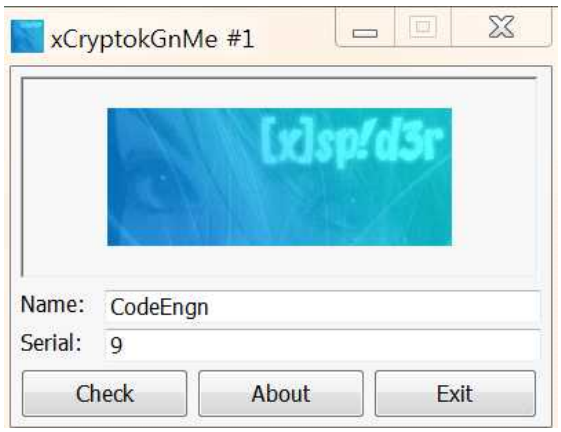
코드 엔진 Challenges: Basic 18

Author: Xsp!d3r
Korean: Name이 CodeEngn일 때 Serial은 무엇인가.

지금까지 진행하면서 많이 봐왔던 프로그램 형식이다.네임값에 따라서 시리얼이 생성되는 프로그램으로 이런한 프로그램을 자주 보다보니 일정한 형식이 있다는 것을 알 수 있다.

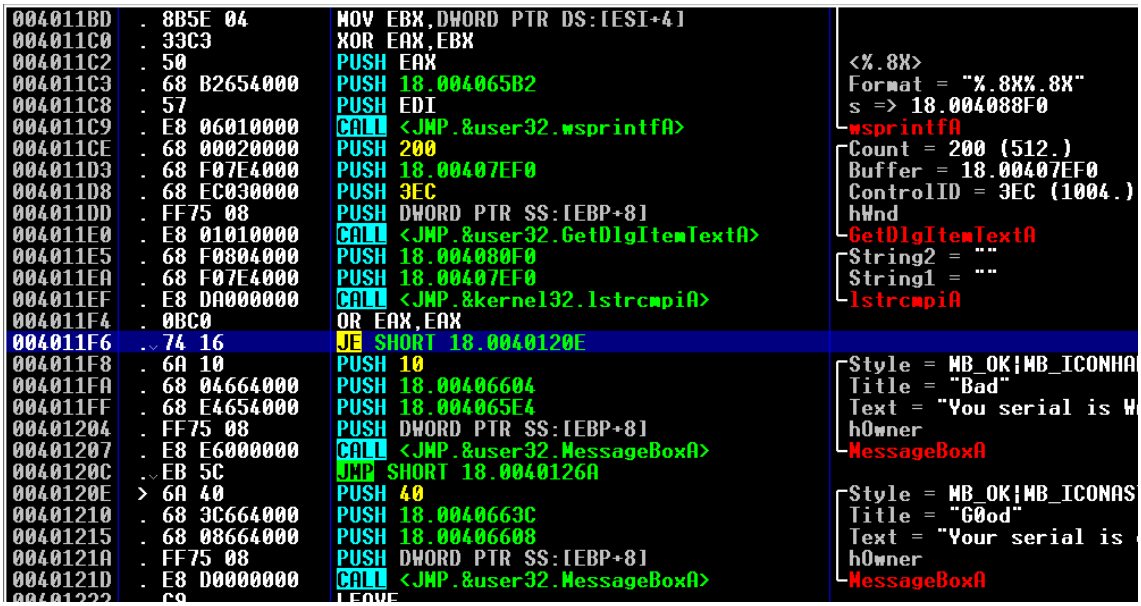


-사용자값 입력받음
-시리얼 생성
-시리얼 값과 사용자 값 비교
-분기
-메시지 출력

프로그램이 패킹되어있지 않으니 올리디버거를 통해 분석해보자.

```
004011A2 PUSH 18.004065B2          ASCII "%.8X%.8X"
004011C3 PUSH 18.004065B2          ASCII "%.8X%.8X"
004011FA PUSH 18.00406604          ASCII "Bad"
004011FF PUSH 18.004065E4          ASCII "You serial is Wrong, try again"
00401210 PUSH 18.0040663C          ASCII "G0od"
00401215 PUSH 18.00406608          ASCII "Your serial is correct! now you know what 2 do :p"
00401230 PUSH 18.00406000          ASCII "About"
```

아까 본 문자열을 찾아 분석하고 주소로 이동해보자.



다음과 같이 분기문을 확인 할 수있다 004011F6의 분기문에의해 해당 라인의 결과에 뜨라 성공/실패 메시지가 출력되는 것을 알 수 있다. 해당 분기문에서 사용되는 조건이 어디로부터 오는 것인지 확인하는 과정을 거치게 되면 문제가 해결될 것 같다. 그 위의 004011F4에서 OR EAX,EAX 명령을 수행하는데 있어 레지스터 EAX는 함수의 리턴 값을 담는 용도로 쓰이기에 바로 윗 라인에 사용되는 함수 lstrcmpiA의 리턴 값일 것이다. lstrcmpiA 함수는 두 문자열을 비교한 결과를 리턴하며 무엇을 비교하는지 알기 위해 004011EF에 BP를 걸고 값을 입력해보자.

입력한 시리얼 값 9가 String1에 입력되고 String2와 비교한 결과 값 1을 리턴하는 것을 알 수있따. String1과 String2를 비교했을 때 값은 달랐고 1이 반환 되었을 때 OR EAX,EAX를 진행했을 때 EAX에 1이 남아있었다 . 밑에 분기문에서 0이 아니기에 0040120E로 점프했고 시리얼이 잘못됐다는 메시지가 나오는데 따라서 String1과 String2의 값이 같아야 성공메시지가 출력되는 구문으로 분기하게 되며 사용자 입력값이었던 String1의 값과 비교되던 06162370056B6AC0이 옳은 시리얼 값임을 알 수 있다. 이 값을 입력해 인증을 해보자 .