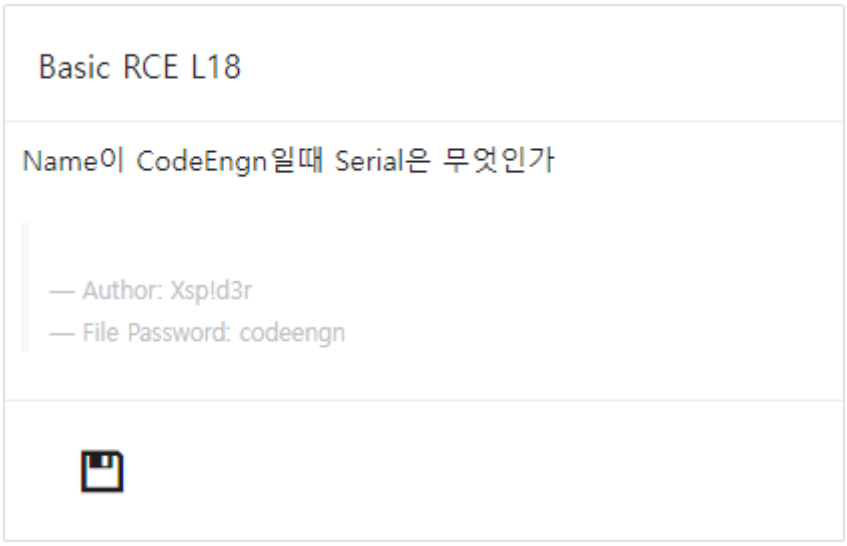
codeengn-basic-L18 풀이

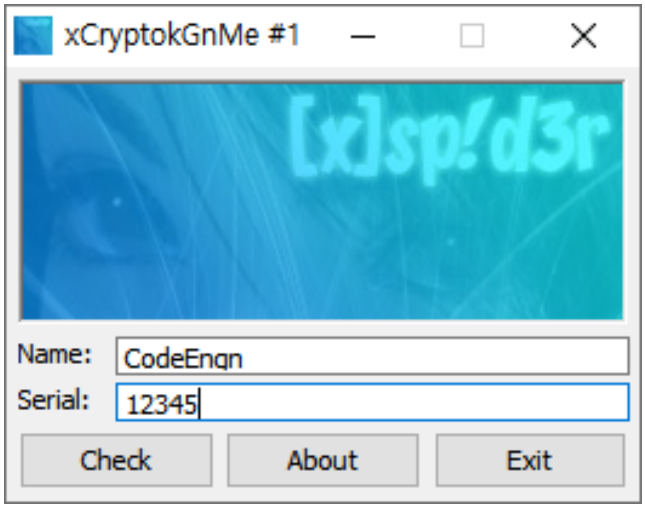
리버싱 문제풀이 / Wonlf / 2022. 4. 22. 11:38



문제는 Name이 CodeEngn일 때 Serial을 원하고 있다.

Die로 열어보니,

ARM Protector라는 것이 보이지만 일단은 먼저 실행시켜본다.



Serial은 아래 input을 얘기하는것 같다. 디버거로 열어본다.

```
004011E0   E8 01010000   call <JMP.&GetDlgItemTextA>
004011E5   68 F0804000   push 18.4080F0                  4080F0:"06162370056B6AC0"
004011EA   68 F07E4000   push 18.407EF0                  407EF0:"12345"
004011EF   E8 DA000000   call <JMP.&lstrcmpiA>
004011F4   0BC0          or eax,eax
004011F6   74 16         je 18.40120E
004011F8   6A 10         push 10
004011FA   68 04664000   push 18.406604                  406604:"Bad"
004011FF   68 E4654000   push 18.4065E4                  4065E4:"You serial is Wrong, try again"
00401204   FF75 08        push dword ptr ss:[ebp+8]
00401207   E8 E6000000   call <JMP.&MessageBoxA>
0040120C   EB 5C         jmp 18.40126A
0040120E   6A 40         push 40
00401210   68 3C664000   push 18.40663C                  40663C:"GOod"
00401215   68 08664000   push 18.406608                  406608:"Your serial is correct\r\n now you know what 2 do :p"
0040121A   FF75 08        push dword ptr ss:[ebp+8]
0040121D   E8 D0000000   call <JMP.&MessageBoxA>
00401222   C9            leave
00401223   C2 1000       ret 10
```

문자열 찾기로 성공 구문으로 가는 분기를 찾았다.

내가 입력한 문자열과 특정 값을 or연산을 한 값을 바탕으로 분기가 이루어지는데,

je는 제로플래그가 1일때와 cmp로 비교했을 때 같다면 점프를 하는 명령어이다.

eax를 or연산을 했을 때 0이 나오고 연산의 결과가 0이여야 제로플래그가 1로 세팅 되면서 je 구문에서 점프를 뛰기 때문에 istrcmpiA의 반환값이 0이여야 한다.

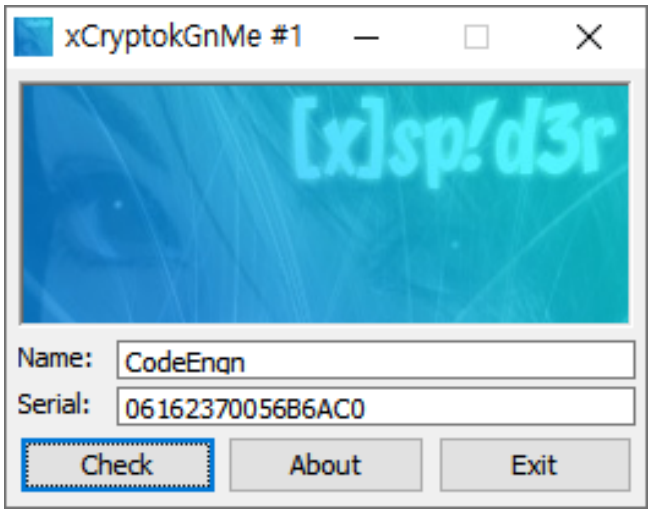
반환 값

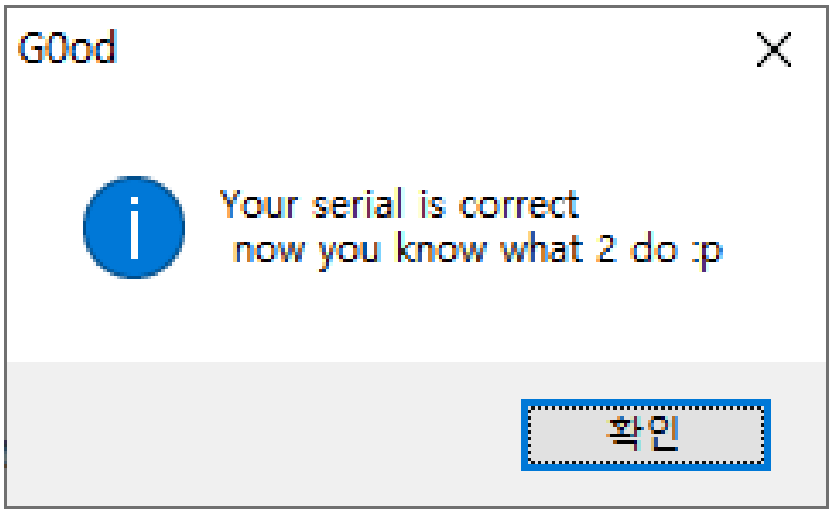
유형: **정수**

lpString1 이 가리키는 문자열이 *lpString2* 가 가리키는 문자열보다 작으면 반환 값은 음수입니다. *lpString1* 이 가리키는 문자열이 *lpString2* 가 가리키는 문자열보다 크면 반환 값은 양수입니다. **문자열이**

같으면 반환 값은 0입니다.

함수의 두 인자값이 같아야 반환값이 0이 되니 12345와 비교하던 문자열을 가져와 시리얼에 입력해보면,





맞다고 하고 페이지에도 인증을 해준다.