# Bomb 实验

## +Phase 1

we execute the objdump-d command find the <phase_1>. Then we find mov $0x402400,%esi, in the function we find the value 0x402400. Border objdump-s. find 402400 border relations with Canada have never been better.
Answer: border relations with Canada have never been better.

## +Phase 2

we found a function <phase_2>, it has a function <read_six_numbers>, then we compare the first element. cmpl $0x1,(%rsp), then a series of deductions is carried out where it is compared with 2,4,8,16, 32
Answer: 1 2 4 8 16 32

## +Phase 3

In the function < phase_3> find when comparing elements from the file password, cmp $0x1,%eax ( we checked whether the first element is dec 1) then go to the line jmp 400fbe <phase_3+0x7b> with which
jump to the line mov $0x137,%eax and cmp 0xc (%rsp),%eax
where we see that the second number should equal 0x137(dec 311)
Answer: 1 311

## +Phase 4

in the function < phase_4> we call callq 400fce <func4> where we go to the function <func4> where is first value 3 so that the bomb does not explode, then we go back to <phase_4> where we find he second value is 0.
Answer: 3 0

## +Phase 5

In the function < phase_5> we call callq 40131b <string_length>, so answer should be String.
In movzbl 0x4024b0(%rdx),%edx find 4024b0 equal (maduiersnfotvbylSo you think you can stop the bomb with ctrl- #c, do you?" ) maduiersnfotvbyl is exactly 16 characters. mov %dl, 0x10(%rsp,%rax, 1) this command generates 6 characters. Find the string "flyers." that's probably the string you'll want to compare. From the above analysis, maduiersnfotvbyl respectively corresponding to the lower 0123456789abcdef character, so in order to generate"flyers "string, the low must be"9FE567", for example, "ionefg" can be.
Answer: ionefg

**+Phase 6**

In the function < phase_6> we call `callq 40145c <read_six_numbers>`, so answer should be 6 numbers. mov %rsp,%r14 rsp as the base address (stack) to read six numbers. Found the loop (6 times), respectively, to test whether the read number is less than or equal to 6 (the actual unsigned number minus 1 is less than or equal to #5, so 0 is not enough), the internal loop to compare the current number and the rest of the numbers are the same.To sum up is to require the six numbers are not the same#, and more than 0 less than 7, so the six numbers can be a combination of 123456. here I stopped and could do no more.