

REPORT:

코드엔진 Basic

RCE 16 Writeup

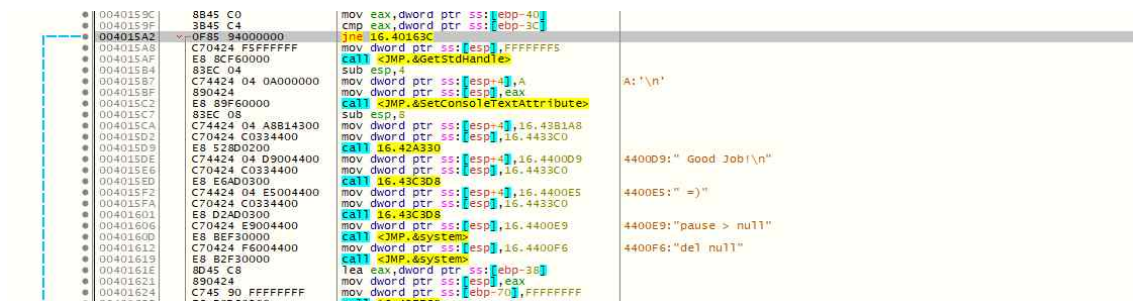
COLONY
1824275 정상지

2021.07.24

Name이 CodeEngn일때 Serial을 구하시오



해당 프로그램 실행 시 Name과 Password를 물어보고 무작위 password 입력 후 틀릴 경우 아래와 같이 Wrong password!라는 문자가 출력된다



문자열 참조를 통해 분기문을 확인한다

분기문에 중단점을 설정하고 디버깅한다

분기문은 EAX와 dword ptr ss:[ebp-3C]와 비교하는 것을 알 수 있다

EAX	00004D2	L 'A'
EBX	00004000	
ECX	00000000	
EDX	E4B88D80	
EBP	0070FF28	
ESP	0070FE70	"` 4D"
ESI	00401220	<16. EntryPoint>
EDI	00401220	<16. EntryPoint>
EIP	004015A2	16.004015A2

EAX레지스터에는 password의 hex값이 저장된다

```

eax=4D2 L 'A'
dword ptr ss:[ebp-3C]=[0070FEEC]=E4C60D97
.text:0040159F 16.exe:$159F #99F

```

ebp-3C의 값은 hex로 E4C60D97이다

E4C6 0D97

HEX E4C6 0D97
DEC 3,838,184,855

해당 dec값은 3838184855이다



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

Enter your Name: CodeEngn
Enter your Password: 3838184855
5

Good Job!
=)
```

해당 password를 입력하여 문제를 풀 수 있다

정답 : 3838184855