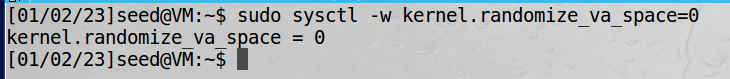
21CY682-SECURE CODING LAB

Name:Ramya Ajay

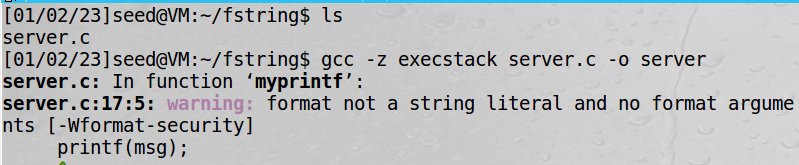
Roll No:CB.EN.P2CYS22004

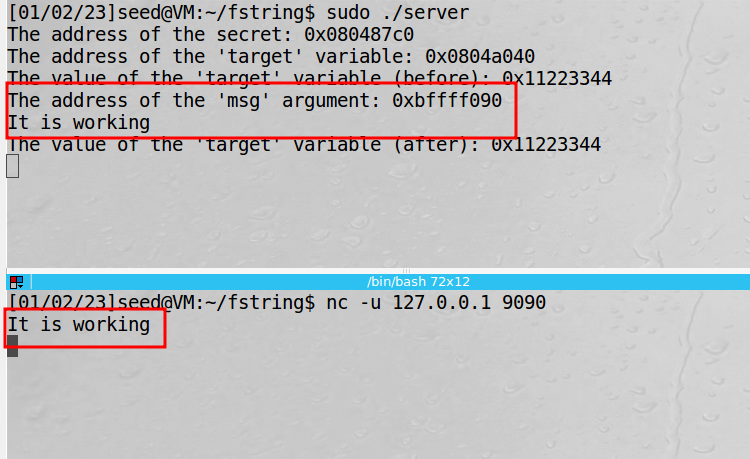
Lab 15:Format String

To Simplify the tasks, we enable address randomization as follows



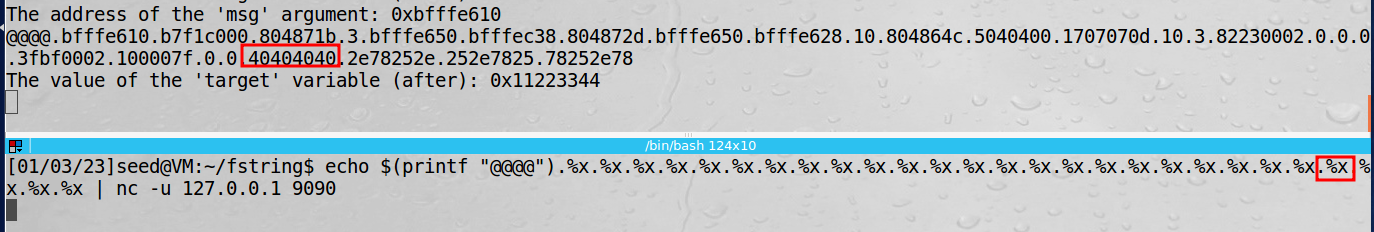
Task 1: The Vulnerable Program





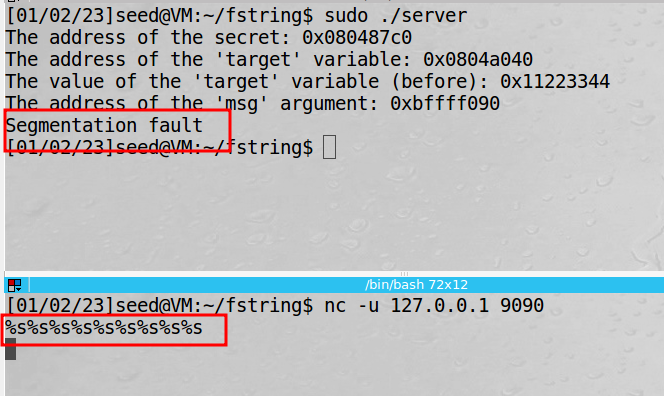
While compiling we receive a warning, which we ignore for time being. We send a basic string “It is working.” to test the program, and we see that whatever we send from the client is printed exactly in the same way on the server, with some additional information

Task 2: Understanding the Layout of the Stack



Task 3: Crash the Program:

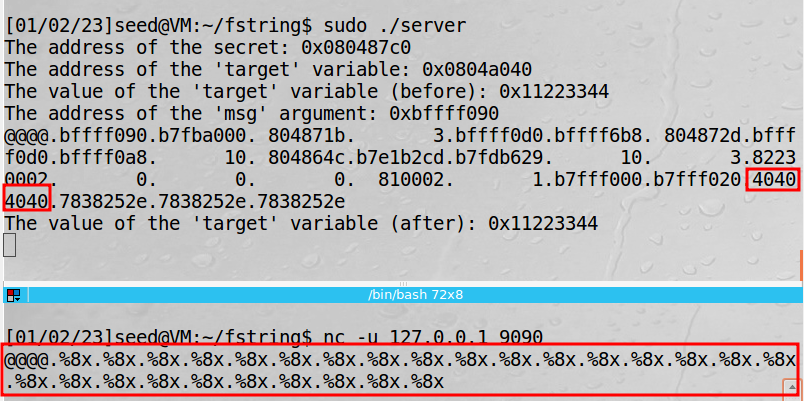
To crash the program, we provide a string of %s as input to the program, and we see the following:



Here, the program crashes because %s treats the obtained value from a location as an address and prints out the data stored at that address. Since, we know that the memory stored was not for the printf function and hence it might not contain addresses in all of the referenced locations, the program crashes. The value might contain references to protected memory or might not contain memory at all, leading to a crash

Task 4: Print Out the Server Program’s Memory

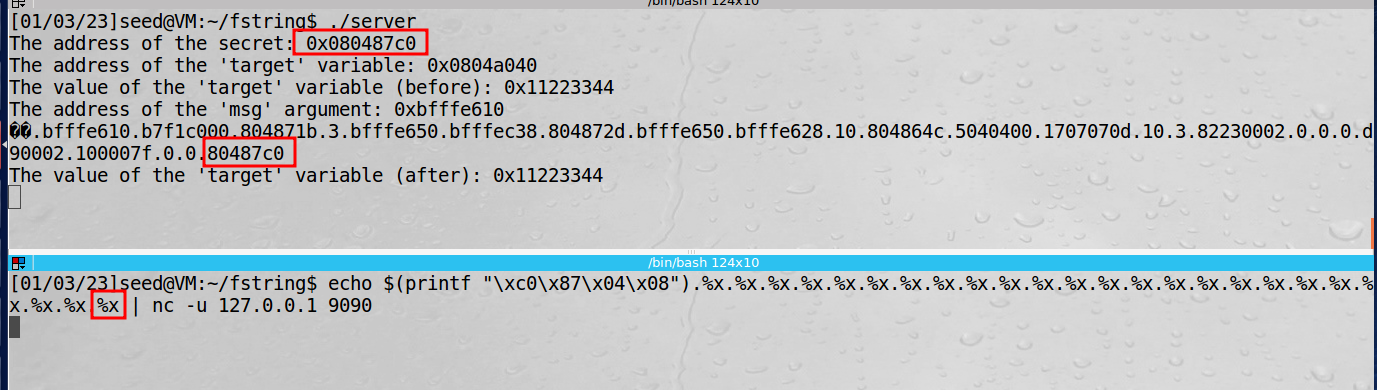
STACK DATA



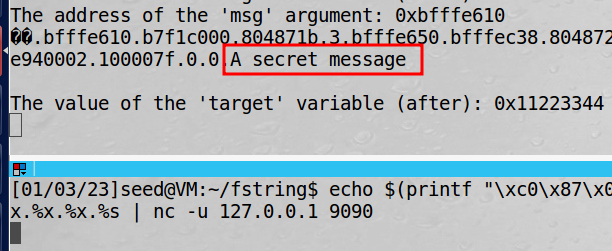
Here, we enter our data -@@@@ and a series of %.8x data. Then we look for our value - @@@@, whose ASCII value is 40404040 as stored in the memory. We see that at the 24th %x, we see our input and hence we were successful in reading our data that is stored on the stack. The rest of the %x is also displaying the content of the stack. We require 24 format specifiers to print out the first 4 bytes of our input

Heap data



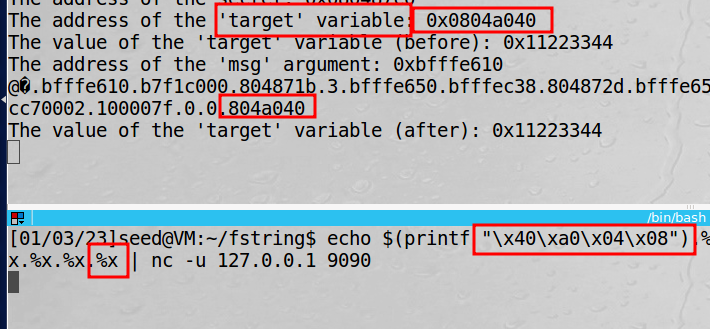


Now we got the same value. To print the value at that location we use %s

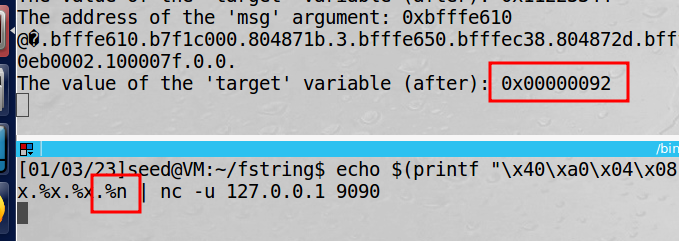


Task 5: Change the Server Program’s Memory

Task 5.A: Change the value to a different value



We got the same value as above



Now target variable value has been changed .

Task 5.B: Change the value to 0x500

Instead of a random value now we try to change it to a specific value.