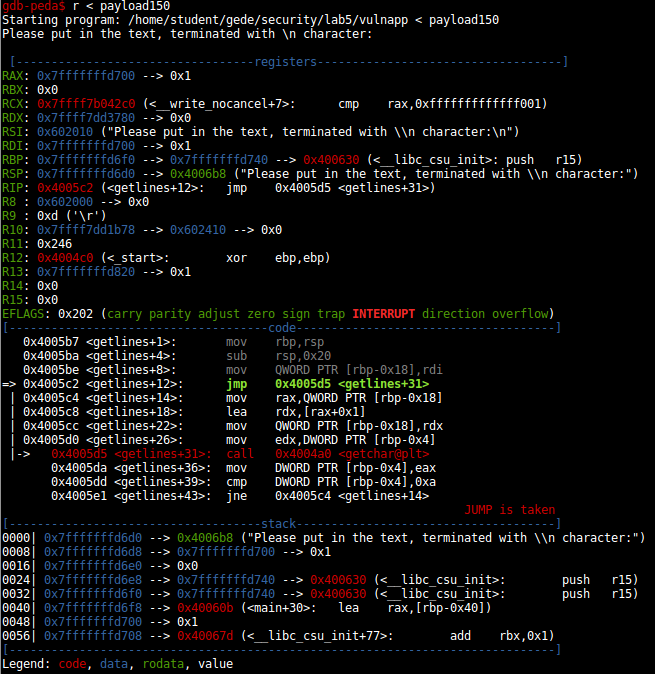
Gede Ria Ghosalya

1001841

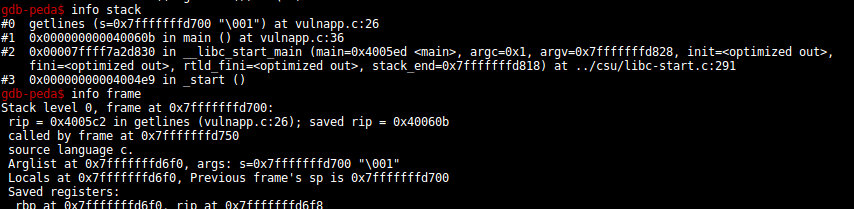
50.020 Security & Communications - Lab 5

1. **Buffer Overflow - Shellcode**

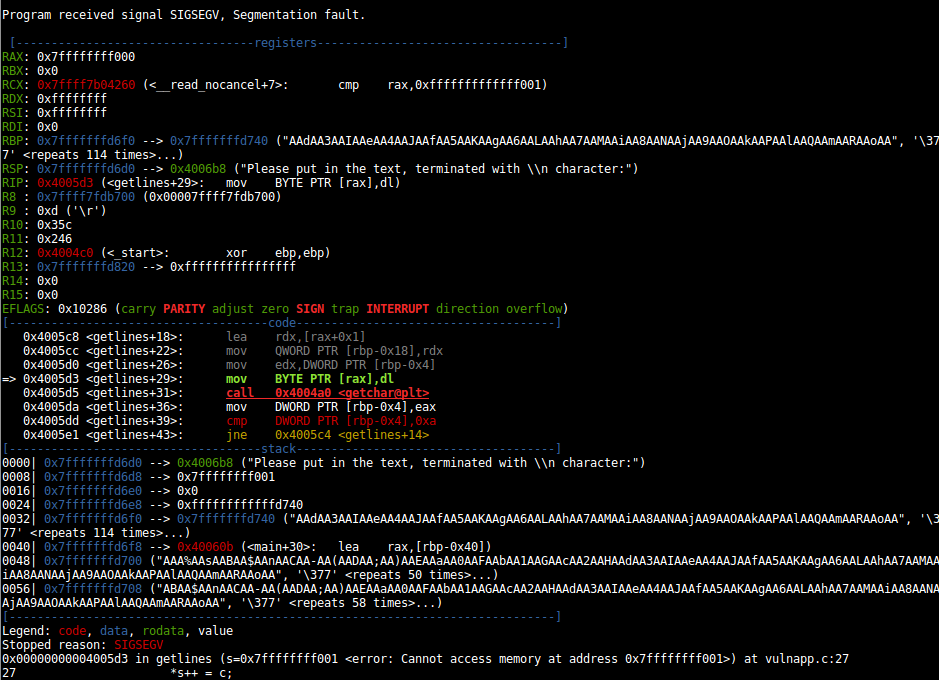
Trying with payload pattern of length 150, with breakpoint in line 25.



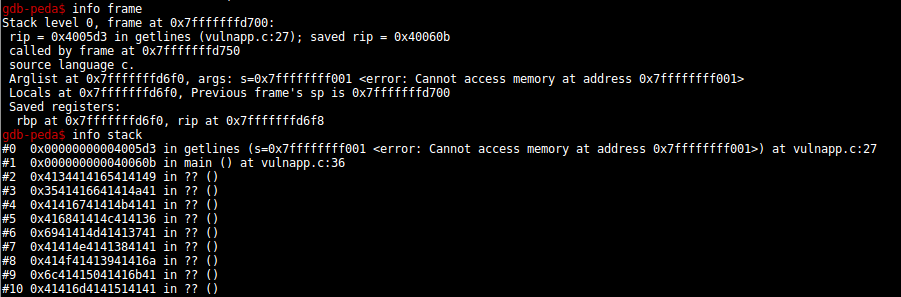
At line 25, the current `info stack` and `info frame` is as follows:



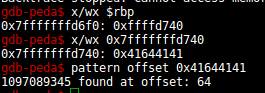
Once the program advances from the breakpoint, it encounters SIGSEGV error.



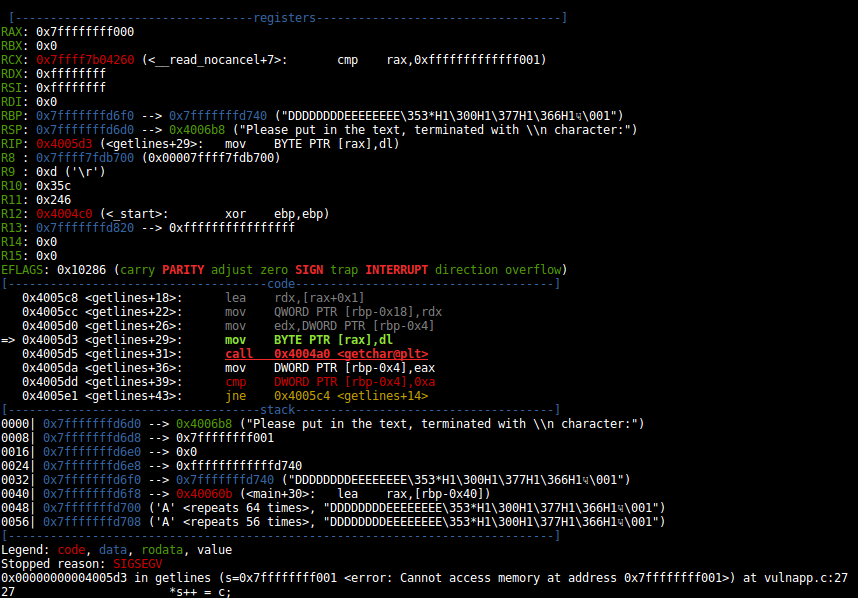
Its info frame & info stack are as follows:



From this, we can see that 150 characters does reach to RBP. Finding the offset required to override RBP properly:



Now that we have the length fill (of 64), using `payload.py` to produce the desired payload, here is the result.



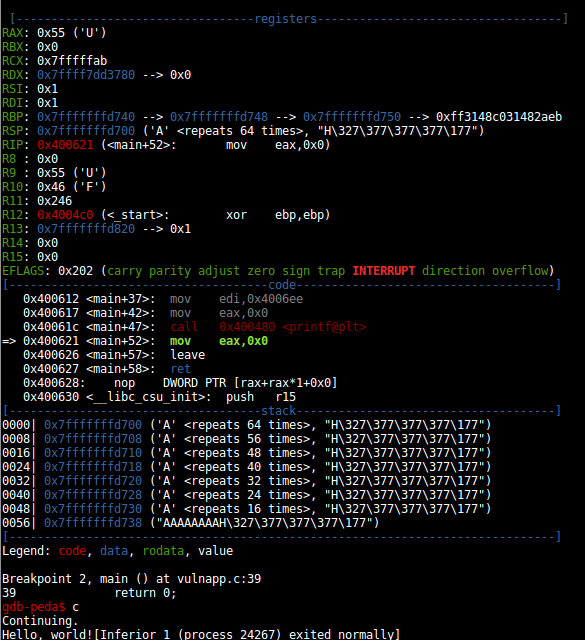
Now the base pointer points to a location with “DDDDDDDD”, and the next row (RIP) is “EEEEEEEE”.

1. **Adding Bogus RIP**

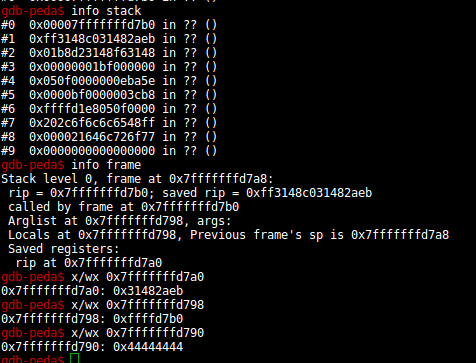
Now that we know the length fill is 64 and are able to poison the RBP & RIP, we can change the “EEEEEEEE” into our shellcode address. Running the code under GDB once, we know that the stored RBP is in 0x7fffffffd740. Thus, the overwritten RIP should be in the next address (+0x8) which is 0x7fffffffd748, and the shellcode (+0x10) is in 0x7fffffffd50. Changing the following:

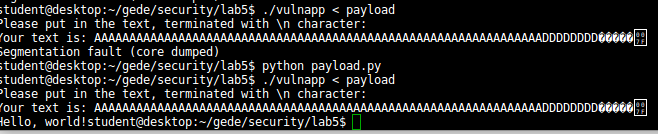
RIP = EEEEEEEE -> 0x7fffffffd750

We will be able to point the program to our shellcode, at least in GDB. Below is the result.



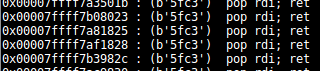
We were able to run the “Hello World!” shellcode after the normal program in GDB. However, this does not work in normal shell. Inspecting core, we found that the RBP is in 0x7fffffffd790, thus our RIP should be 0x7fffffffd7a0.



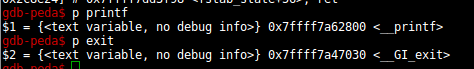


1. **Return to LibC**

Some of the searched LibC addresses for “pop rdi”:



For printf & exit:



The payload has repeating ‘A’s for 51 times, and then the ‘Hello World!\0’ so that it is 64 bytes before the RBP. Then we put the fake RBP (DDDDDDDDD). Afterwards, we put the gadget address, the string address (which is RBP-0xD), the printf address, and finally exit address.

