코드엔진 Basic RCE L17

문제

CodeEngn.com [코드엔진]

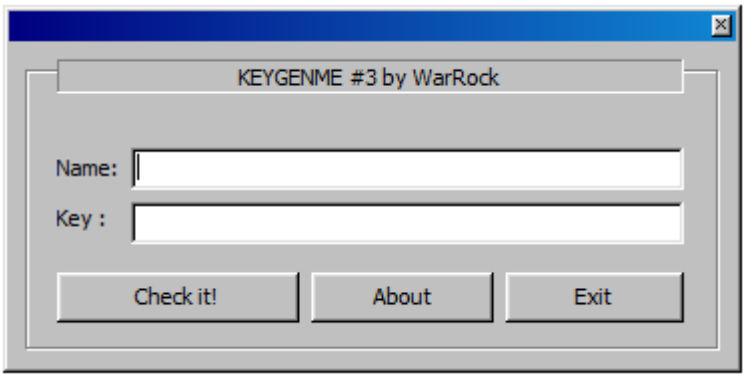
코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.

https://ch.codeengn.com/

의 Basic RCE L17

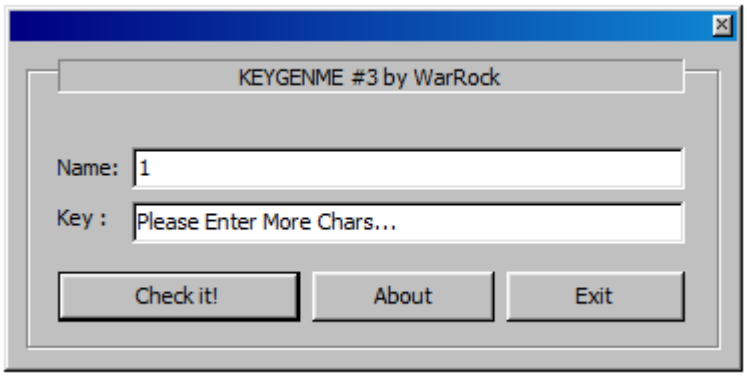
해결 과정

- 실행 파일을 실행해 보면 입력을 요구하는 두개의 칸을 볼 수 있습니다.



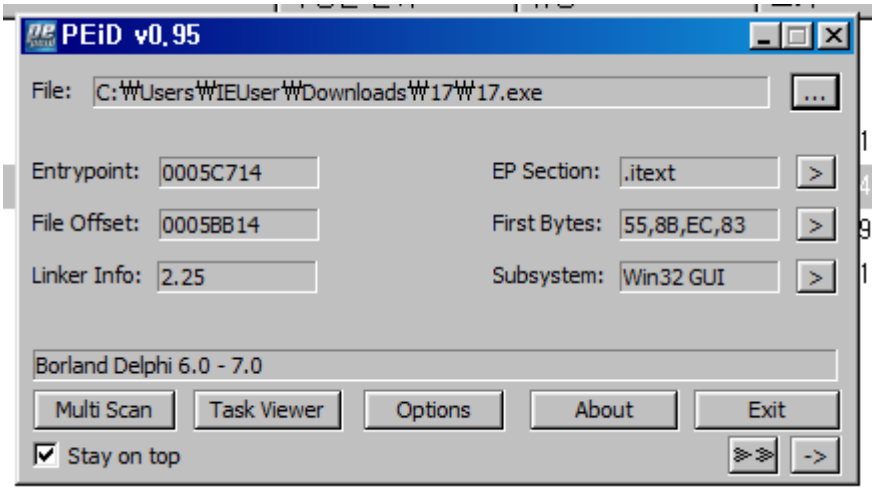
실행파일을 실행해 본 결과

- 칸에 문제에 있는 조건대로 Key는 BEDA-2F56-BC4F4368-8A71-870B로 넣고 Name은 한자리 숫자 아니면 알파벳을 넣어보면 Name이 더 길어야 한다고 Key 칸에서 알려주고 있습니다.



Name이 더 길어야 한다고 알려주는 실행파일

- 하지만, 문제의 조건으로 'Name은 한자리 숫자 아니면 알파벳이다.'가 있으므로 문제의 조건에 맞게끔 실행파일의 코드를 바꿔야 함을 알 수 있습니다.
- 다음으로, PEiD를 통해 실행파일의 정보를 파악합니다.



PEiD를 통해 보는 실행파일의 정보들

- 실행파일을 ollyDbg를 통해 바로 분석해도 문제가 없을 듯 하므로 ollyDbg로 분석을 시작합니다.
- 먼저, ollyDbg에서 모든 레퍼런스 되는 문자열들을 검색하면 성공시 출력되는 것으로 보이는 문자열들과 Name의 길이가 짧을 때 출력되는 문자열을 확인할 수 있습니다.

```
MOV     EDX, 0045BC18                ASCII "Please Enter More Chars..."
MOV     EDX, 0045BC3C                ASCII "Please Enter Not More Then 30 Chars..."
MOV     ECX, 0045BC64                ASCII "Good Boy!!!"
MOV     EDX, 0045BC70                ASCII "Well done!"
```

성공 시 출력되는 것으로 추정되는 문자열들과 Name의 길이가 짧을 때 출력되는 문자열

- 문자열을 클릭하면 그 문자열을 레퍼런스하는 명령어를 찾을 수 있는데, 먼저 길이가 짧을 때 출력되는 문자열을 클릭하여 그 근처에 비교하는 명령어가 있는지 확인해 보겠습니다.

```
CMP     EAX, 3
JGE     SHORT 0045BB3E
MOV     EDX, 0045BC18                ASCII "Please Enter More Chars..."
MOV     EAX, DWORD PTR DS:[EBX+374]
CALL    0043A0A4
JMP     0045BBCF
```

문자열을 레퍼런스 하는 코드와 그 코드의 주변 코드들

- 주변 명령어들을 살펴보면 ‘CMP EAX, 3’ 이라는 명령어가 보이고 그 아래에 ‘JGE SHORT 0045BB3E’ 라는 명령어가 보입니다.
- 이 명령어 두개는 EAX와 3을 비교한 후 EAX가 3보다 크거나 같으면 0045BB3E 부분으로 점프를 수행합니다.
- 그렇다면 EAX에는 어떤 값이 들어오는 지 확인해 보도록 하겠습니다.

Name 칸에 한자리 숫자를 넣었을 때

Name 칸에 두자리 숫자를 넣었을 때

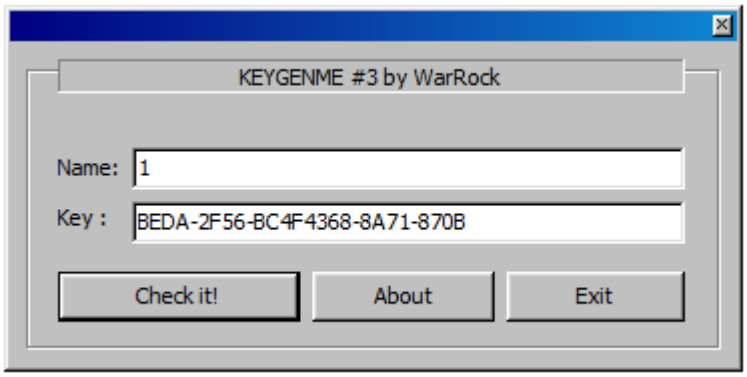
- Name 칸에 넣은 값의 자리에 따라 EAX 값이 바뀌는 것을 확인할 수 있습니다.
- 따라서, ‘CMP EAX, 3’ 명령어를 ‘CMP EAX, 1’로 바꾸어 주면 문제의 조건에 맞게 실행파일을 바꿀 수 있습니다.
- 실행파일의 내용을 바꾸기 위해 HxD라는 프로그램을 사용하겠습니다.

```
Offset(h)  00 01 02 03 04 05 06 07
0005AF20   E8 04 8B 00 83 F8 01 7D
```

HxD를 사용해 변경한 5AF26의 값

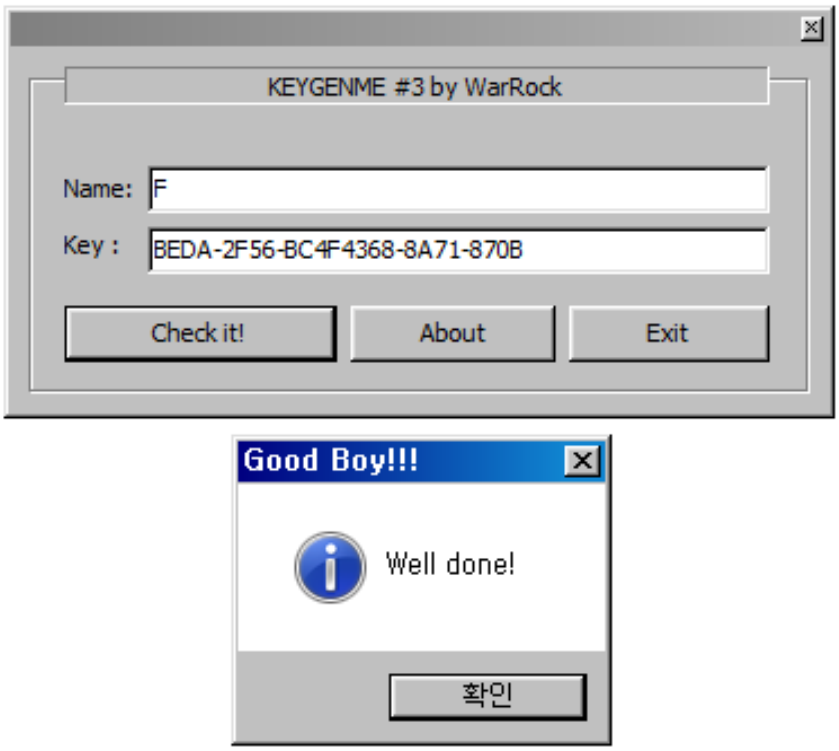
- 5AF24 부터 5AF26 까지가 원래 ‘CMP EAX, 3’ 명령어 값을 가지고 있던 주소입니다.
- 이 주소 범위에서 5AF26이 3의 값을 가지고 있었으므로 5AF26의 값을 1로 변경시켜 주었습니다.

- 실제로 실행해보면 Name이 한자리여도 Name의 길이가 짧을 때 출력되는 문자열이 출력되지 않는 것을 확인할 수 있습니다.



Name의 길이가 짧을 때 출력되는 문자열이 출력되지 않음

- 그 다음에는 문제의 조건에 맞는 Name 값을 하나 하나씩 입력하면서 브루트 포스 식으로 문제를 풀면 F가 알맞은 Name 값이라는 것을 확인할 수 있습니다.



알맞은 Name 값을 입력하자 성공 메시지 박스를 출력하는 실행파일

실행 구조

- 사용자로부터 Name과 Key라는 두개의 입력값을 받습니다.
- Name의 길이가 3미만인지 확인하여 3 미만이면 Name의 길이가 짧다는 문자열을 Key칸에 출력합니다.
- 마찬가지로 Name의 길이가 30초과 인지 확인하여 30초과면 길이가 30을 넘어서는 안된다는 문자열을 Key칸에 출력합니다.
- 다음으로 Name과 Key에 어떠한 처리를 수행합니다.
- 마지막으로 처리한 결과가 같다라는 상태로 나오면 성공 메시지 박스를 출력하고 그렇지 않으면 아무것도 출력하지 않고 두 경우 모두 다음 입력을 기다립니다.