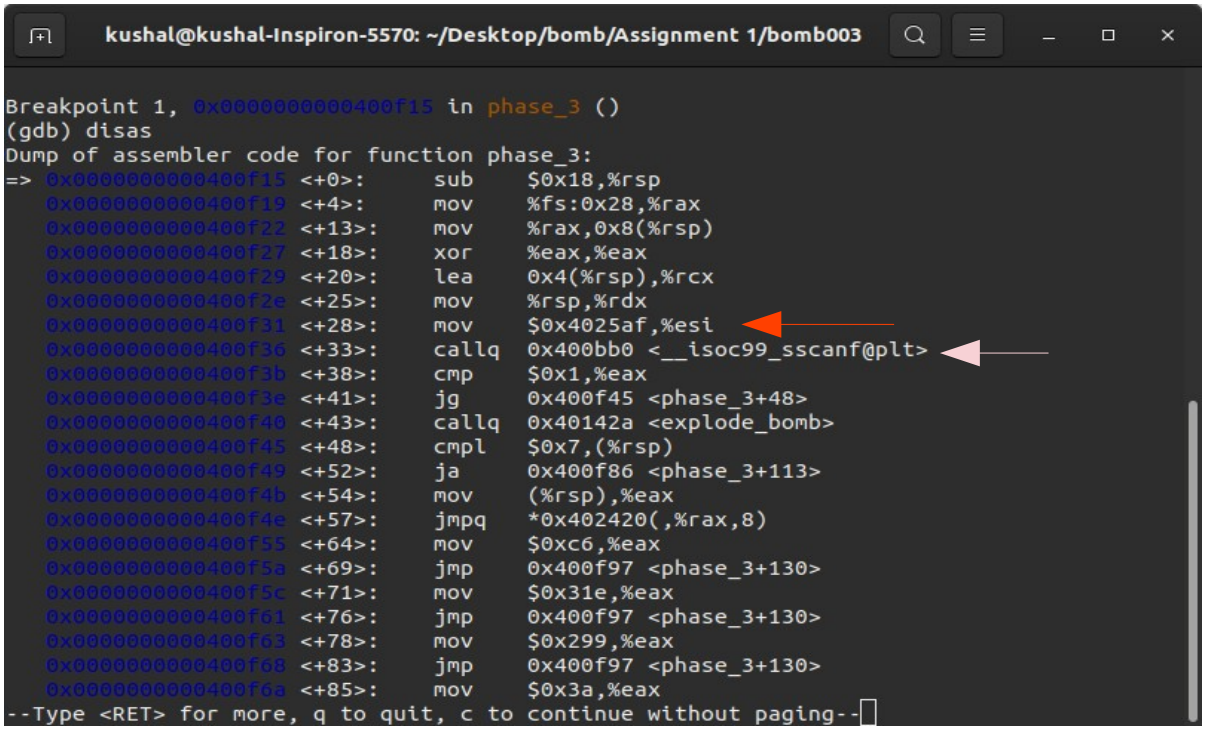
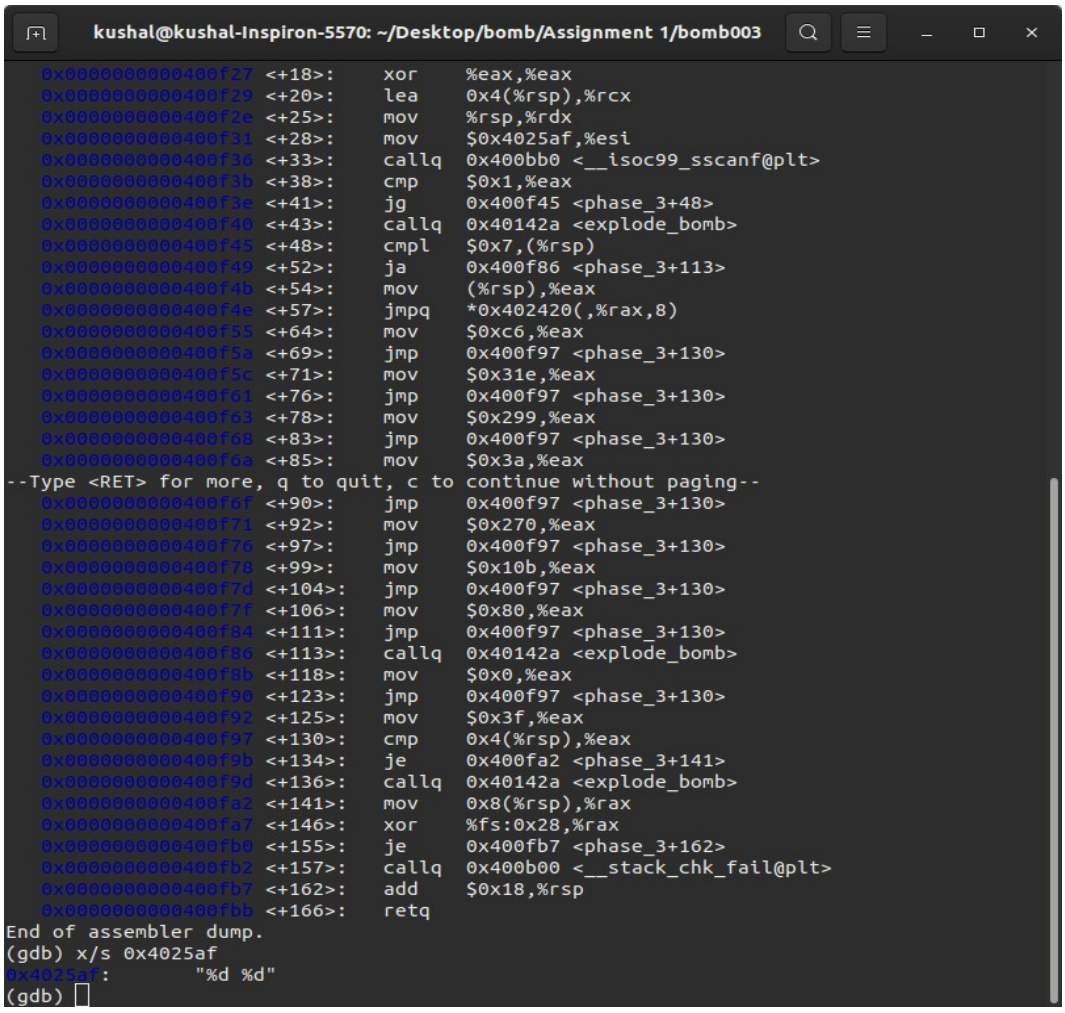
Binary Bomb(Group 3)
Phase 03
“Final Blow”

First phase was about the string, second was about giving the correct six numbers. Now the third phase. Phase 3 is all about giving two integer. If the two integers are correct than the phase_3 bomb will be diffused. Else it will explode.

First of all to know if the input is two numbers we have to open the “gdb bomb” and set break point at phase three “b phase_3” and run the answers.txt file and than input the phase_2 numbers and after that give some random inputs. After that we have to open the dissembler and the system will show the assembly code present in phase_3

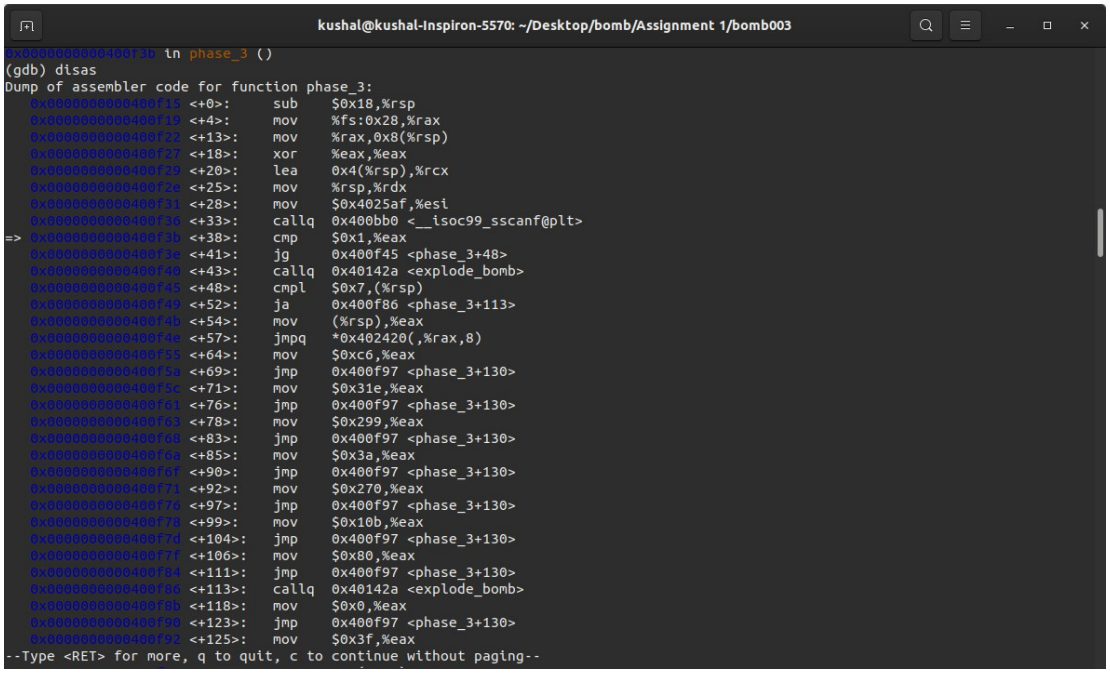


First we will look at line <+33> where there is callq function and it calls “scanf” so next lets look at the line above it at line <+28>. We can see that there is one hex address. So we can write **“x/s the hex number”** in this case “**x/s 0x4025af**” After giving this command we will get a clue saying that the input for phase_3 are two integers.



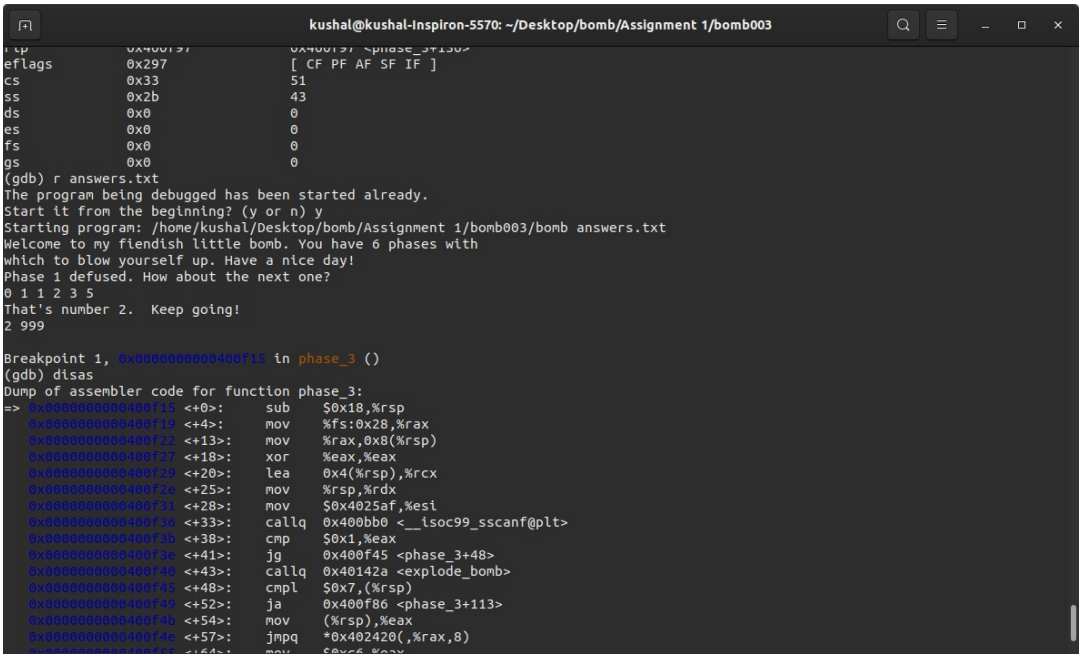
We got the clue that the inputs are two integers as there is two “**“%d” “%d”**”.

Now lets see the compare code below the line <+33>. We have to compare (1 and %eax). We can move directly to line <+38> by commanding “**until* address**” After that we don’t know the value of eax so we can find it with the help of information register.



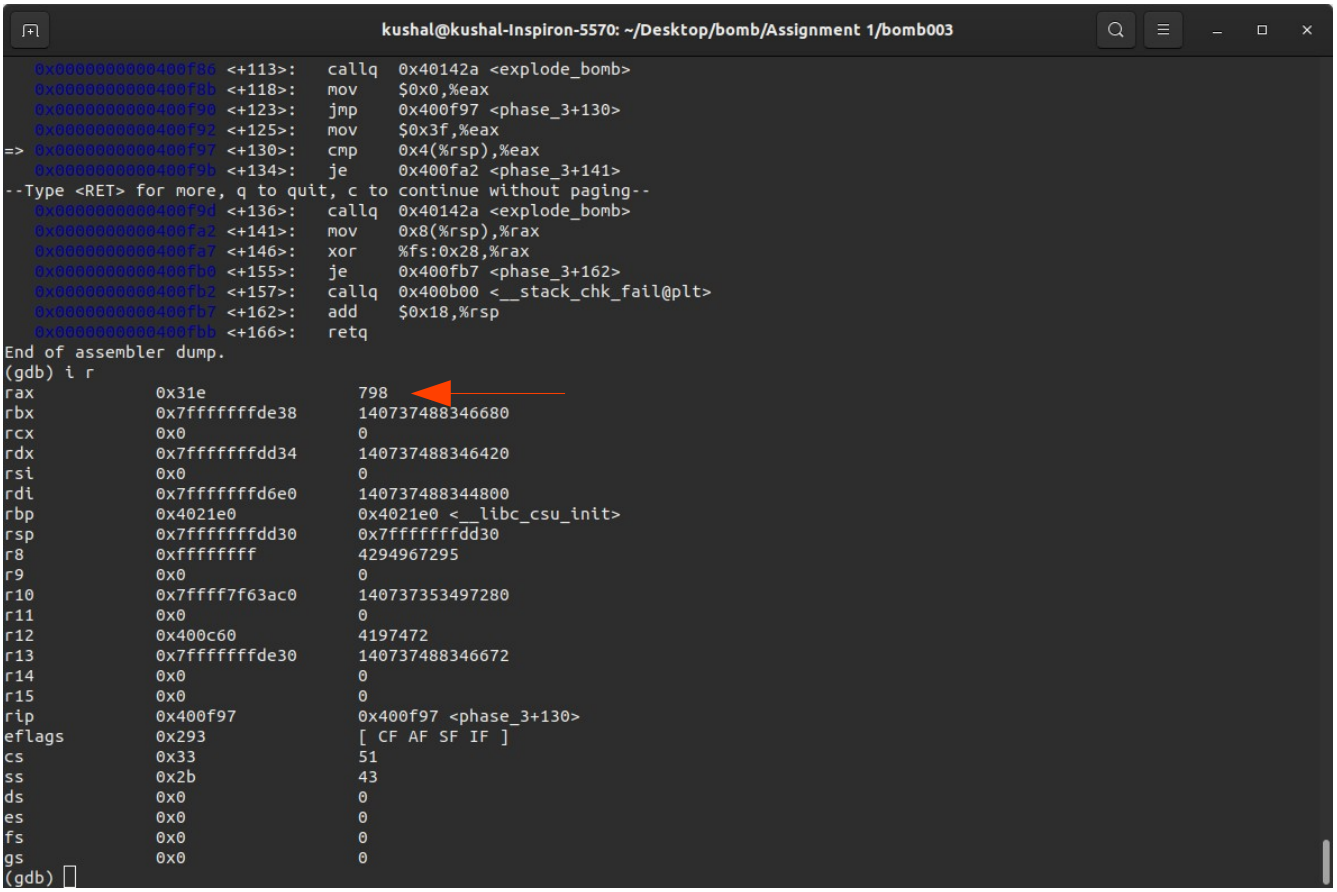
Lets trace into the assembly code so first up lets go to line <+38> which compares (1 and %eax) and the line below that states a function which says jg(it is unsigned and it jump if greater than). We can trace out that if the input is less than 1 the bomb will be exploded. So the first digit should be greater than or equal to 1. If it is greater the function will move to line <+41> and call the “jg” function. After that the jg function will move to line <+48> where it compares (7 and %rsp) . The operations done here will impact the next function, if the value of rsp is greater than 7. If the value of rsp is greater than 7 than the function will move towards <+113> and the bomb will be exploded.
So we got one big clue that says the first input should be greater than or equal to 1 and less than or equal to 7.

Lets run the program and give the first input as any number from range (1-7) since the number should be greater than or equal to 1 and less than or equal to 7.

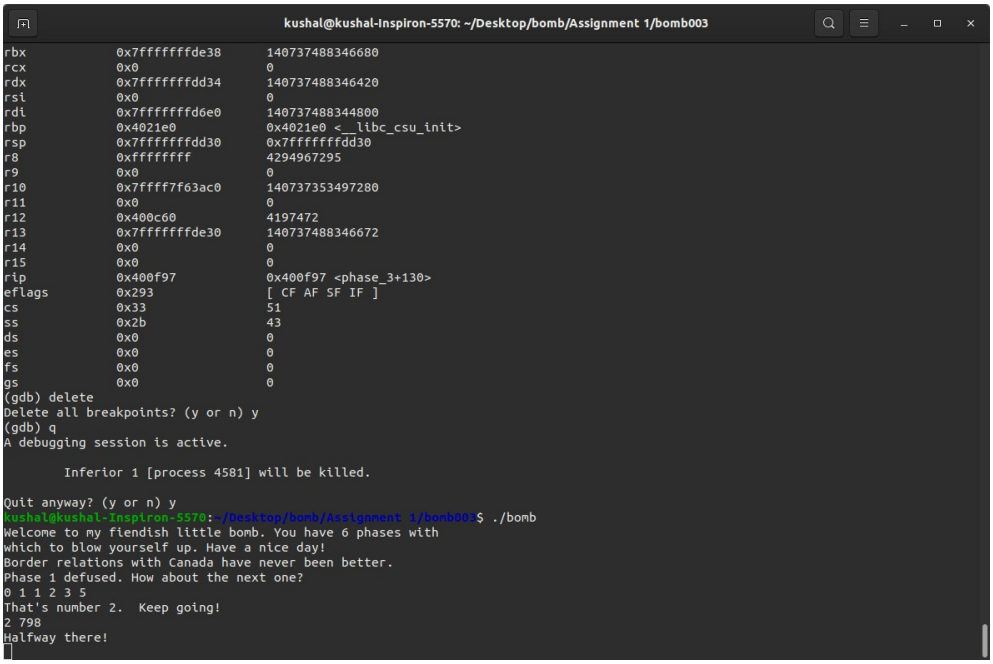


So in this case I gave the first input as “2”. So lets find the second integer input. For that we have to go to the first compare function at line <+38>. There it will compare the given user input integer with 1. If it is greater than or equal to 1 it will move to the next function which is jg(jump if greater than or equals to) at line<+41>. After that the function will move to line <+48>. There we have to compare our input with “7”. It will check if the number is less than or equal to 7. If the number is greater than 7 it will go to next line and the boob will be exploded. Since right now our input is less than 7 so it will move to line <+54>.

After that we have several mov and jump functions. We will now go to the next compare function which is present at line <+130>. And by opening the information register we get the second integer input, since the second input is be stored in the %eax register.

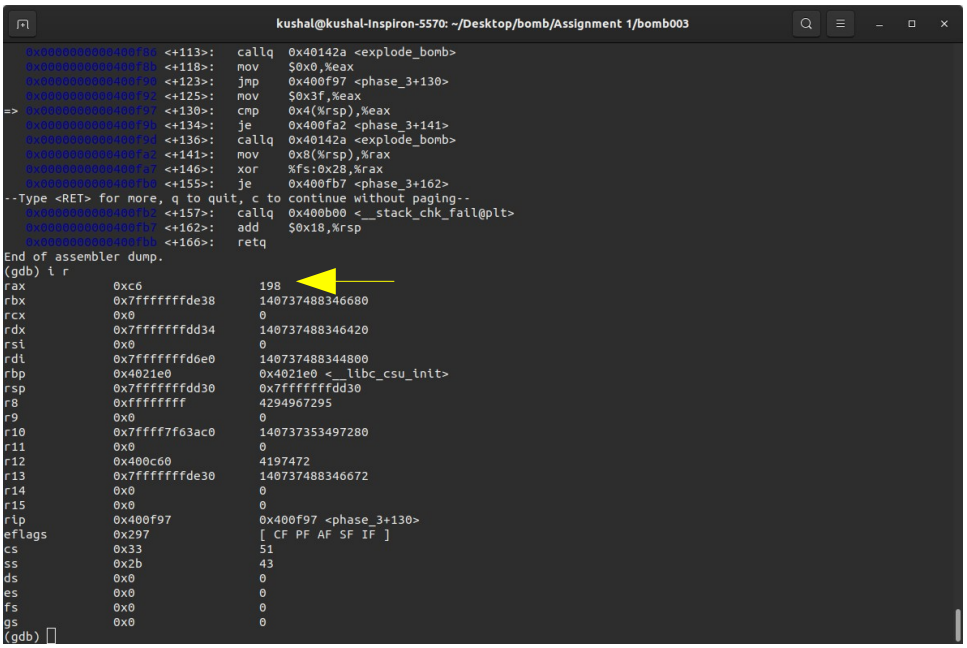


Here we can see that for the first input 2 we get the second input as 798. So lets try to put 2 and 798 to see if the bomb will be diffused or not.

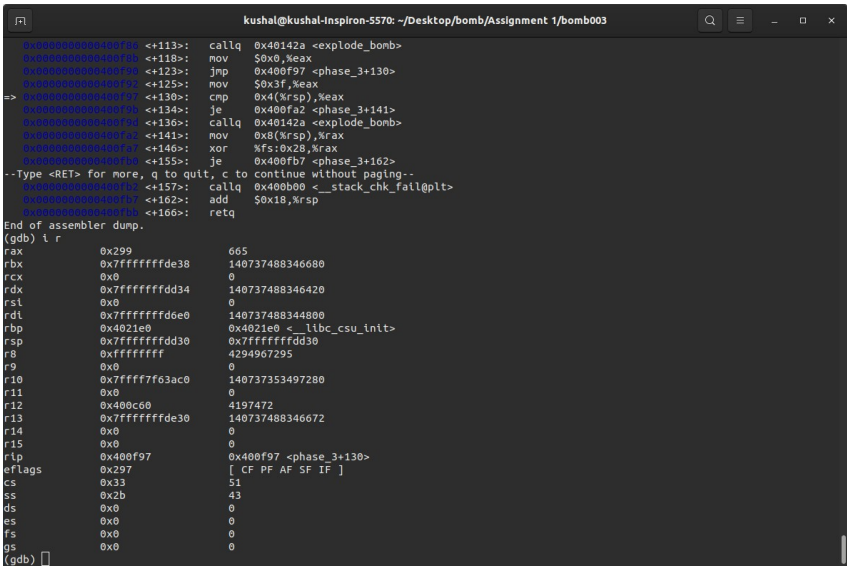


So my input was correct. But since this phase_3 accepts the first inputs in the range of (1-7) we can give any first input in the range (1-7) so for different first input, there will be different second input. Like for 2 it was 798.

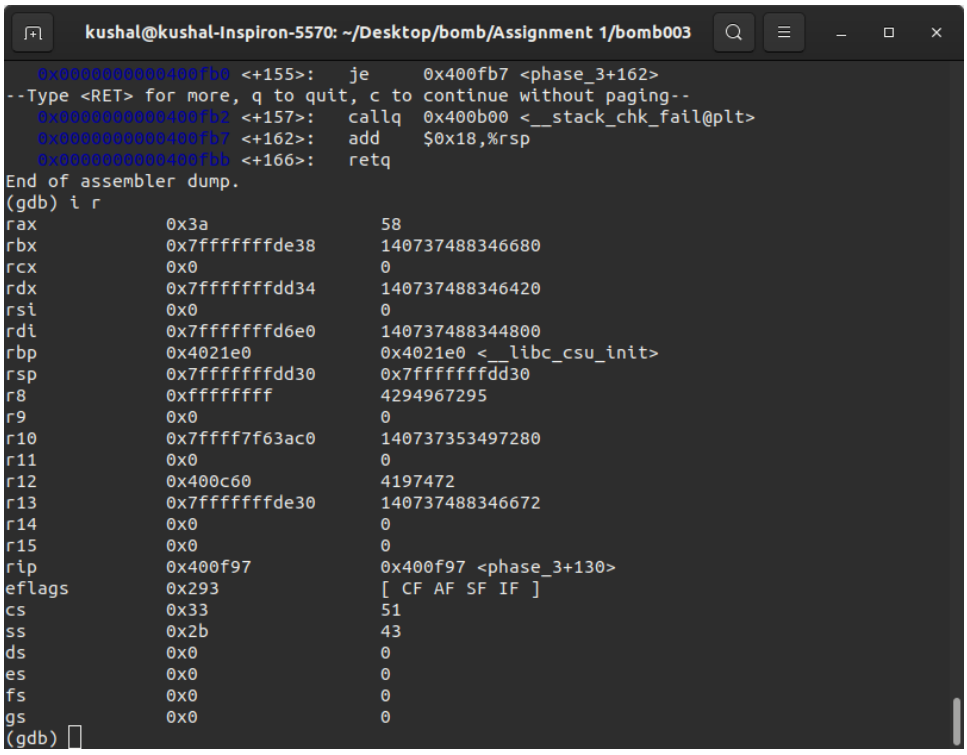
As it lets check for every first input in the range of (1-7).
For First input 1 The second input is 198



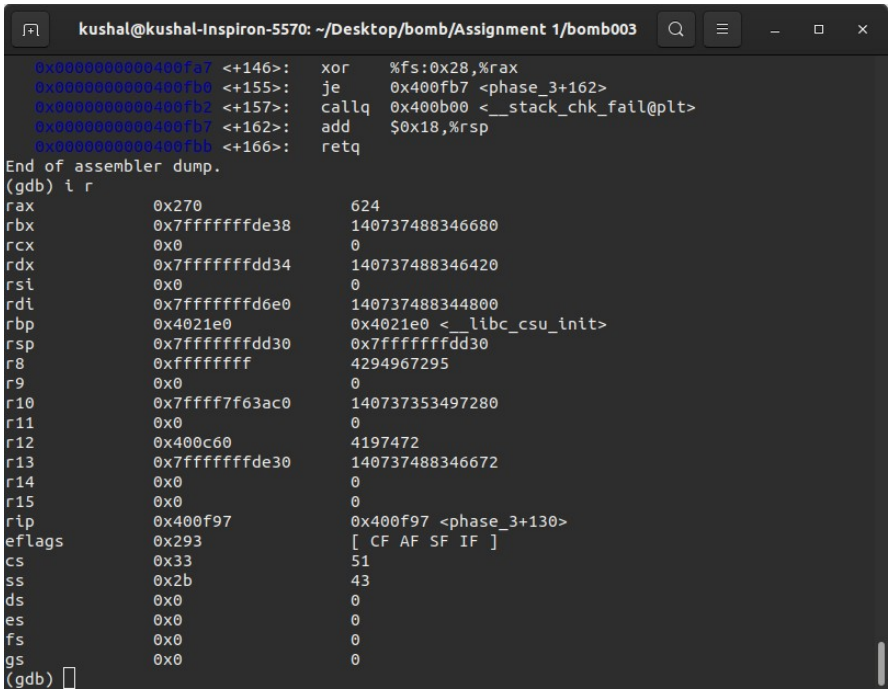
For First input 3 The second input is 655



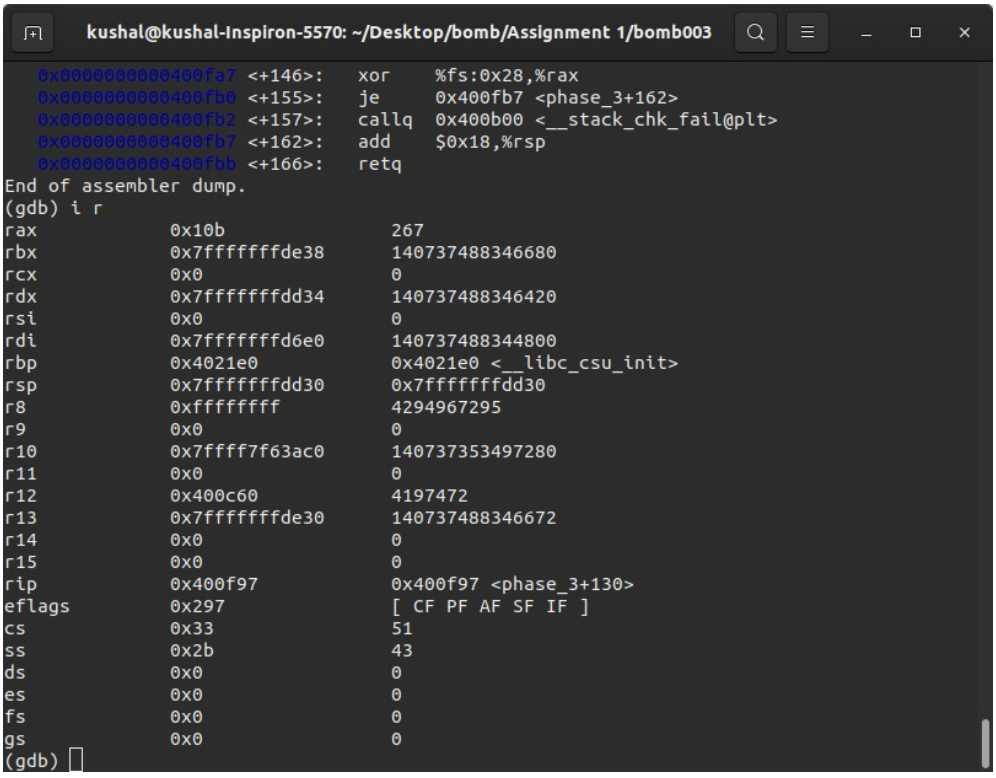
For First input 4 The second input is 58



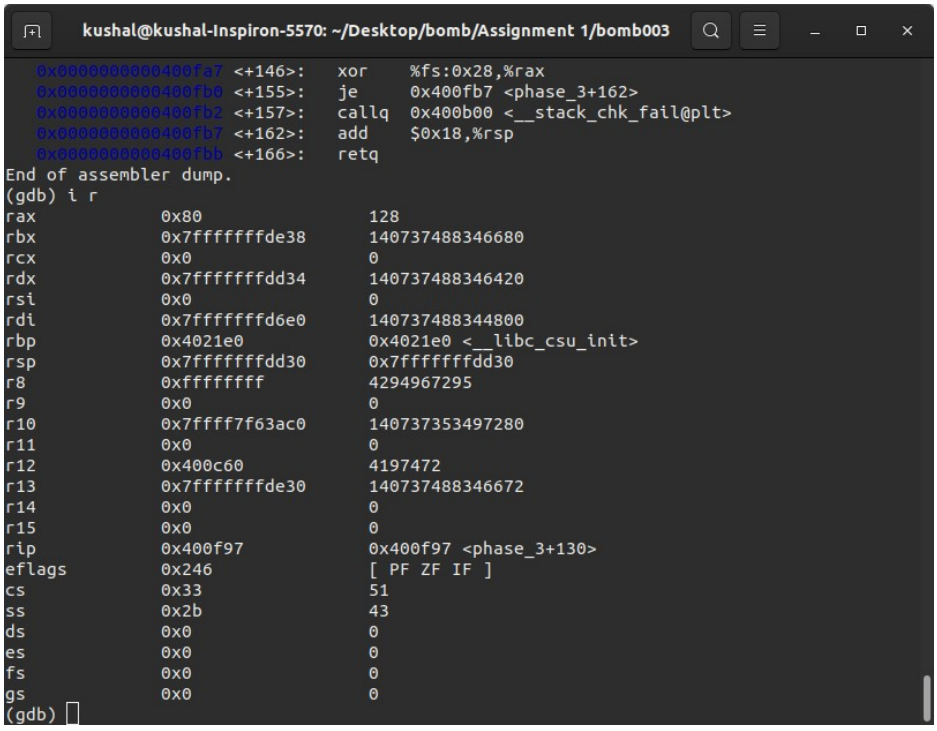
For First input 5 The second input is 624



For First input 6 The second input is 267



For First input 7 The second input is 128



Phase 3 completed…..
“Dr.Evil see I told you I will crack your bombs”
“Till then I will see you after midterm in assignment 2”

THANK YOU