

코드엔진 Basic RCE L11

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 L11

해결 과정

- PEiD를 통해 실행파일이 upx로 패킹된 것을 파악
- POPAD와 JUMP OEP 사이에 있을 Stolenbyte를 파악
- upx로 실행파일을 언패킹한 후, OEP를 파악해 해결