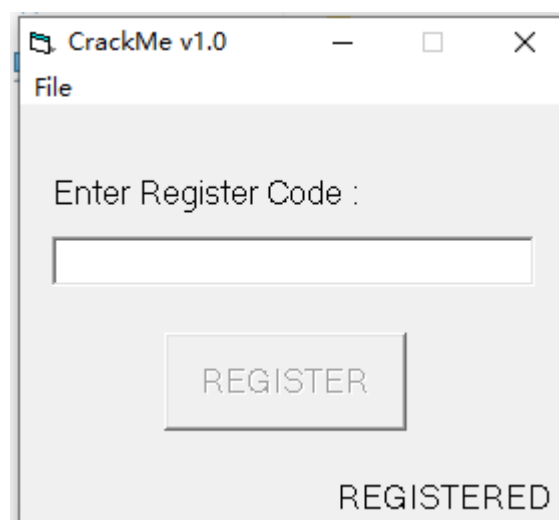
输入序列号，显示注册成功，破解完成



另外我想吐槽的一点是，这个Crackme一旦注册成功了，右下角就会显示一个已注册的提示，然后编辑框被禁用



就算你再次打开，编辑框也还是被禁用



哈哈哈 这个作者套路果然深啊

需要相关文件的可以到我的Github下载：<https://github.com/TonyChen56/160-Crackme>