

[Code_Engn] Basic RCE L05

🕒 생성일	@2022년 12월 8일 오후 1:33
☰ 태그	Rev

Basic RCE L05

이 프로그램의 등록키는 무엇인가

— Author: Acid Bytes [CFF]
— File Password: codeengn



Crackers For Freedom CrackMe v3.0

Official CFF CrackMe v3.0	
<input type="text" value="Unregistered..."/>	Coder Acid Bytes [CFF]
<input type="text" value="754-GFX-IER-954"/>	Rel. Date 05/08/2000
Register now !	This is the official CFF CrackMe If you can manage to crack it, mail Name/Serial to: acidbytes@gmx.net
Quit the CrackMe	

실행화면

Beggar off! ✕

Wrong Serial,try again!

확인

String A	문자열
0044108C	"wrong Serial,try again!"
0044108C	"wrong Serial,try again!"

문자열 검색에서wrong을 검색해서 해당위치로 이동했습니다.

00440F1E	8D55 FC	lea eax,dword ptr ss:[ebp-4]	
00440F21	8883 C4020000	mov eax,dword ptr ds:[ebx+2C4]	
00440F27	E8 F4FEFFFF	call 05.420E20	
00440F2C	8845 FC	mov eax,dword ptr ss:[ebp-4]	
00440F2F	BA 14104400	mov edx,05.441014	441014:"Registered User"
00440F34	E8 F328FCFF	call 05.40382C	
00440F39	75 51	jne 05.440F8C	
00440F3B	8D55 FC	lea edx,dword ptr ss:[ebp-4]	
00440F3E	8883 C8020000	mov eax,dword ptr ds:[ebx+2C8]	
00440F44	E8 D7FEFFFF	call 05.420E20	
00440F49	8845 FC	mov eax,dword ptr ss:[ebp-4]	
00440F4C	BA 2C104400	mov edx,05.44102C	44102C:"GFX-754-IER-954"
00440F51	E8 D628FCFF	call 05.40382C	
00440F56	75 1A	jne 05.440F72	
00440F58	6A 00	push 0	
00440F5A	B9 3C104400	mov ecx,05.44103C	44103C:"CrackMe cracked successfully"
00440F5F	BA 5C104400	mov edx,05.44105C	44105C:"Congrats! You cracked this CrackMe!"
00440F64	A1 442C4400	mov eax,dword ptr ds:[442C44]	
00440F69	8800	mov eax,dword ptr ds:[eax]	
00440F6B	E8 F8C0FFFF	call 05.43D068	
00440F70	75 32	jmp 05.440FA4	
00440F72	6A 00	push 0	
00440F74	B9 80104400	mov ecx,05.441080	441080:"Beggar off!"
00440F79	BA 8C104400	mov edx,05.44108C	44108C:"Wrong Serial,try again!"
00440F7E	A1 442C4400	mov eax,dword ptr ds:[442C44]	
00440F83	8800	mov eax,dword ptr ds:[eax]	

바로 위에서 시리얼키를 찾을 수 있었습니다.

답 : GFX-754-IER-954