

codeengn Basic RCE L16



search reference text string

| | | | |
|----------|--------------|--|-------------------------|
| 004015BF | 890424 | MOV DWORD PTR SS:[ESP],EAX | |
| 004015C2 | EB 89F60000 | CALL <JMP.&KERNEL32.SetConsoleTextAttribute> | SetConsoleTextAttribute |
| 004015C4 | 83EC 08 | SUB ESP,8 | |
| 004015CA | C74424 04 A8 | MOV DWORD PTR SS:[ESP+4],16.0043B1A8 | |
| 004015D2 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 004015D9 | EB 528D0200 | CALL 16.0042A330 | |
| 004015DE | C74424 04 D9 | MOV DWORD PTR SS:[ESP+4],16.004400D9 | ASCII " Good Job!" |
| 004015E6 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 004015F1 | EB F6000200 | CALL 16.0043C3D8 | |

good job 앞에 있는 이 함수인거 같아서 bp 설정해봤으나, 걸리지 않음. 실패.

| | | | |
|----------|--------------|--------------------------------------|---------------------------------------|
| 00401442 | EB 528D0200 | CALL 16.0042A330 | |
| 00401447 | C74424 04 35 | MOV DWORD PTR SS:[ESP+4],16.00440035 | ASCII " ReWrit's Crackme#5" |
| 0040144F | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 00401456 | E8 7DAF0300 | CALL 16.0043C3D8 | |
| 0040145B | C74424 04 4C | MOV DWORD PTR SS:[ESP+4],16.0044004C | ASCII " *****" |
| 00401463 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 0040146A | E8 69AF0300 | CALL 16.0043C3D8 | |
| 0040146F | C74424 04 6C | MOV DWORD PTR SS:[ESP+4],16.0044006C | ASCII " * This is my 5th crackme, * |
| 00401477 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 0040147E | E8 55AF0300 | CALL 16.0043C3D8 | |
| 00401483 | C74424 04 8C | MOV DWORD PTR SS:[ESP+4],16.0044008C | ASCII " * i hope you will enjoy it. * |
| 0040148B | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 00401492 | E8 41AF0300 | CALL 16.0043C3D8 | |
| 00401497 | C74424 04 4C | MOV DWORD PTR SS:[ESP+4],16.0044004C | ASCII " *****" |
| 0040149F | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 004014A6 | E8 2DAF0300 | CALL 16.0043C3D8 | |
| 004014AB | C74424 04 AC | MOV DWORD PTR SS:[ESP+4],16.004400AC | ASCII " " |
| 004014B3 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |
| 004014BA | E8 19AF0300 | CALL 16.0043C3D8 | |
| 004014BF | C74424 04 AF | MOV DWORD PTR SS:[ESP+4],16.004400AF | ASCII " Enter your Name: " |
| 004014C7 | C70424 C0334 | MOV DWORD PTR SS:[ESP],16.004433C0 | |

CALL 0043C3D8은 print 인 듯하다.

| | | | |
|----------|---------------|--------------------------------------|--|
| 0040159C | 8B45 C0 | MOV EAX,DWORD PTR SS:[EBP-40] | |
| 0040159F | 3B45 C4 | CMP EAX,DWORD PTR SS:[EBP-3C] | |
| 004015A2 | 0F85 94000000 | JNZ 16.0040163C | |
| 004015A8 | C70424 F5FFF | MOV DWORD PTR SS:[ESP],-0B | |
| 004015AF | E8 8CF60000 | CALL <JMP.&KERNEL32.GetStdHandle> | |
| 004015B4 | 83EC 04 | SUB ESP,4 | |
| 004015B7 | C74424 04 80 | MOV DWORD PTR SS:[ESP+4],16.00440080 | |

내려가다 보니 0x004015A2에서 JNZ가 있고, 성공과 실패 구문이 나뉜다.

| | | | |
|----------|---------------|--------------------------------------|--|
| 0040159C | C70424 00344 | MOV DWORD PTR SS:[ESP],16.00443400 | |
| 0040159E | E8 B2740200 | CALL 16.00428A40 | |
| 004015B8 | 8B45 C4 | MOV EAX,DWORD PTR SS:[EBP-3C] | |
| 00401591 | 69D0 00CE0A00 | IMUL EDX,EAX,0ACE0A00 | |
| 00401597 | 8D45 C4 | LEA EAX,DWORD PTR SS:[EBP-3C] | |
| 0040159A | 0110 | ADD DWORD PTR DS:[EAX],EDX | |
| 0040159C | 8B45 C0 | MOV EAX,DWORD PTR SS:[EBP-40] | |
| 0040159E | 3B45 C4 | CMP EAX,DWORD PTR SS:[EBP-3C] | |
| 004015A2 | 0F85 94000000 | JNZ 16.0040163C | |
| 004015B7 | C74424 04 80 | MOV DWORD PTR SS:[ESP+4],16.00440080 | |

CMP에서 무엇과 무엇을 비교하는지를 중점적으로 살펴보자.

이것저것을 계속 대입해본 결과, EAX에는 내가 패스워드로 입력한 숫자가 들어감을 알 수 있었다. 반면, DWORD PTR [EBP-3C]는 항상 고정된 값이 들어가는 것을 확인하였다.

$ebp-40$
 $ebp-3c$

| | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|
| 0070FEE4 | CC | FF | 70 | 00 | 4E | 61 | BC | 00 |
| 0070FEEC | 97 | 0D | C6 | E4 | 4C | 28 | 12 | 00 |
| 0070FEF4 | F4 | 85 | 4F | 77 | 79 | 92 | 51 | 77 |
| 0070FEFC | 00 | 3D | 12 | 00 | 3F | 72 | 00 | |
| 0070FF04 | 4F | 84 | 51 | 77 | 00 | 00 | 00 | |

참고로 여기에는 패스워드로 '12345678'을 입력하였고, 이를 16진수로 표현한 값이 'BC614E'이다. 따라서 $ebp-3c$ 의 값을 10진수로 변환해서 패스워드로 넣어주면 정답이다.
 정답은 383818485!

```

ReWrit's Crackme#5
*****
* This is my 5th crackme, *
* i hope you will enjoy it. *
*****

Enter your Name: CodeEngn
Enter your Password: 383818485
5

Good Job!
=)
  
```