코드엔진 Basic RCE L15

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 L15

해결 과정

- PEiD를 통해 실행파일을 조사한 결과 별다른 것이 없음을 확인
- 문자열 검색을 통해 성공시 출력하는 문자열을 찾음
- 성공시 출력하는 문자열을 이용하여 성공 메시지 박스를 출력하는 코드를 찾음
- 그 코드 위에 있는 비교 코드를 찾아 비교를 위해 사용하는 두 인자에 들어가는 값이 각각 Name과 Serial중 어떤 값에 의해 영향을 받는지 확인
- 이 실행파일에서는 EAX 레지스터와 메모리 주소 [45B844]번지를 인자로 하여 비교함수를 통해 값을 비교하고 있음
- 직접 값을 입력칸에 넣어 확인해 보면 EAX 레지스터는 Serial에 영향을 받고 메모리 주소 [45B844]번지는 Name에 영향을 받는 것을 알 수 있음
- 다음으로 Name은 유지하고 이전에 넣은 Serial값에 1을 더한 새로운 Serial값을 입력창에 넣음
- 그러면 EAX 레지스터도 똑같이 이전과 비교하여 1이 증가한 것을 확인할 수 있음
- 따라서, Serial 값을 구하려면 [45B844]번지의 값에서 EAX 레지스터의 값을 뺀것을 10진수로 변환하여 이 변환한 값과 현재 입력한 Serial값을 더하면 올바른 Serial을 알 수 있음
- Name으로 CodeEngn을 입력한 후, 이렇게 얻은 Serial을 입력하면 성공 메시지 박스를 출력하는 것을 확인할 수 있음