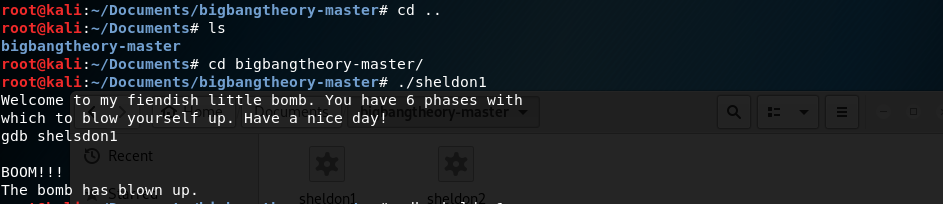
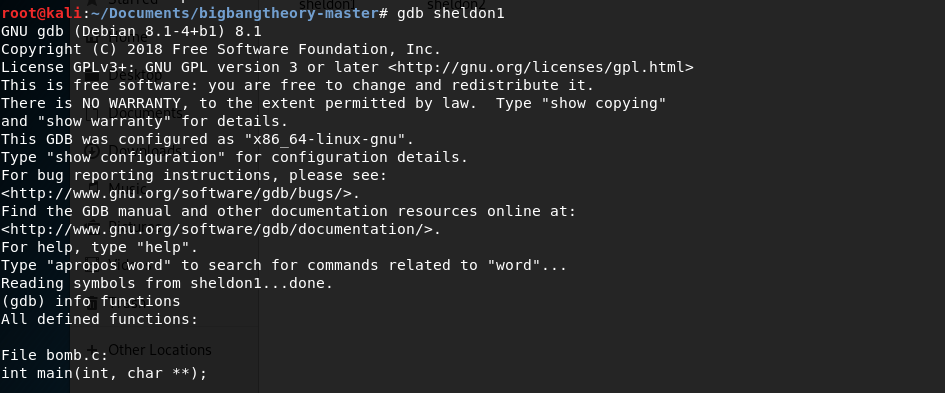
# Big Bang Theory – IT17069564

## Phase 01

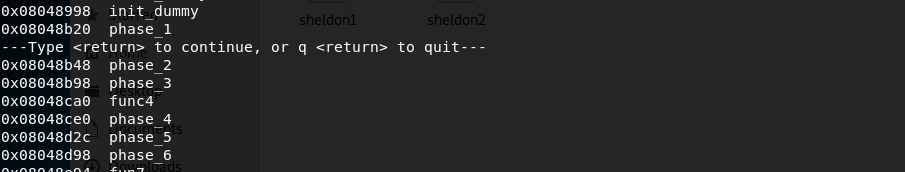
First, I executed the Sheldon1. Then understood that there are 6 Phases in here

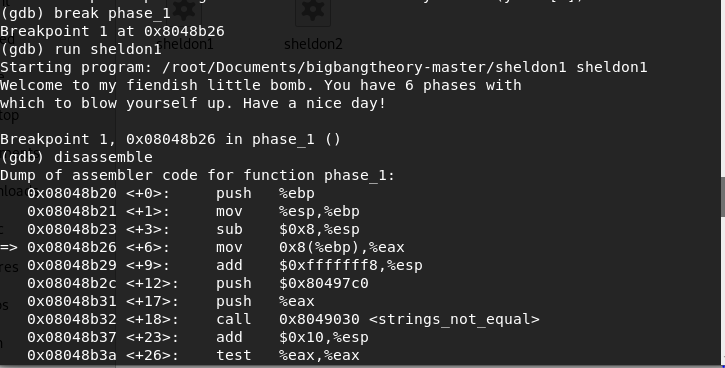


Then gave gdb shedon1 to get the assembly code. Then gave info functions command to get the available functions.

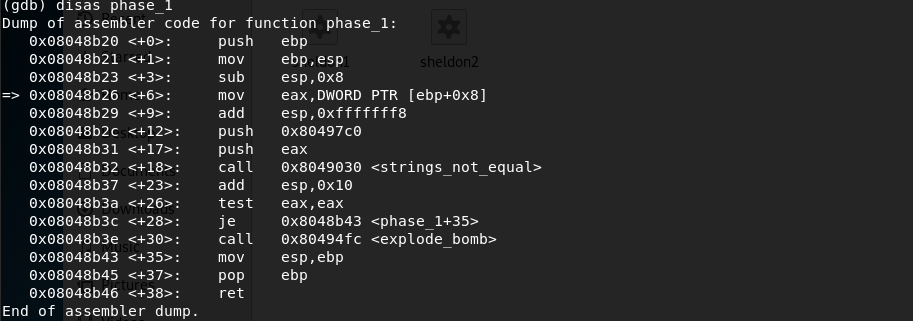


In there is a function name as “phase\_1”. Since when I first enter the password bomb has blown. I understand that there should be some condition that compare our input with it.

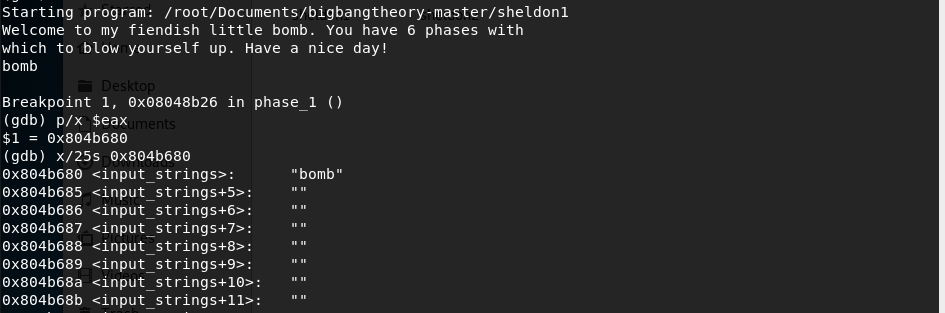


So, I added a breakpoint in the phase\_1. Then disassemble the phase\_1 to get the assemble code. 

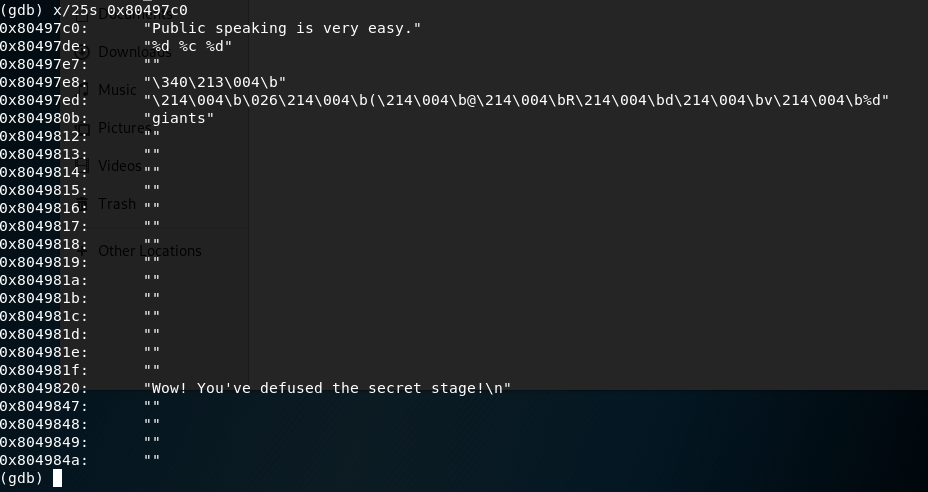
In here we can see that values in $eax location and 0x80497c0 location pushes to the stack and call <strings\_not\_equal> function. So I assume that our input and compare with value in 0x80497c0.



So, to test this theory I just type some string as “bomb” in the password field. Then got the memory address of $eax by using p/x $eax command. Then examine the string value of the address using x/25s 0x804b680 command. As in the snapshot indicate it clearly show the value of the address as “bomb”



Then I execute the same steps with the address 0x80497c0. In there it shows the string value “Public speaking is very easy.”



When I type that value as password, Phases 1 is defused.

