2013

Code Engn Basic 16

4.Z320

elttzero@gmail.com

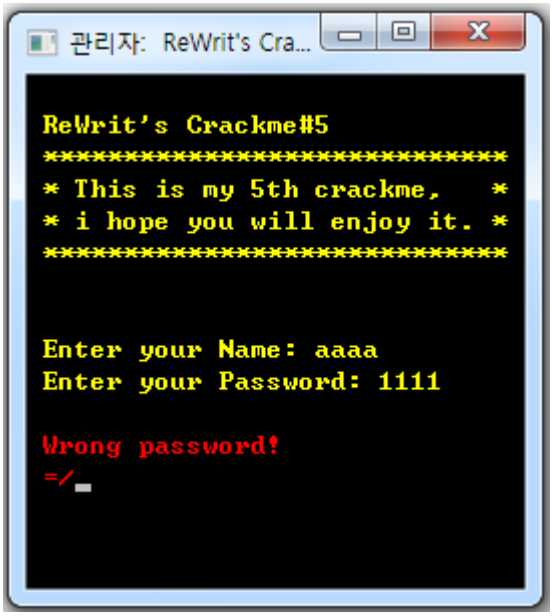
Challenges : Basic 16

Author : ReWrit

Korea :
Name이 CodeEngn일때 Serial을 구하시오

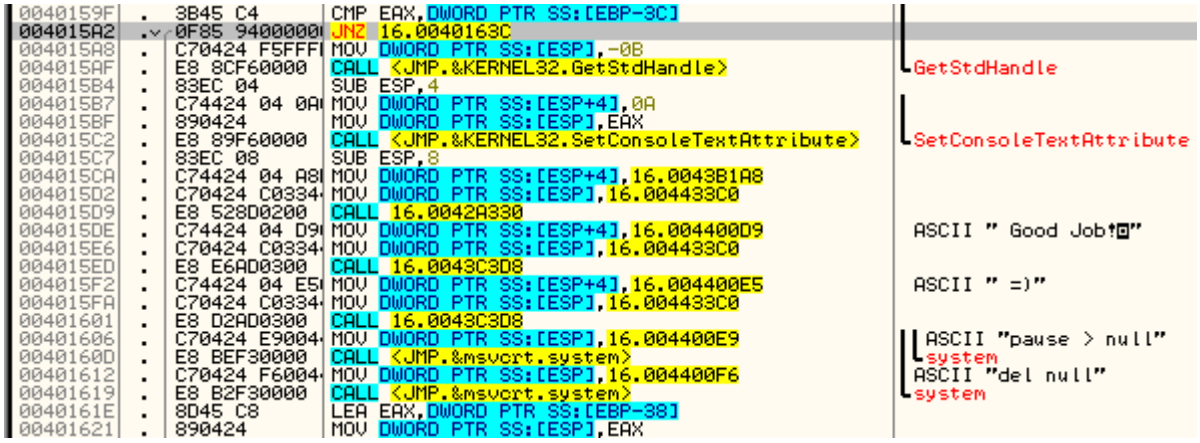
English :
Find the Serial when the Name is CodeEngn

Name 에 따른 Serial 을 구하는 문제입니다.



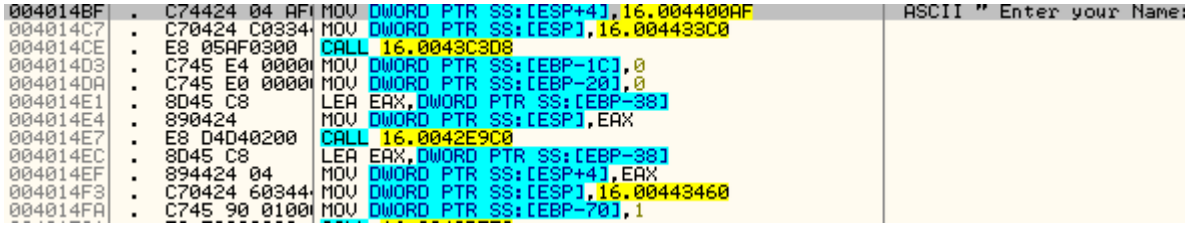
프로그램을 실행시켜 보면 Name 과 Serial 을 입력받고 그 결과를 출력해주는 것을 확인할 수 있습니다.

여기서 에러 메세지로 나온 'Wrong password!'를 따라가 보면 프로그램에 사용되는 문자열들이 모여있는것을 확인할 수 있고 거기서 조금만 위로 올리게 되면 JMP 문이 있는것을 찾을 수 있습니다.

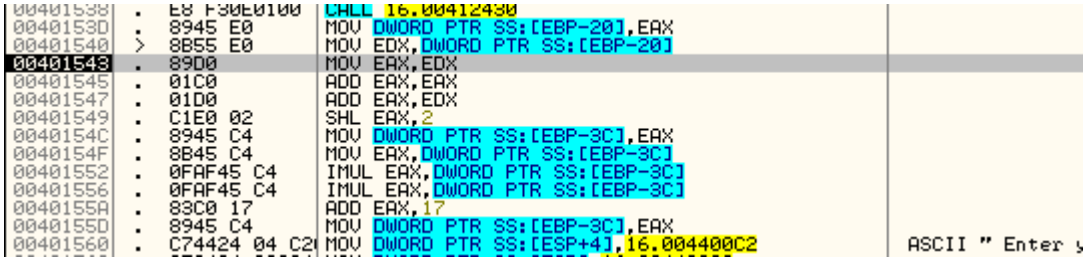


이 JMP 문과 그 위의 CMP 문을 보았을때 EAX 값과 [EBP-3C]값에 따라 이 프로그램의 성공유무가 나뉘는것을 확인할 수 있습니다.

이제 Name 과 Serial 을 처리하기 위한 함수를 찾아 위로 올려보면



이렇게 'Enter your Name : '과 함께 여러 함수가 호출되는것을 찾을 수 있고 여기서 Name 값을 변조한다는것을 찾을 수 있습니다.



Name 문자열의 길이는 [EBP-20]에 저장되어 있으며 이를 EAX, EDX 에 넣고 연산을 시작합니다.

우선 문자열의 길이를 3 번 더한 뒤 거기에 SHL 2 를 실시하고 그 값을 3 제곱 후에 17 을 더합니다. 그리고 이렇게 만들어진 값을 [EBP-3C]에 저장합니다.

이로서 CMP 구문에 나온 [EBP-3C]가 이 값임을 추측할 수 있습니다.

```
00401550  .  8945 C4       MOV DWORD PTR SS:[EBP-3C],EAX
00401560  .  C74424 04 C2  MOV DWORD PTR SS:[ESP+4],16.004400C2   ASCII " Enter your Passw
00401568  .  C70424 C0334  MOV DWORD PTR SS:[ESP],16.004433C0
0040156F  .  C745 90 0100  MOV DWORD PTR SS:[EBP-70],1
00401576  .  E8 5DAE0300   CALL 16.0043C3D8
0040157B  .  8D45 C0       LEA EAX,DWORD PTR SS:[EBP-40]
0040157E  .  894424 04     MOV DWORD PTR SS:[ESP+4],EAX
00401582  .  C70424 60344  MOV DWORD PTR SS:[ESP],16.00443460
00401589  .  E8 B2740200   CALL 16.00428A40
0040158E  .  8B45 C4       MOV EAX,DWORD PTR SS:[EBP-3C]
00401591  .  69D0 80CE0A0  IMUL EDX,EAX,0ACE80
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]
0040159F  .  3B45 C4       CMP EAX,DWORD PTR SS:[EBP-3C]
```

그 밑에있는 Serial 을 입력받는 구문입니다

EAX 에 [EBP-40]의 포인터를 주고 함수를 호출하여 값을 저장하는 것을 확인할 수 있습니다.

그리고 EAX 에 [EBP-3C]를 다시 입력하여 연산을 실시하는것을 볼 수 있습니다. 즉 Name 의 변조는 여기까지 해야지 끝나는 것입니다.

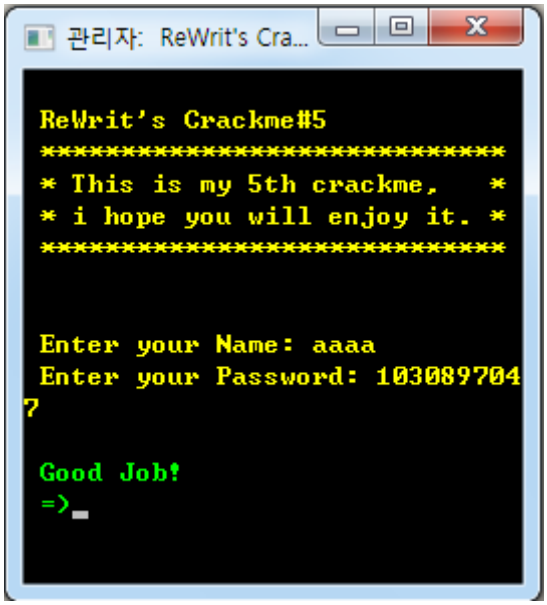
Name 의 변조에 대해 조금 적어보면 문자열의 길이를 x 라고 할때

y = {(x+x+x)*2*2}^3 + 17

z = y * ACE80 + y

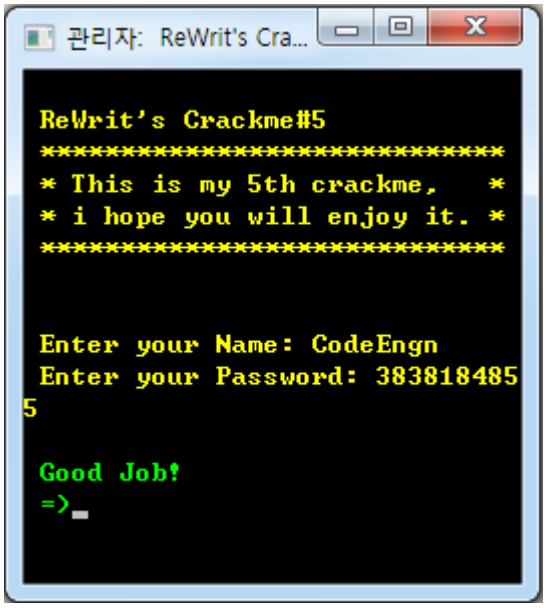
가 되어 z 값이 Serial 이 됩니다. (곱할때 DWORD 임을 감안하시고 계산하셔야 합니다)

X 에 입력한 Name 의 길이인 4 를 넣게 되면 3D723D97 이 나오게 되고 이를 10 진수로 바꿔서 넣게되면



이렇게 성공했다는 메세지가 나오게 됩니다.

이번 문제는 CodeEngn 일때의 값을 구하라고 했으므로 문자열 길이에 8 을 넣고 계산하게 되면 E4C60D97 이 나오게 되며 이를 10 진수로 고쳐서 입력하게 되면



이렇게 성공했다는 메세지가 나오게 됩니다.

그러므로 이번 문제의 답은 3838184855 가 됩니다.