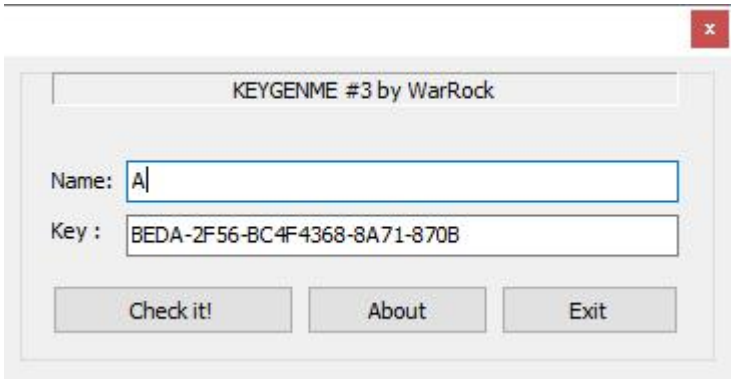
REPORT:

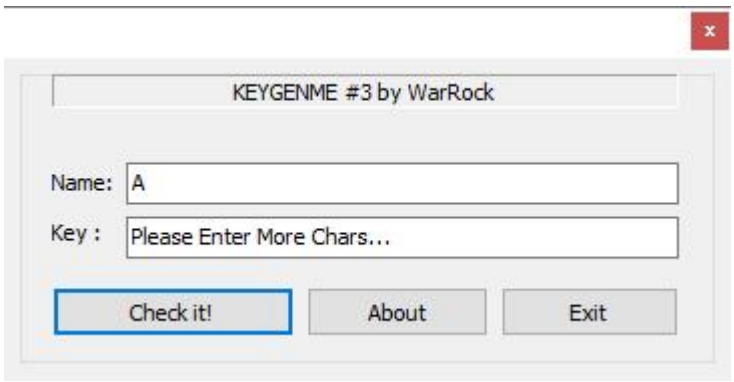
코드엔진 Basic RCE 17 Writeup

COLONY
1824275 정상지

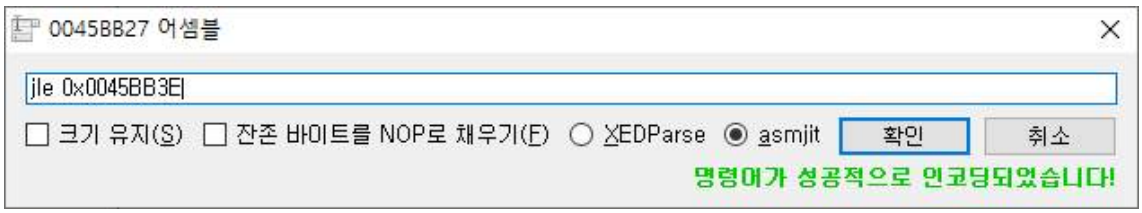
2021.07.24

Key 값이 BEDA-2F56-BC4F4368-8A71-870B 일때 Name은 무엇인가

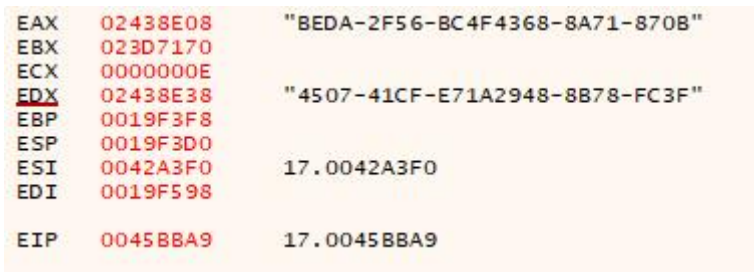


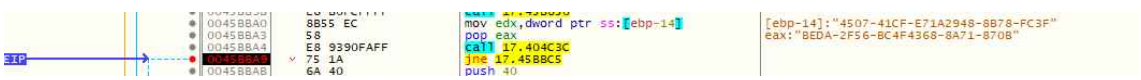


key값을 입력 후 확인 시 Please Enter More Chars라는 문구가 띄워지는 것을 확인할 수 있다
디버깅하여 해당 문자열의 크기를 확인하는 분기문에서 jge->jle로 바꾸어준다



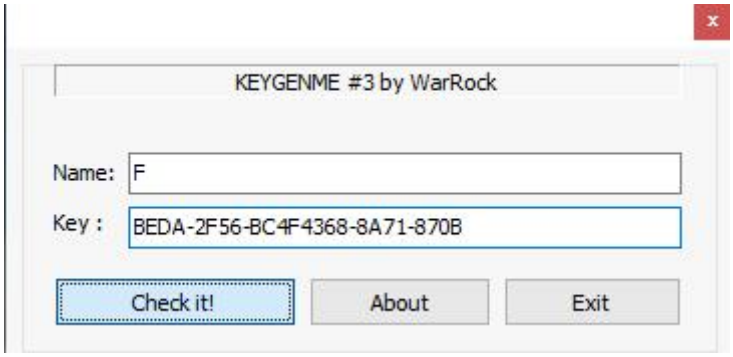
EAX에는 key값이 EDX에는 다른 값이 존재하는 것을 알 수 있다





edx의 값과 [ebp-14]의 값을 비교하는 분기문을 통해 password를 확인하는 것을 알 수 있다

힌트에서 문자가 한글자라고 하여 무작위 글자로 입력하여 분기문을 지나가는 값을 구한다



Name에 F입력 시 분기문을 통과한다

해당 글자의 MD5 값이 정답이므로

정답 : 800618943025315F869E4E1F09471012