

查壳  
分析程序  
验证结果

## 查壳



目标程序是一个VB写的，没有加壳。单纯的序列号保护

## 分析程序

004FEC42	74 6E	je short cupofcof.004FECB2	EDX 004
004FEC44	B9 04000280	mov ecx,0x80020004	EBX 7FF
004FEC49	B8 0A000000	mov eax,0xA	ESP 001
004FEC4E	894D AC	mov dword ptr ss:[ebp-0x54],ecx	EBP 001
004FEC51	894D BC	mov dword ptr ss:[ebp-0x44],ecx	ESI 000
004FEC54	894D CC	mov dword ptr ss:[ebp-0x34],ecx	EDI 000
004FEC57	8D55 94	lea edx,dword ptr ss:[ebp-0x6C]	EIP 004
004FEC5A	8D4D D4	lea ecx,dword ptr ss:[ebp-0x2C]	C 0 ES
004FEC5D	8945 A4	mov dword ptr ss:[ebp-0x5C],eax	P 1 CS
004FEC60	8945 B4	mov dword ptr ss:[ebp-0x4C],eax	A 0 SS
004FEC63	8945 C4	mov dword ptr ss:[ebp-0x3C],eax	Z 1 DS
004FEC66	C745 9C 001C40	mov dword ptr ss:[ebp-0x64],cupofcof.00401C00	S 0 FS
004FEC6D	C745 94 080000	mov dword ptr ss:[ebp-0x6C],0x8	T 0 GS
004FEC74	FF15 38115000	call dword ptr ds:[&MSVBVM50. __vbaVarDup]	D 0
004FEC7A	8D55 A4	lea edx,dword ptr ss:[ebp-0x5C]	0 0 La
004FEC7D	8D45 B4	lea eax,dword ptr ss:[ebp-0x4C]	EFL 000
004FEC80	52	push edx	ST0 emp
004FEC81	8D4D C4	lea ecx,dword ptr ss:[ebp-0x3C]	ST1 emp
004FEC84	50	push eax	ST2 emp
00401C00-cupofcof.00401C00 (UNICODE "Incorrect password")			
堆栈 ss:[0012F30]-00000000			
地址	HEX 数据	ASCII	地址 数值 注释

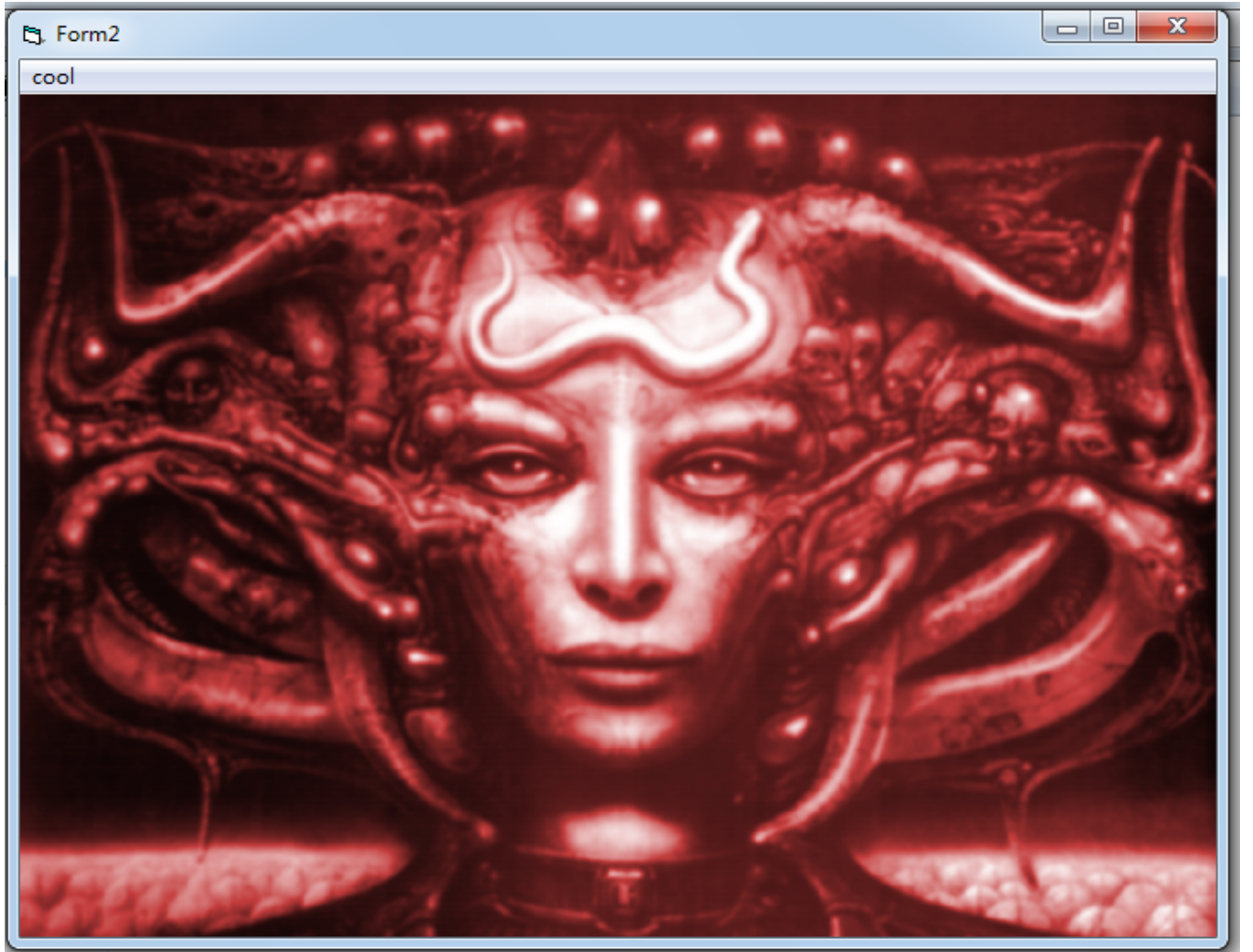
根据字符串的错误提示，跟进去，然后接着向上找。在上面你会发现一个比较函数，下断点，随便输入一个序列号等待程序断下。

地址	HEX 数据	反汇编	注释	寄存器 (FPU)		
004FEC07	68 D01B4000	push cupofcof.00401BD0		EAX 00000000		
004FEC0C	56	push esi		ECX 001E7F7C UNICODE "11111111111111111111"		
004FEC0D	50	push eax		EDX 00000004		
004FEC0E	FF15 D4105000	call dword ptr ds:[&MSVBVM50.__vbaHresultCheckObj]	msvbvm50.__vbaHresultCheckObj	EBX 004FFA5C cupofcof.004FFA5C		
004FEC14	8B4D E8	mov ecx,dword ptr ss:[ebp-0x18]		ESP 0012F3B0		
004FEC17	51	push ecx		EBP 0012F474		
004FEC18	68 E41B4000	push cupofcof.00401BE4		ESI 00345114		
004FEC1D	FF15 F8105000	call dword ptr ds:[&MSVBVM50.__vbaStrCmp]	msvbvm50.__vbaStrCmp	EDI 00000000		
004FEC23	8BF0	mov esi,eax		EIP 004FEC1D cupofcof.004FEC1D		
004FEC25	8D4D E8	lea ecx,dword ptr ss:[ebp-0x18]		C 0 ES 0023 32位 0(FFFFFFFF)		
004FEC28	F7DE	neg esi		P 1 CS 001B 32位 0(FFFFFFFF)		
004FEC2A	1BF6	sbb esi,esi		A 0 SS 0023 32位 0(FFFFFFFF)		
004FEC2C	F7DE	neg esi		Z 1 DS 0023 32位 0(FFFFFFFF)		
004FEC2E	F7DE	neg esi		S 0 FS 003B 32位 7FFDE000(FFF)		
004FEC30	FF15 4C115000	call dword ptr ds:[&MSVBVM50.__vbaFreeStr]	msvbvm50.__vbaFreeStr	T 0 GS 0000 NULL		
004FEC36	8D4D E4	lea ecx,dword ptr ss:[ebp-0x1C]		D 0		
004FEC39	FF15 50115000	call dword ptr ds:[&MSVBVM50.__vbaFreeObj]	msvbvm50.__vbaFreeObj	0 0 LastErr ERROR_SUCCESS (00000000)		
004FEC3F	66:3BF7	cmp si,di		EFL 00000246 (NO,NB,E, BE, NS, PE, GE,		
004FEC42	74 6E	je short cupofcof.004FECB2		ST0 empty 0.0		
004FEC44	B9 04000280	mov ecx,0x80020004		ST1 empty 0.0		
004FEC49	B8 0A000000	mov eax,0xA		ST2 empty 0.0		
esi=00345114						
地址	HEX 数据	反汇编	ASCII	地址	数值	注释
004FF000	00 00 00 00	00 00 00 00	20 15 1E 00	00 00 00 00	00401BE4	UNICODE "....."
004FF010	E8 1C 1E 00	00 00 00 00	00 00 00 00	00 00 00 00	98 4A 1E 00	?.....桶
004FF020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	.....
004FF030	00 00 00 00	00 00 00 00	00 00 00 00	00 00 40 00	00 0E 1D 00	.....@..
004FF040	48 16 01 0F	02 00 00 00	00 00 00 00	E4 19 40 00	H? ..?@.	
004FF050	2A 00 5C 00	41 00 44 00	3A 00 5C 00	56 00 42 00	*.\.A.D.:.\.V.B.	
004FF060	5C 00 50 00	41 00 53 00	53 00 57 00	4F 00 52 00	\.P.A.S.S.W.O.R.	
004FF070	44 00 2F 00	56 00 42 00	5A 00 00 00	00 00 00 00	D V R P	
0012F3B0	00401BE4					UNICODE "....."
0012F3B4	001E7F7C					UNICODE "11111111111111111111"
0012F3B8	0012F480					返回到 0012F480
0012F3BC	0012F55C					
0012F3C0	00344FFC					
0012F3C4	FFFFFFF					
0012F3C8	0012F408					
0012F3CC	770056D9					返回到 user32.770056D9.来自 Ink InkDrawTextF

看堆栈中有一个自己输入的序列号和一个字符串，这个字符串是十个英文状态下的点(.)。这个作者还是挺有意思的

## 验证结果

输入刚刚看到的序列号：十个点，记得把输入法调成英文



提示cool，成功了。

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