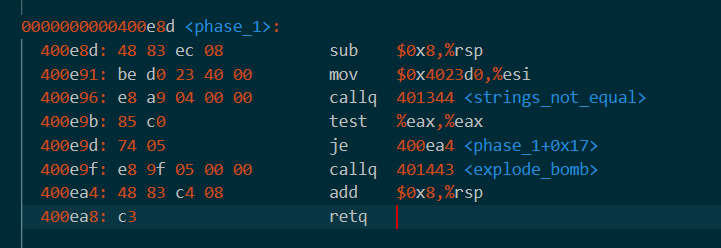
CA BOMB LAB(5)

YASH GUPTA  
S20200010234

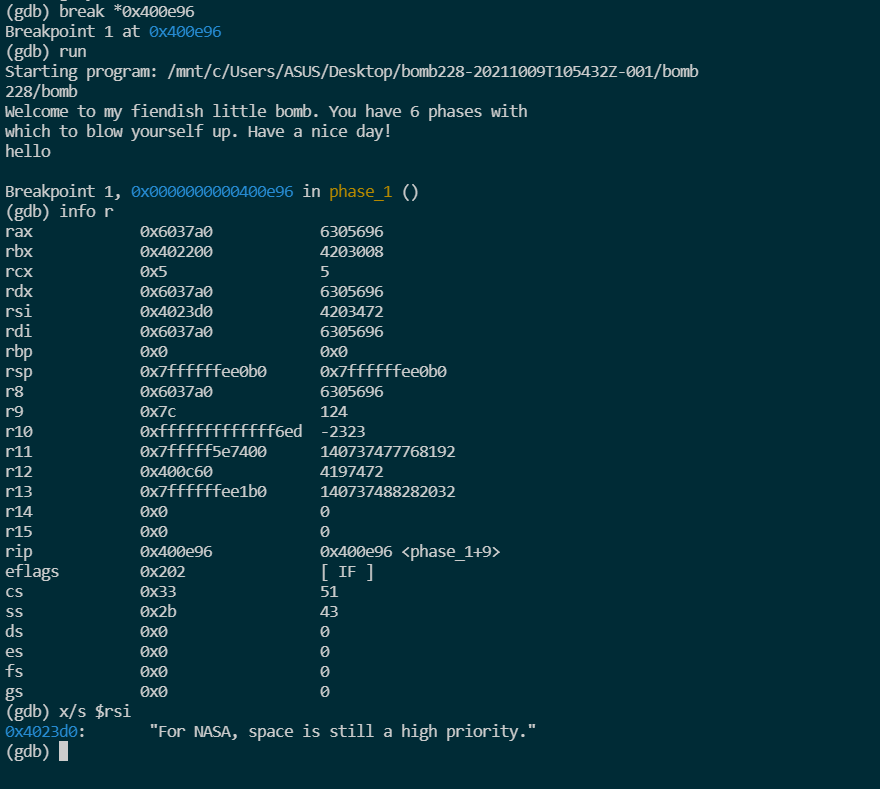
1. PHASE-1

>Set the break point at <String not equal> i.e address 0x400e96

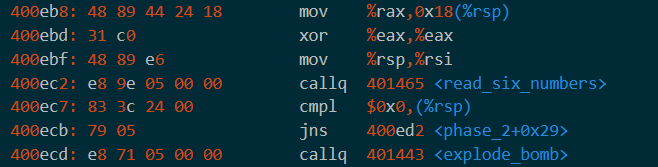


> Look for the register which contains the correct string value

> Check the value stored in register that is the correct key for phase 1

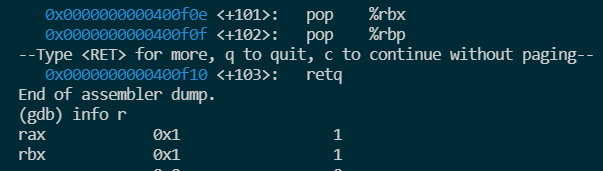
>Hence the string value =”For NASA, space is still a high priority.”

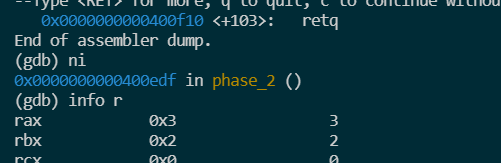
1. PHASE-2

>Assuming 6 numbers must be taken.

>From this we can conclude that the first number is 0 or else the bomb will explode.

>Run gdb and add a breakpoint at before theexplode\_bomb call in phase 2



>Check the register value for rax to get the next value. Then update the input given with the found value

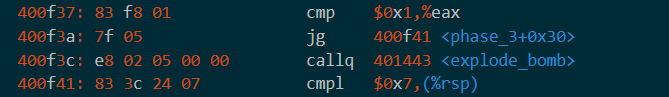
>Similarly repeat this process and find the value of all 6 digits

>After solving you will get the key as “0 1 3 6 10 15”

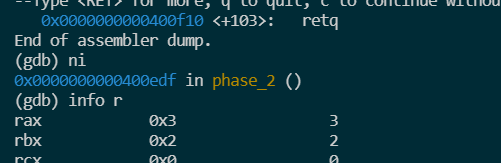
1. PHASE -3

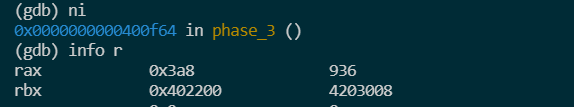
>By looking at the code we can conclude that the input consist two integers

>First integer is in the range of 1 to 7



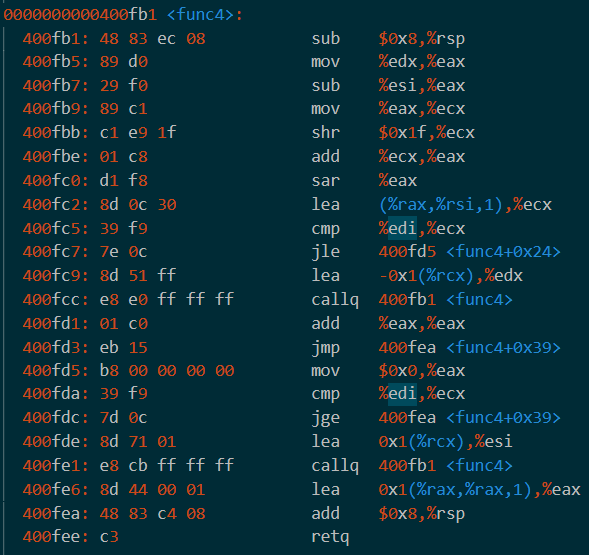
>By checking the value at registers we get both the values

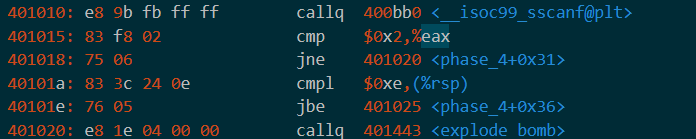




>Hence the key of this phase =”3 936”

1. PHASE 4

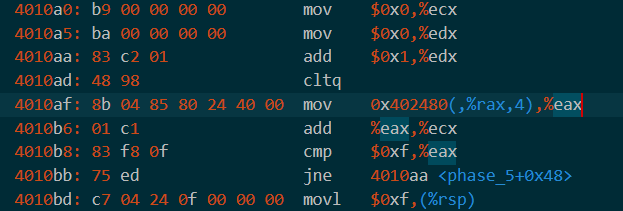
>After reading the whole phase\_4 code, we came to know that the key contains two integers and one of them is passed through a function called func4, it returns an integer and my key will be correct only if the returned number is equal to the other number of input.



>After checking the value at registers we came to know the key of phase 4 =”4 2”.

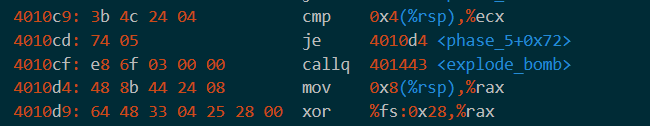
1. PHASE 5

> After reading the whole phase\_5 code, we came to know that the key contains two integers.



> In the above set of lines there is a loop running until eax is not equal to 15 and I must make sure that our edx should also be 15 or else the bomb will explode

> So, I’ve tried different values of first argument in key and when I kept 5 as first int in the key the gdb have surpassed the explode function, like this I got to know the first number is 5.

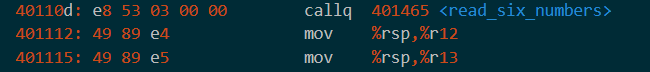


> In the above code it is comparing my second number with the value in ecx register So, I’ve used ‘info r’ to find what is the value stored there

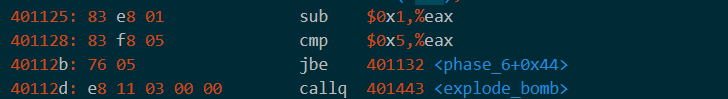
> Like this I got to know my second number of key is 115.

>Hence the final key of phase 5=”5 115”

1. PHASE 6



>From this we conclude there will be an input of 6 integers.



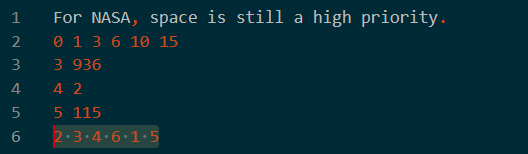
>The numbers will be between 1 to 6.

>From code we can conclude the numbers need to be unique.

>After further solving and checking the value of registers we can find each integers.

>Hence the final key i.e of phase\_6 =”2 3 4 561 5”

ALL KEYS:-



THANK YOU