# OHTS – LAB 01

# It17111034 – U.C.S Bandara

Netgarage is a series of war games which can play by exploiting the vulnerabilities.

**Level 01**

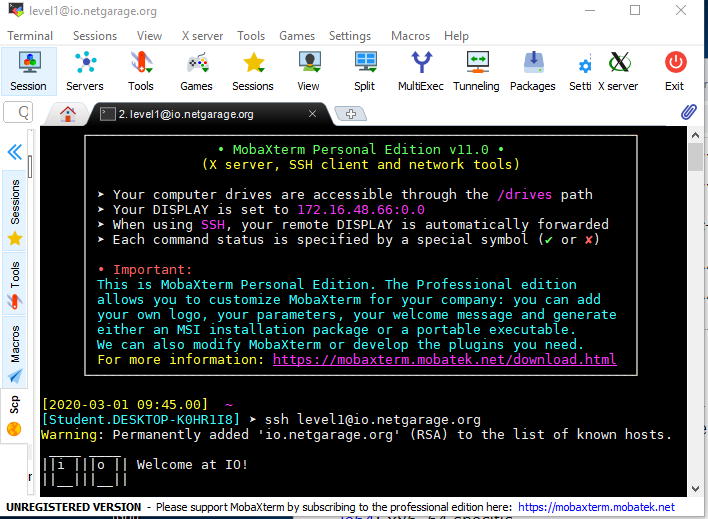
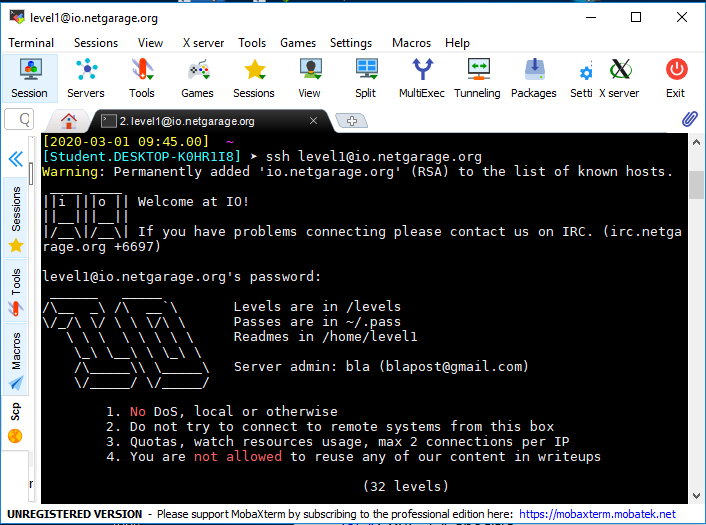
In the beginning we have to connect to the server using SSH. After connecting following instructions will appear.

Figure 2

Figure 1

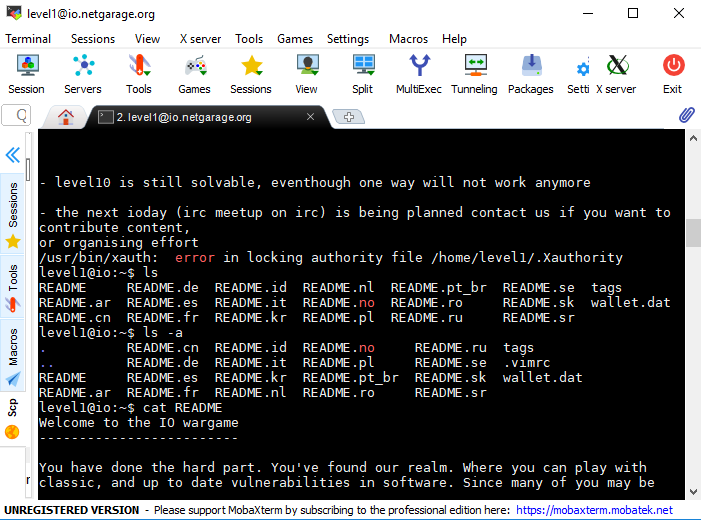
After that there are few readme files available and we can get the idea how to play.

Figure 3

All the files according to the levels are in the levels directory.

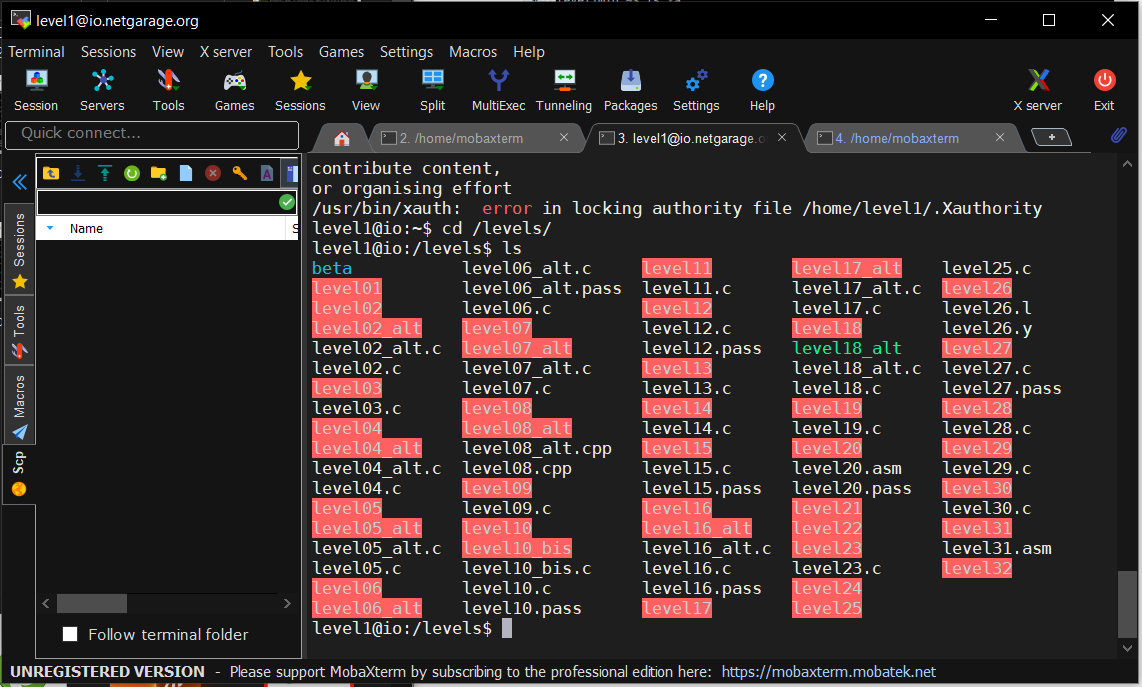
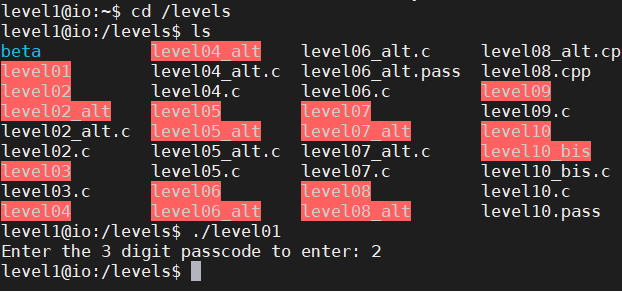


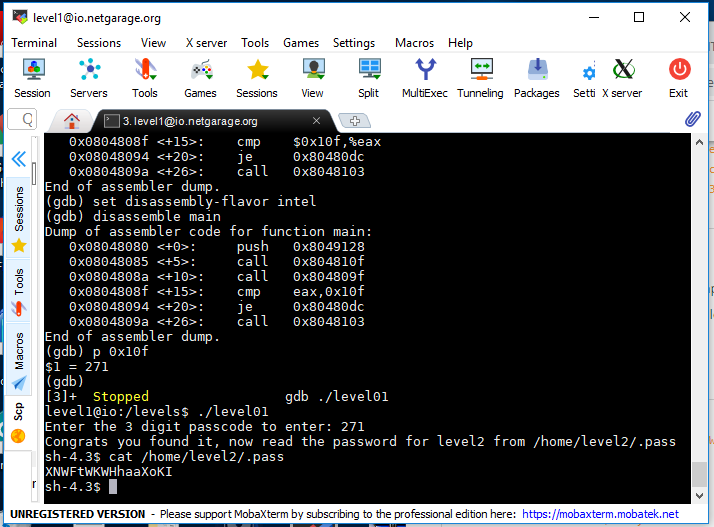
Figure 4

There is only one executable which is named as level one. We have execute it and find what happening



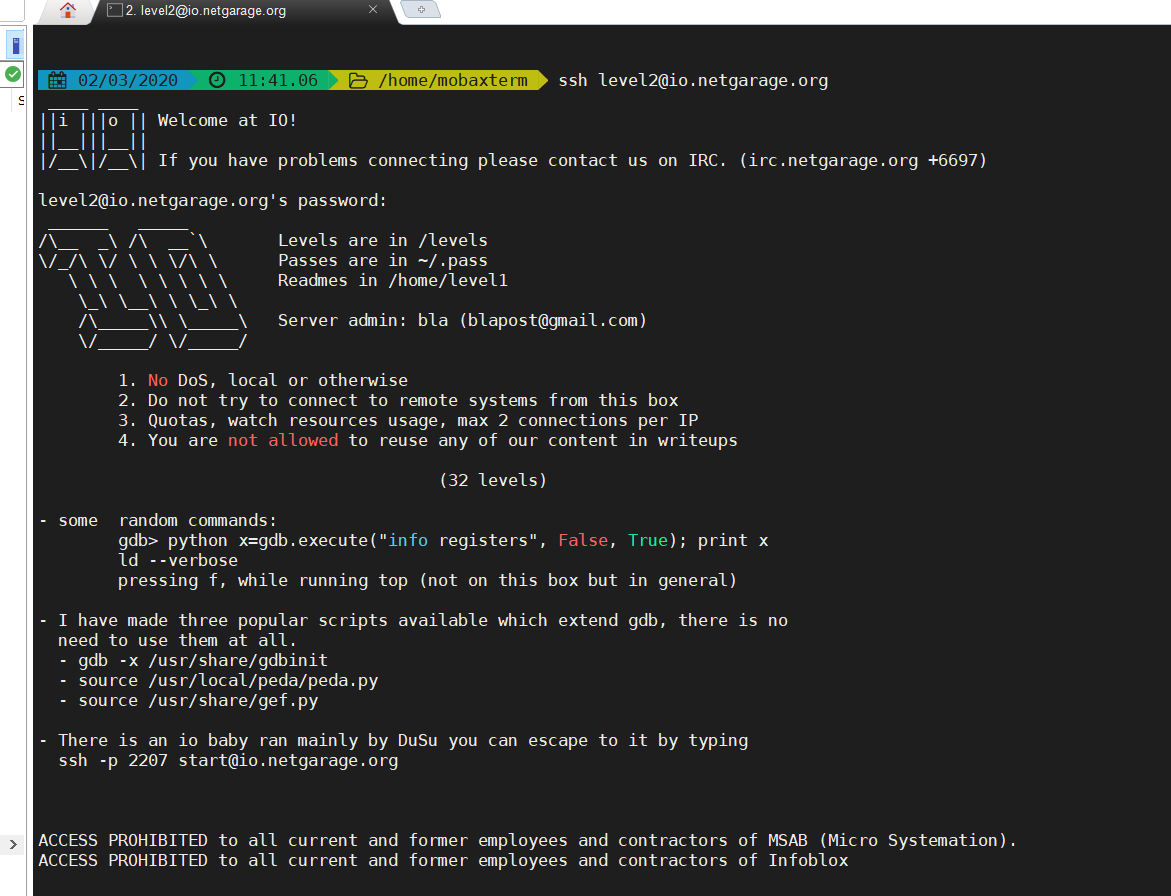
Then it asks for a 3-digit code. We have to find the code to go to the next level.

Then using GDB looking for the code dump and find any clues when looking to the dump we can notice there is a comparison. Then we have to find the value which is comparing.

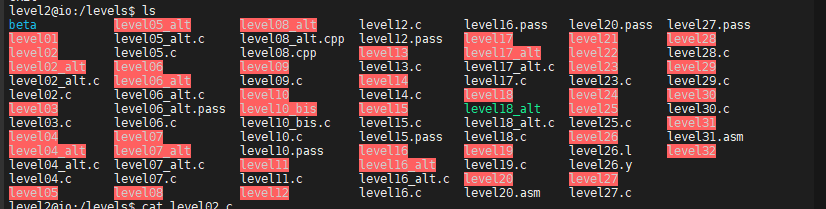


After that we can decode the value as 271. Then we have to again execute the command and enter that number. Then we can see that the user mode is changing and tell us to access the level 2 password location. After go in to that location we can find the key to level2.

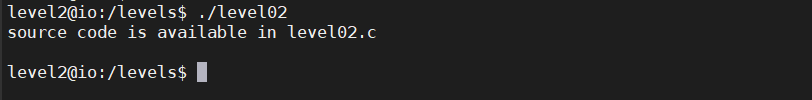
**Level 2**



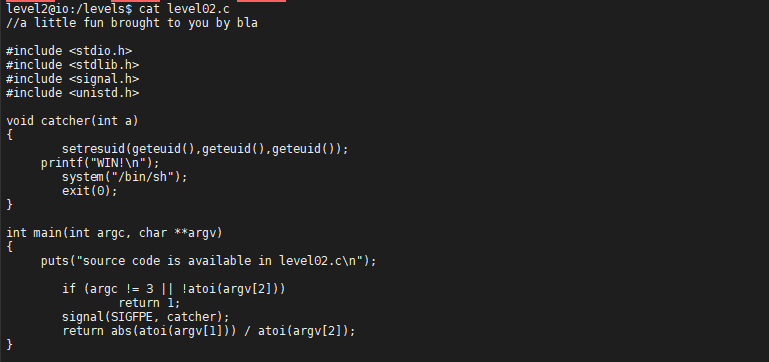
Using the password found in level 1 we can log in to the level 2. In here also we have to access the levels directory.



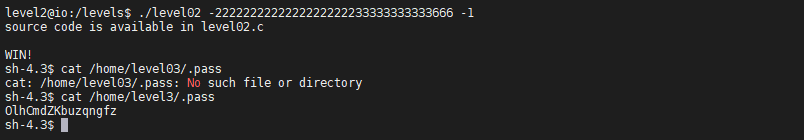
Then we have to execute the level02 program. Then we can see it says look in to the source code.



Then we have look in to the code.

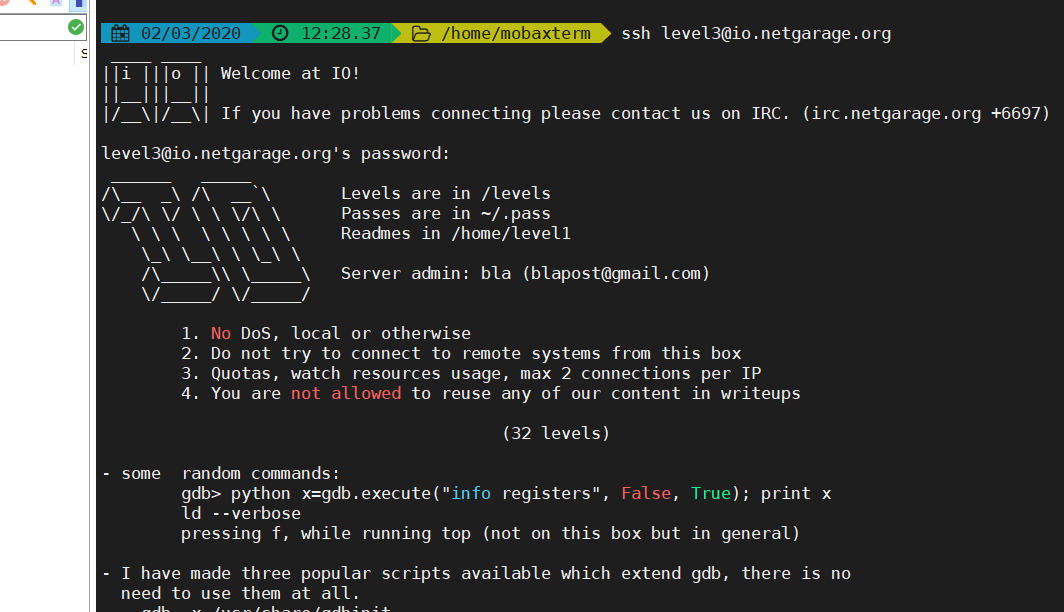


There is an exception in here called SIGFPE. To trigger this exception, we have to enter large negative value and to make pass the atoi function we have to pass -1.

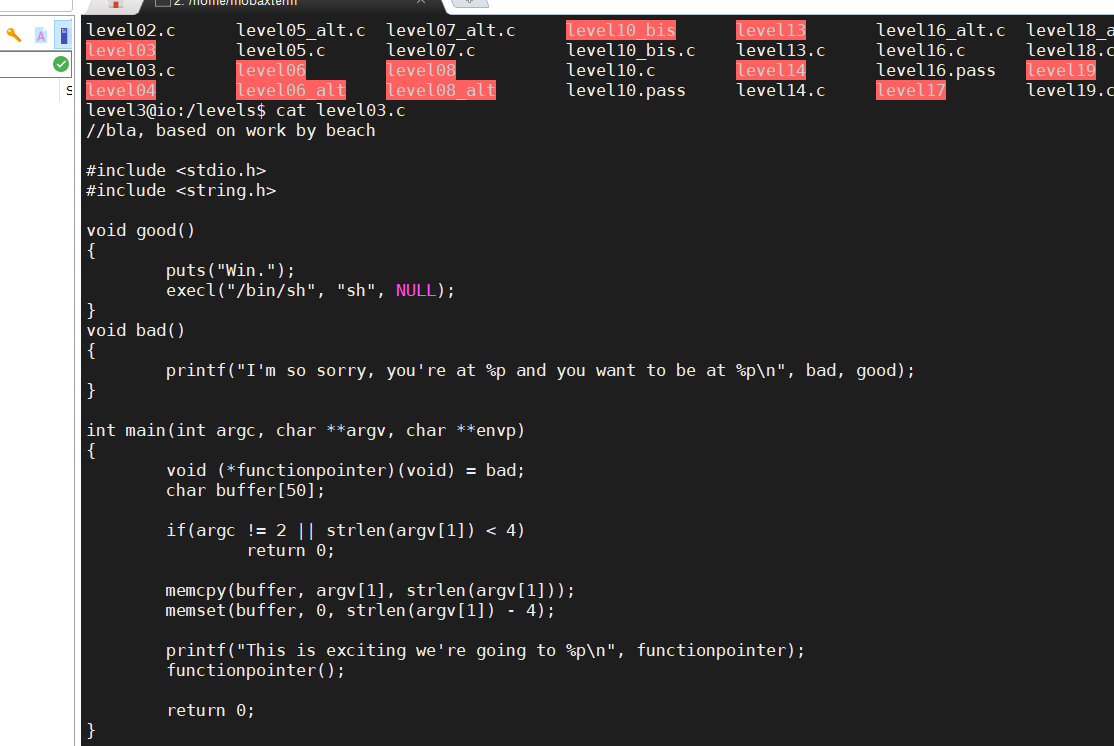


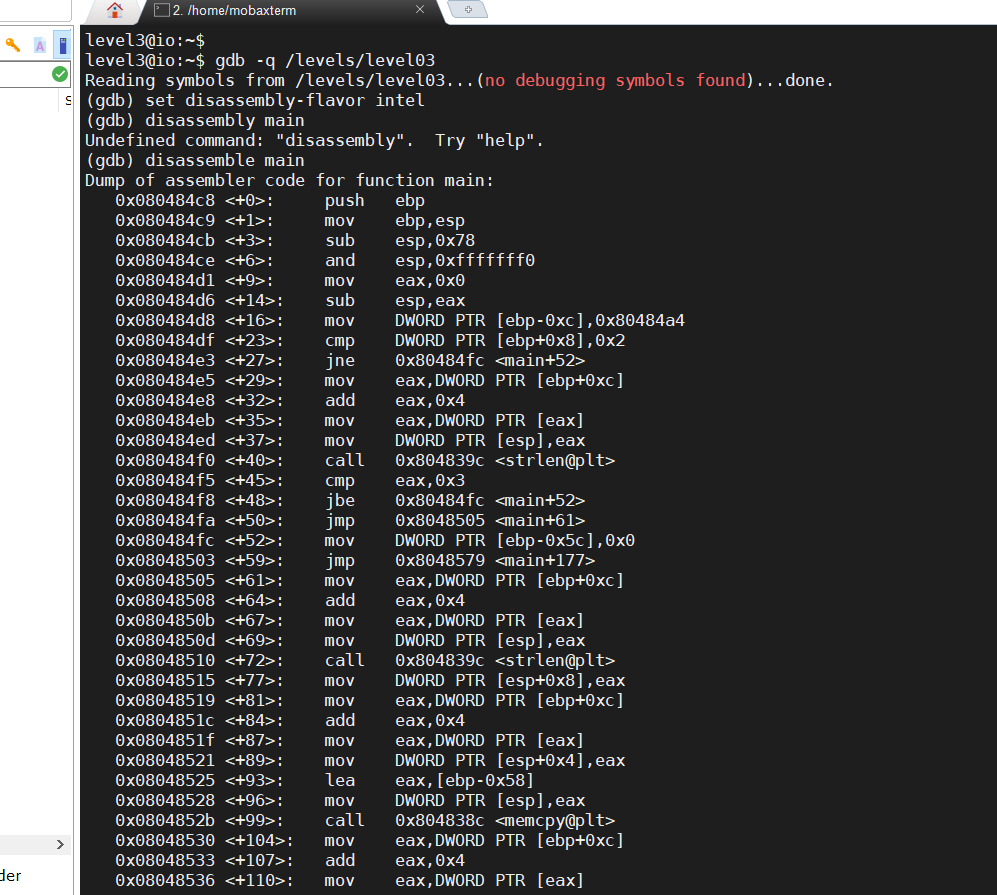
When we execute the level02 by passing -2222222222222222222233333333333666 and -1 then the user mode changes and can be access the password of level 3.

**Level 3**

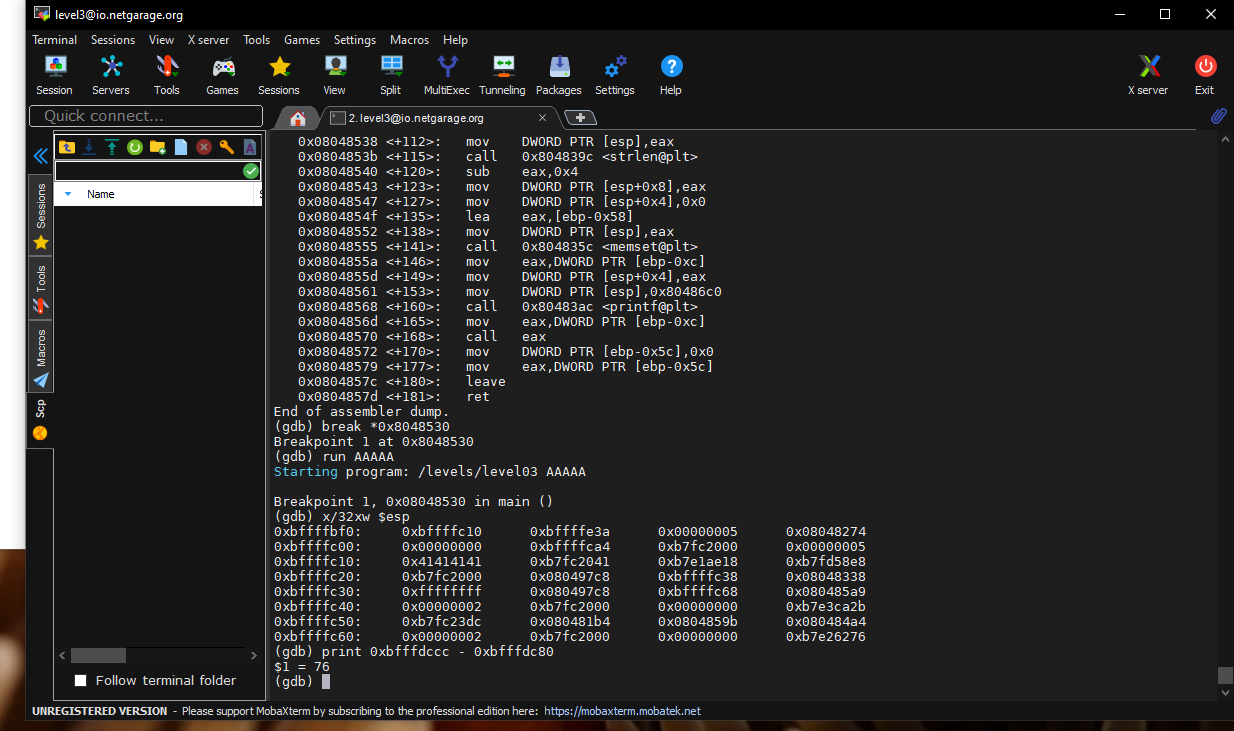


In level 3 also we have to analyze the code of the level03 program.



In the code there are two functions called good() and bad(). We want to run the good() function. But in the main function it is initialized into bad(). Also in the main there is a buffer size is given. Therefore we can get the idea that we have to do a buffer over flow attack. 

Now we have to make a brake point and over flow some data. Lets select 0x8048530 as our brake point and lets input AAAA as input data.



And we have to find exact number which we need to overflow. And by using python code we can print A s as we wanted and at the end we have to add the address we need to add

