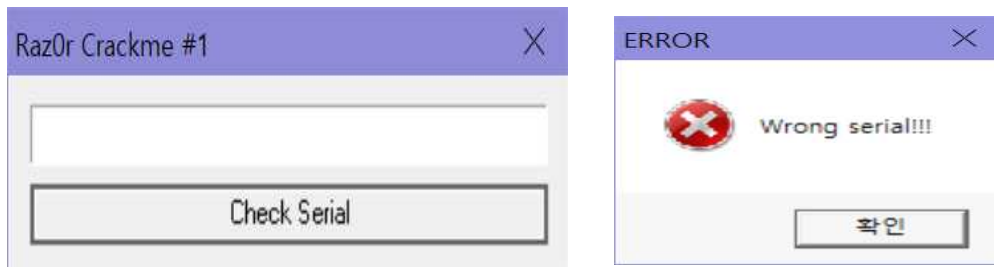


CodeEngn Basic RCE L06

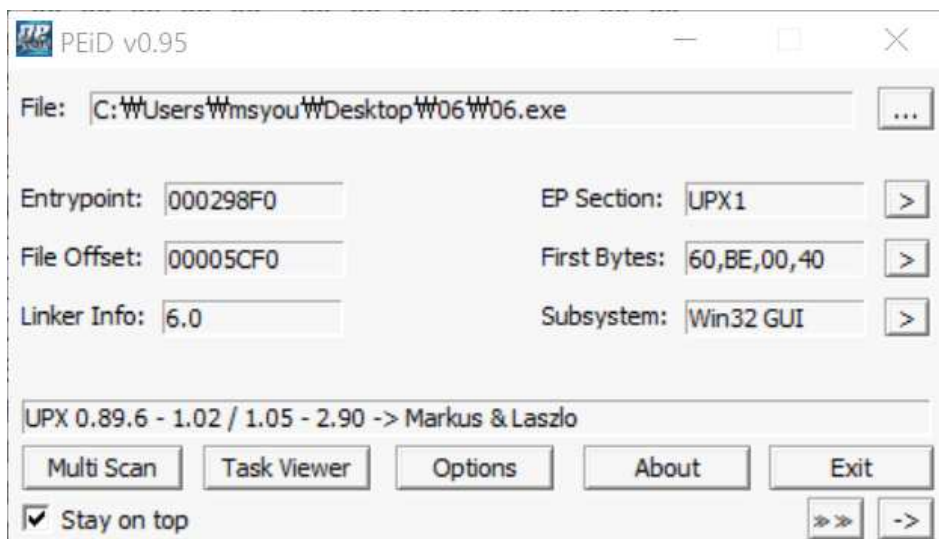
: Unpack을 한 후 Serial을 찾으시오.

정답인증은 OEP + Serial

Ex) 00400000PASSWORD



06.exe 실행하면 위와 같이 에러메세지가 나온다.



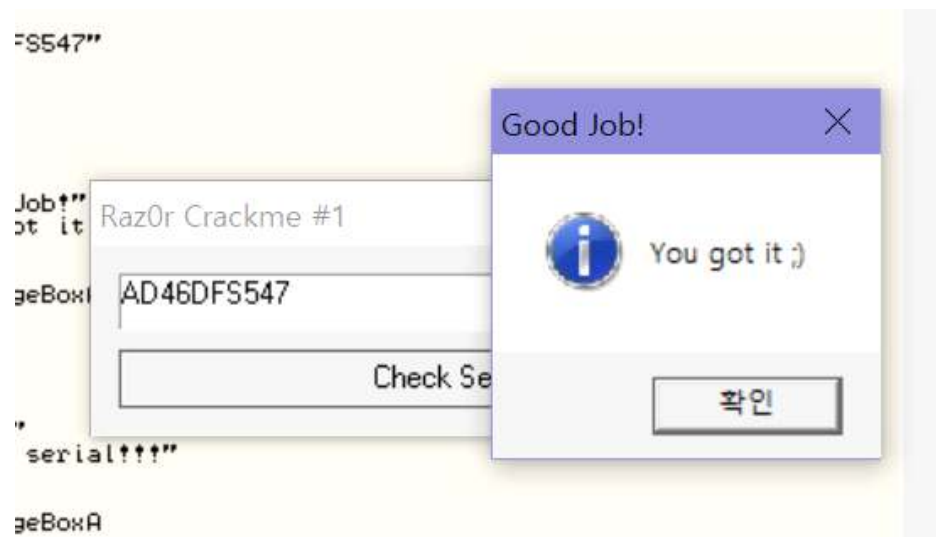
코드엔진 베이직을 5문제 풀어서 그런지 문제 풀때마다 루트가 일단 실행 한번 해보고 -> PEView로 봐주고, 패킹 의심되면 PEiD 틀어서 보는데 이번 문제는 5번 문제처럼 UPX로 패킹되어있었다.

00429A0B	> 8BAE 30940200	MOV EBP,DWORD PTR DS:[ESI+29430]	
00429A11	. 80BE 00F0FFFF	LEA EDI,DWORD PTR DS:[ESI-1000]	
00429A17	. BB 00100000	MOV EBX,1000	
00429A1C	. 50	PUSH EAX	
00429A1D	. 54	PUSH ESP	
00429A1E	. 6A 04	PUSH 4	
00429A20	. 53	PUSH EBX	
00429A21	. 57	PUSH EDI	
00429A22	. FFD5	CALL EBP	
00429A24	. 8087 EF010000	LEA EAX,DWORD PTR DS:[EDI+1EF]	
00429A2A	. 8020 7F	AND BYTE PTR DS:[EAX],7F	
00429A2D	. 8060 28 7F	AND BYTE PTR DS:[EAX+28],7F	
00429A31	. 58	POP EAX	
00429A32	. 50	PUSH EAX	
00429A33	. 54	PUSH ESP	
00429A34	. 50	PUSH EAX	
00429A35	. 53	PUSH EBX	
00429A36	. 57	PUSH EDI	
00429A37	. FFD5	CALL EBP	
00429A39	. 58	POP EAX	
00429A3B	. 61	POPAD	
00429A38	. 804424 80	LEA EAX,DWORD PTR SS:[ESP-80]	
00429A3F	> 6A 00	PUSH 0	
00429A41	. 39C4	CMP ESP,EAX	
00429A43	. ^75 FA	JNZ SHORT 06.00429A3F	
00429A45	. 83EC 80	SUB ESP,-80	
00429A48	. -E9 1379FDFF	JMP 06.00401360	
00429A4D	. 00	DB 00	
00429A4E	. 00	DB 00	
00429A4F	. 00	DB 00	
00429A50	. 00	DB 00	
00429A51	. 00	DB 00	
00429A52	. 00	DB 00	
00429A53	. 00	DB 00	
00429A54	. 00	DB 00	
00429A55	. 00	DB 00	

search for로 popad를 찾아주고, 그 뒤로의 명령어들을 읽어보면 BP걸어둔 JMP명령어가 위치하는 곳이 OEP라는 것을 알 수 있다. 즉 00401360이 OEP시작주소이다.

00401043	8BF4	MOV ESI,ESP	
00401044	6A 64	PUSH 64	
0040104C	68 D4354200	PUSH 06.004235D4	
00401051	68 E8030000	PUSH 3E8	
00401056	A1 38364200	MOV EAX,DWORD PTR DS:[423638]	
0040105B	50	PUSH EAX	
0040105C	FF15 B0524200	CALL DWORD PTR DS:[4252B0]	USER32.GetDlgItemTextA
00401062	3BF4	CMP ESI,ESP	
00401064	E8 B7020000	CALL 06.00401320	
00401069	68 D4354200	PUSH 06.004235D4	
0040106E	68 302A4200	PUSH 06.00422A30	ASCII "AD46DFSS47"
00401073	E8 18020000	CALL 06.00401290	
00401078	83C4 08	ADD ESP,8	
0040107B	85C0	TEST EAX,EAX	
0040107D	^75 24	JNZ SHORT 06.004010A3	
0040107F	8BF4	MOV ESI,ESP	
00401081	6A 40	PUSH 40	
00401083	68 48004200	PUSH 06.00420048	ASCII "Good Job!"
00401088	68 38004200	PUSH 06.00420038	ASCII "You got it ;)"
0040108D	8B0D 38364200	MOV ECX,DWORD PTR DS:[423638]	
00401093	51	PUSH ECX	
00401094	FF15 B4524200	CALL DWORD PTR DS:[4252B4]	USER32.MessageBoxA
0040109A	3BF4	CMP ESI,ESP	
0040109C	E8 7F020000	CALL 06.00401320	
004010A1	^EB 22	JMP SHORT 06.004010C5	
004010A3	8BF4	MOV ESI,ESP	
004010A5	6A 10	PUSH 10	
004010A7	68 30004200	PUSH 06.00420030	ASCII "ERROR"
004010AC	68 1C004200	PUSH 06.0042001C	ASCII "Wrong serial!!!"
004010B1	8B15 38364200	MOV EDX,DWORD PTR DS:[423638]	
004010B7	52	PUSH EDX	
004010B8	FF15 B4524200	CALL DWORD PTR DS:[4252B4]	USER32.MessageBoxA
004010BE	3BF4	CMP ESI,ESP	
004010C0	E8 5B020000	CALL 06.00401320	
004010C5	33C0	XOR EAX,EAX	

OEP로 들어가는 해당 명령어에 BP를 걸고 F9->F8을 누르면 위와 같은 화면이 나오는데, 나는 우연인지 모르겠지만 바로 Wrong serial 부분이 나왔다.아닌 사람들은 string 찾기로 Wrong을 검색하면 될것이라고 생각한다.



Good job! 윗 부분에 "AD~~~~"로 시작하는 부분이 시리얼 번호라는 것을 추측할 수 있다.