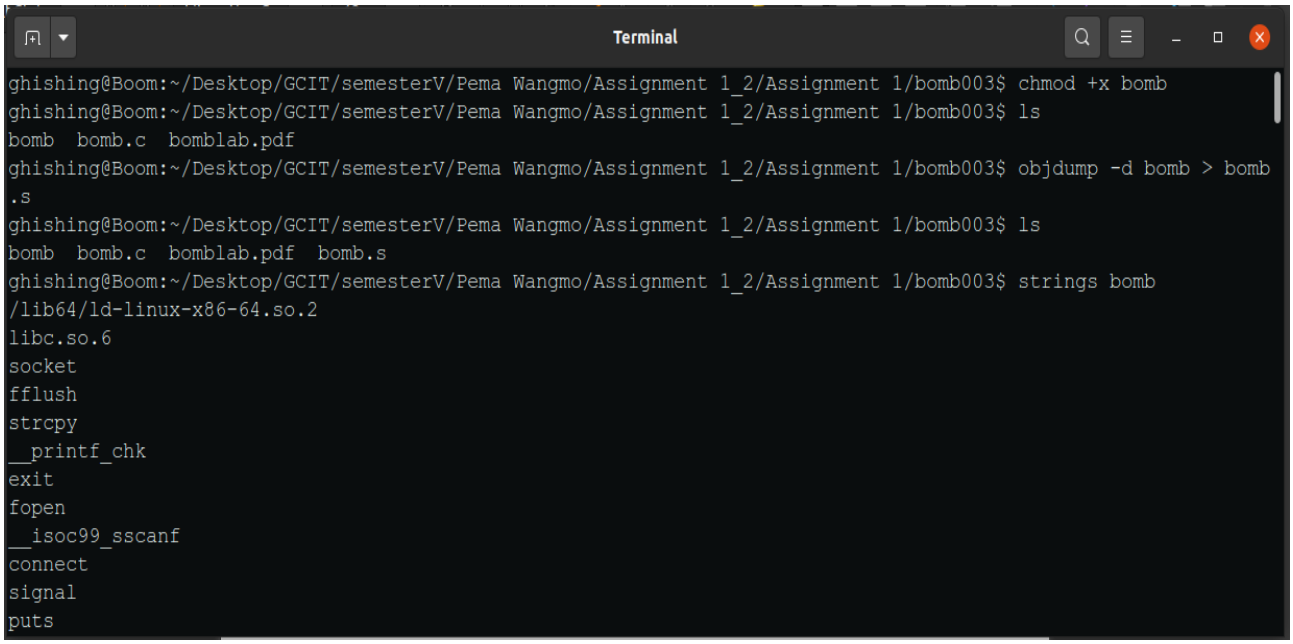
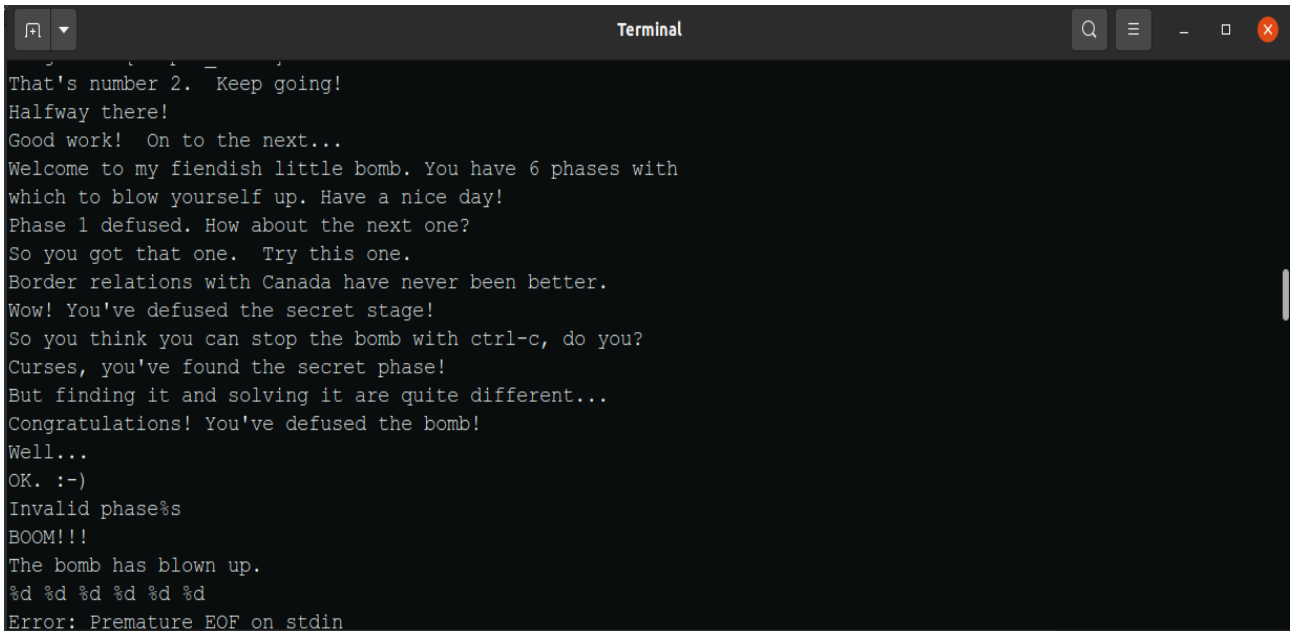
Task: Assignment consists of three different binary bombs and each bomb consists of three phase. We are asked to defuse binary bomb stepping each phase, phase_1,phase_2, and phase_3 accordingly. To execute this assembly files, linux shell was used through out the assignment.

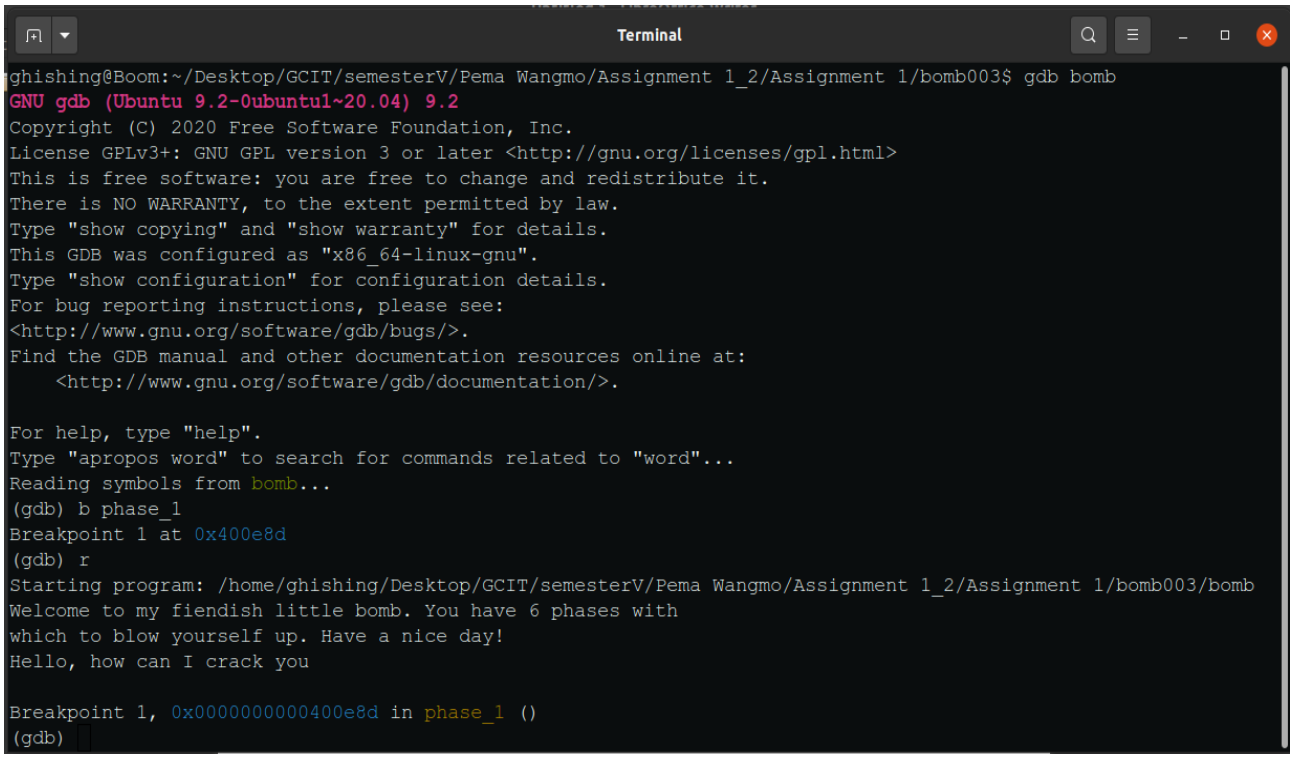
Phase 01

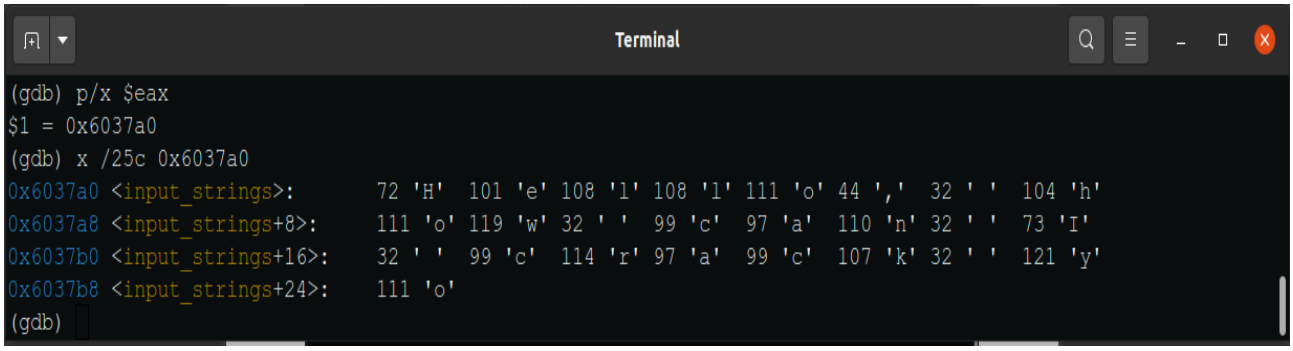
After saving the files to linux system, first of all, to access the folder, “chmod +x bomb” command was executed and permission to access file was granted by the system. To view the executable assembly form for the bomb file, “objdump -d bomb > bomb.s” was executed and “strings bomb” command was executed to display all the strings stored in the bomb file.



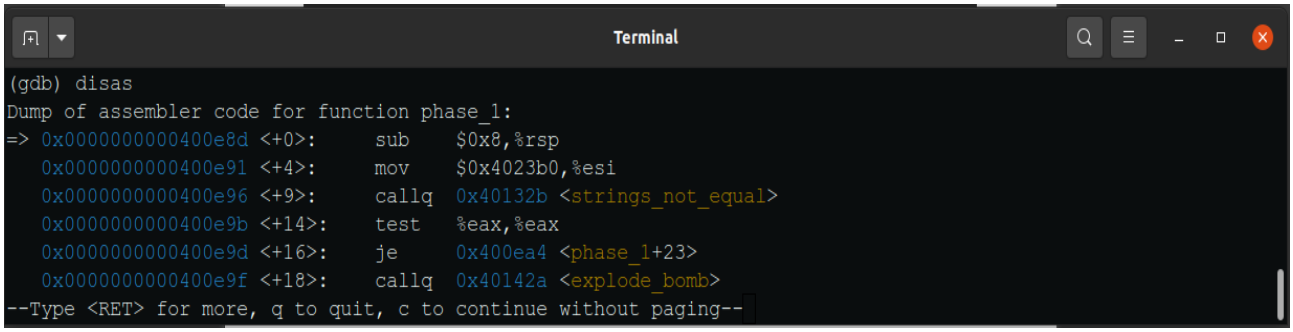


On continuation, debugger gdb was used to execute the assembly programs and break point was set to ensure that the bomb will not blow up. To run the program, “run” or “r” command is used and program asks user to give input. For a trail, “Hello, how can I crack you” was given as a test string and this test string is stored in $eax register. To check our string in $eax, “p/x $eax” was executed and it displays address of $eax register. Now it becomes easy to check the string from the given address. “ x /25c 0x6037a0” was executed to display the string.



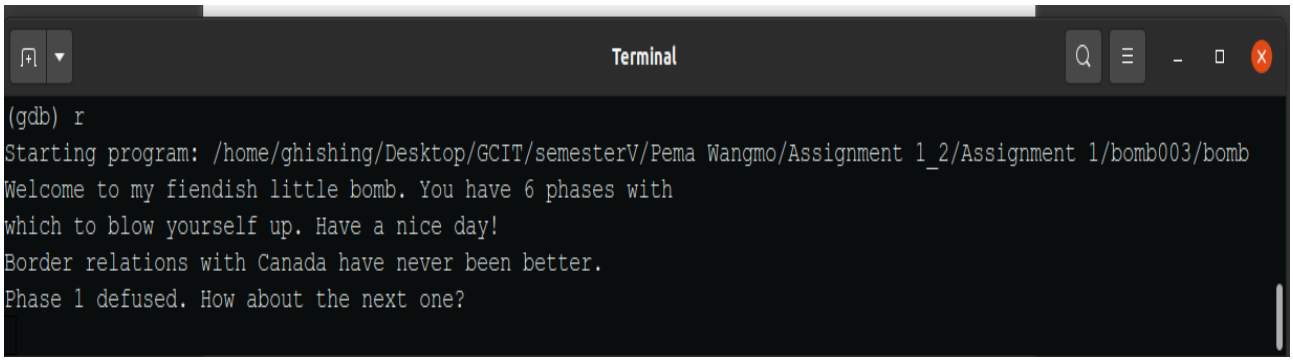


Understanding the programs



We have used “disas” to figure out the function in the program for the phase one. As soon as command was executed it displays the program code in assembly language. From this code we can understand function is being called <strings_not_equal> , some string value is stored in $0x4023b0 address(which the address of %eax). From this we can understand that answer for the given program is in string. To view the value stored in $0x4023b0 we use “x/25c 0x4023b0” to display the value till 25 characters. It displays the strings which is initially stored in the program in $eax register and the string was “Border relations with Canada have never been better.”

From the code we can understand that input value given by user in stored in %eax register and it compares to the initial value stored in address $0x4023b0. If it matches, program will take user to another phase but if it fails then, it displays the message “Bomb blown up”. To figure out the program logic, program was run and string value “Border relations with Canada have never been better.” was provided.



The user input and the string stored in the program register (%eax) matched and the bomb defused successfully.