[2-2] 분석

[1] load_passcode에서는 buffer overflow를 일으킬 수 없다. 무작위로 난수가 발생되기 때문에 버퍼오버플로우를 일으키는 것은 불가능하다.

[2] print_secret을 얻기 위해서는 무작위로 출력되는 난수와 내가 input한 코드가 같아야 한다. 그러나 무작위로 출력되는 난수를 맞출 수 없기 때문에 우리는 input을 buffer overflow를 시켜야 한다. - Input[20]

그래서 A*19를 하고 x00(null 문자)로 채워준다.

[3] 0x0000000000400b68 <+188>: lea 0x30(%rsp),%rdx

0x0000000000400b6d <+193>: lea 0x10(%rsp),%rax

이 두 어셈블리어를 통해 passcode와 input의 거리를 찾아준다. 48-16=32임을 알 수 있다.

이에 A*31+ x00(null 문자)로 채워준다.

그래서 이를 통해 python 코드를 만들어냈다.