코드엔진 Basic RCE L12

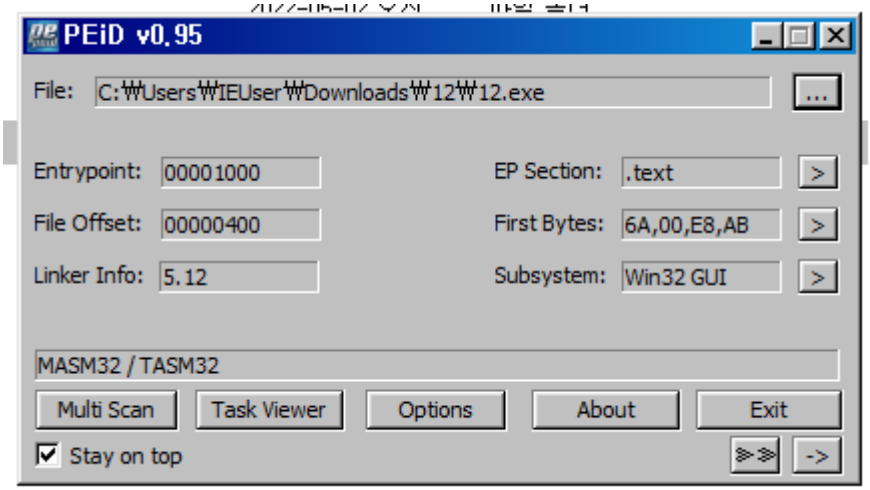
문제

> 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 L12

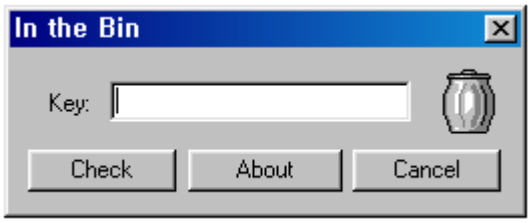
해결 과정

- PEiD를 사용하여 실행파일의 정보파악(압축여부, 프로그래밍 언어 종류등)



PEiD로 확인한 실행파일 정보

- 확인결과 압축되지 않은 파일임을 확인
- 실행파일 실행해 보기



실행 중인 실행파일

- 실행파일을 실행해 보니 key를 입력하는 칸이 존재하며, 아무 키나 입력하여 check 버튼을 눌러본 결과 아무런 창도 나타나지 않음
- ollyDbg에서 문자열 검색을 통해 알맞은 key를 입력할 시 나오는 문자열이 있는지 확인

Disassembly	Text string
MOV ESI, 00403000	(Initial CPU selection)
PUSH 00403530	ASCII "In the Bin"
PUSH 0040353B	ASCII "Congratulation, you found the right key"

문자열 검색 결과

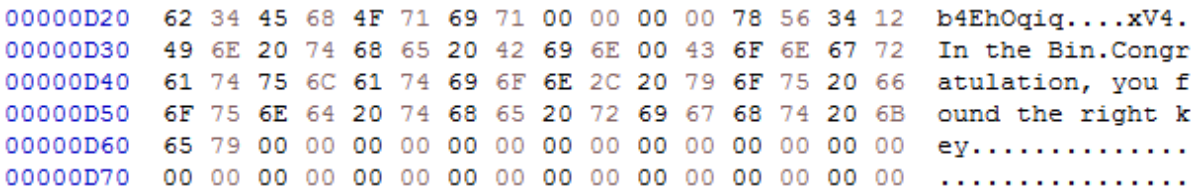
- 문자열 검색 결과 알맞은 key를 입력할시 나오는 것으로 추정되는 문자열 확인

```
0040105E   .  E8 31010000   CALL   <JMP.&USER32.GetDlgItemInt>   GetDlgItemInt
00401063   .  BE 00304000   MOV    ESI, 00403000                 ASCII "Oqiqb4E
00401068   >  833E 00       CMP    DWORD PTR DS:[ESI], 0
0040106B   .v 75 04         JNZ    SHORT 00401071
0040106D   .v EB 0E         JMP    SHORT 0040107D
0040106F   .v EB 0C         JMP    SHORT 0040107D
00401071   >  8B1E          MOV    EBX, DWORD PTR DS:[ESI]
00401073   .  E8 97000000   CALL   0040110F
00401078   .  83C6 04       ADD    ESI, 4
0040107B   .^ EB EB         JMP    SHORT 00401068
0040107D   >  3D BF96287A   CMP    EAX, 7A2896BF
```

실행파일의 어셈블리 실행 코드들

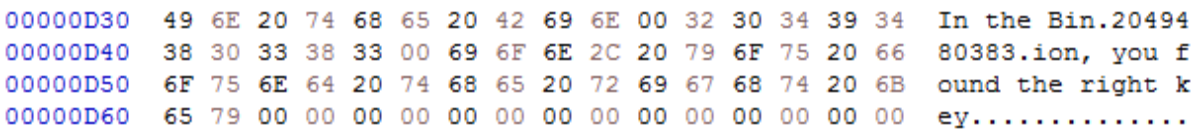
- 위 사진을 보면 getDlgItemInt 함수를 부른 직후와 어떠한 반복되는 로직이 끝난 직후에 바로 브레이크 포인트를 건 것을 볼 수 있는데 이를 통해 EAX 값의 변화를 확인할 수 있음
- 실제로 걸어 놓고 실행해 보면 getDlgItemInt 함수는 입력하는 칸을 통해 수를 입력받아 그 수를 16진수로 변환하여 EAX 레지스터에 저장하고 어떠한 반복되는 로직(시작과 끝을 포함한 빨간 화살표가 감싸는 코드들)이 끝난 이후에도 EAX의 값은 변하지 않는다는 것을 볼 수 있음
- EAX의 값이 변하지 않는 것이 중요한 이유는 맨 아래의 CMP(비교 명령어) 이후에 JNZ(CMP로 두 수를 비교하였을 때 다르면 점프 수행)로 분기가 나누어 지기 때문

- 점프가 발생할 경우 잘못된 키값을 입력한 것이고, 점프가 발생하지 않을경우 올바른 키값을 입력한 것임
- 다시 CMP로 돌아가면 CMP 명령어에서는 EAX의 값과 7A2896BF를 비교하고 있으므로 CMP로 비교할 시점에 EAX값이 7A2896BF이면 올바른 키값을 입력한 것
- 위에서 알아낸 것을 통해 7A2896BF를 10진수로 변환한 값이 올바른 키값임을 알 수 있음
- Key값이 성공메시지 대신 messageBox에 출력되도록 하기위해 HxD를 사용



HxD로 성공문자열과 성공문자열이 위치한 곳의 주소를 볼 수 있음

- Congratulation,... 문자열의 맨 처음 단어인 C부터 시작하여 문자열을 Key값으로 바꾸어야 함
- 단, 문자열의 마지막은 null값이어야 함



성공문자열대신 key 값이 출력되도록 문자열을 변경한 결과

- 이 방법을 통해 0x0D3B부터 0x0D45 까지가 key 값을 출력하기 위해 overwrite해야할 범위임을 알 수 있음
- 따라서 정답은 20494803830D3B0D45 임을 알 수 있음