

코드엔진 Basic RCE L19

문제

CodeEngn.com [코드엔진]

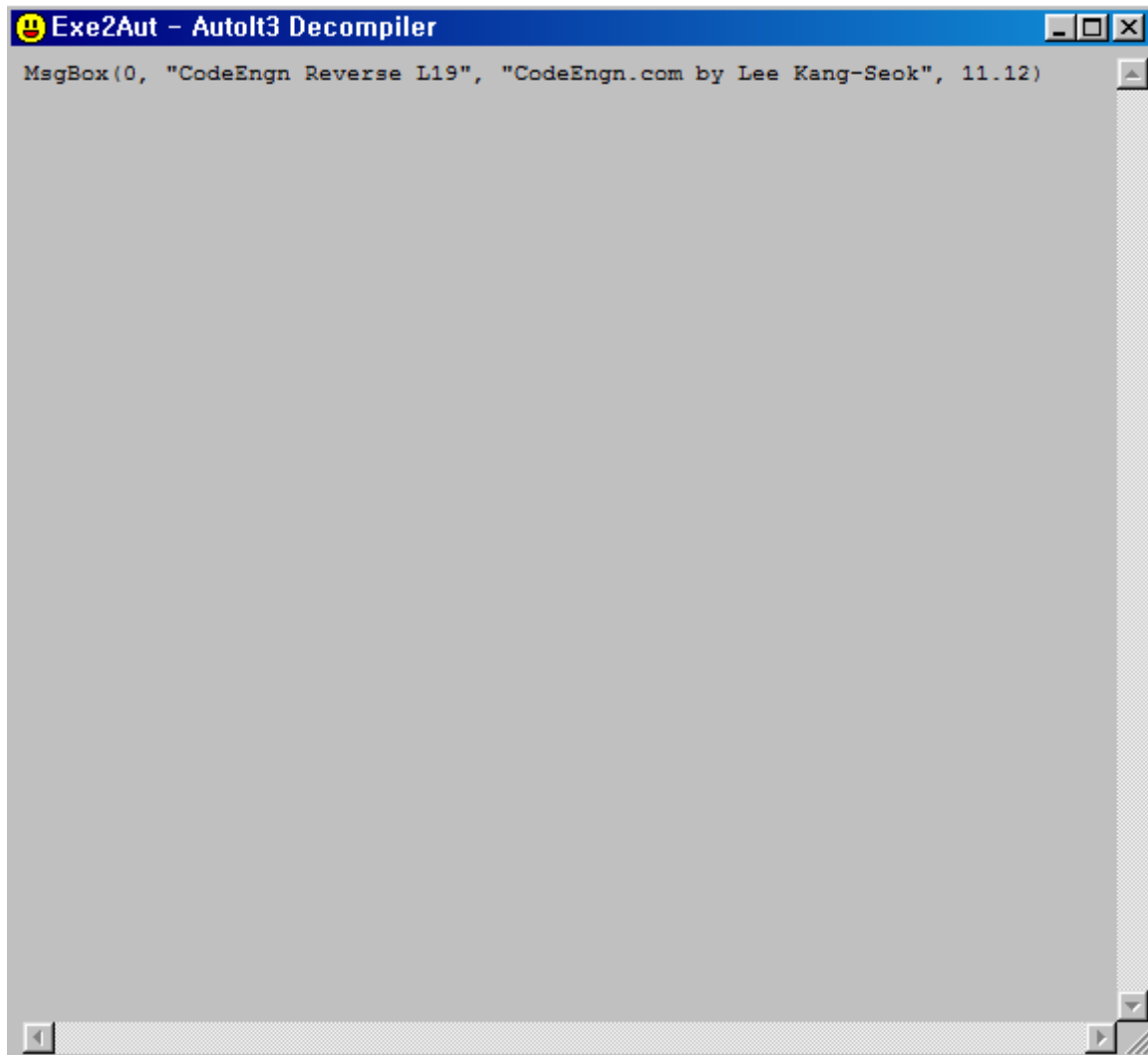
코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을
현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.

 <https://ch.codeengn.com/>

의 Basic RCE L19

해결 과정

- 이 실행파일은 AutoIt 프리웨어 자동화 언어로 작성한 것으로 AutoIt의 버전 3를 사용하였습니다.
- 그렇기에 ollyDbg로 분석하기 어렵습니다.
- 하지만, exe2aut이라는 AutoIt 버전 3용 디컴파일러를 사용하여 디버깅을 쉽게 수행할 수 있습니다.



exe2aut을 사용하여 실행파일을 디버깅한 결과

- Autolt 사이트에서 제공하는 함수 레퍼런스에서 MsgBox에 대한 내용을 확인할 수 있는데 Msgbox의 4번째 인자가 timeout값을 넣어주는 인자로 나옵니다.
- 따라서 timeout 값은 11.12이므로 이 값을 밀리세컨드로 바꾸면 11120이 정답임을 알 수 있습니다.

실행구조

- autoit에서 제공하는 함수인 MsgBox를 사용하여 메시지 박스를 생성합니다.
- 이 메시지 박스는 확인버튼을 누르거나 누르지 않고 11.12초가 지나면 종료됩니다.