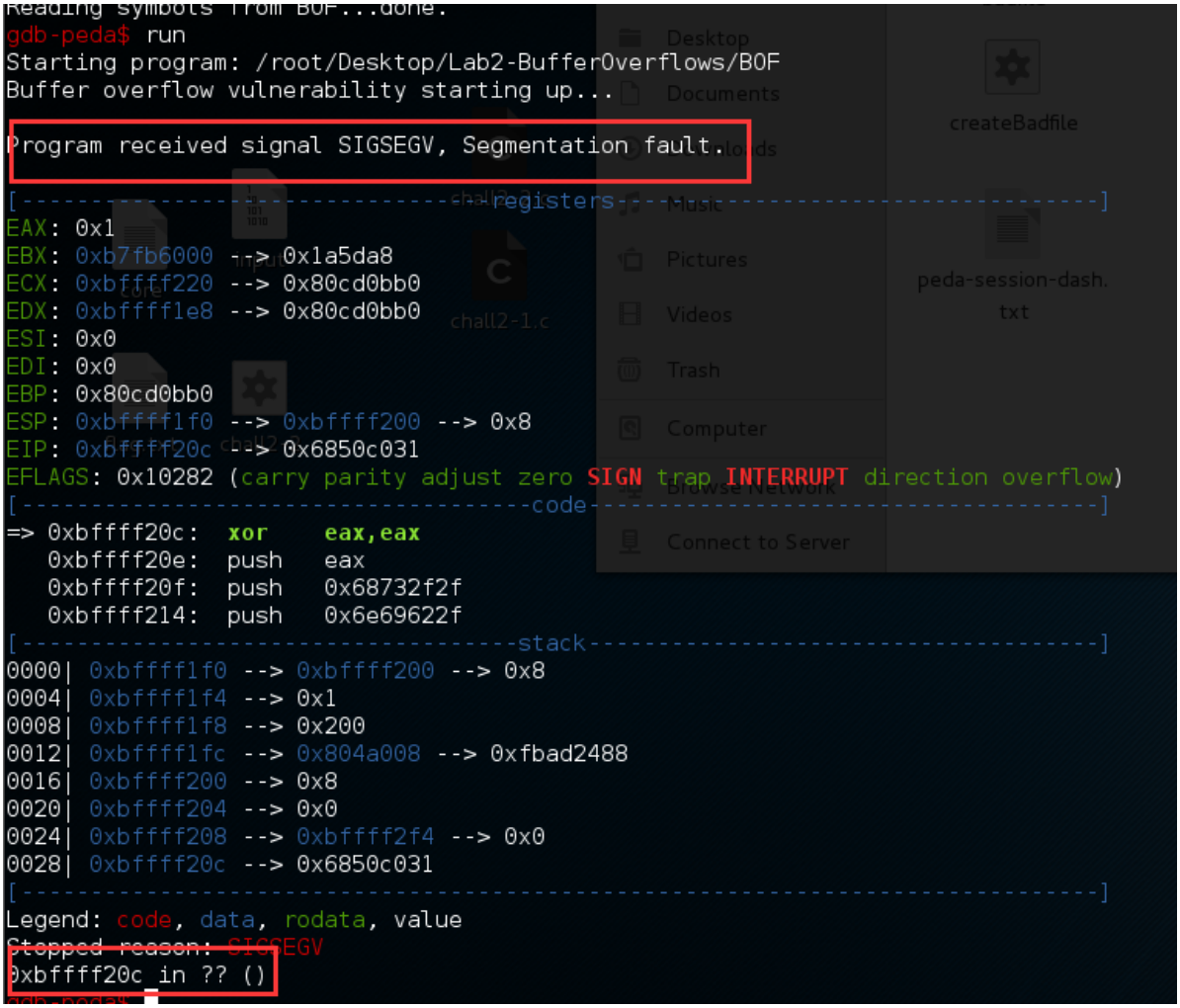
Lab2 report

11912039 郑鑫颖

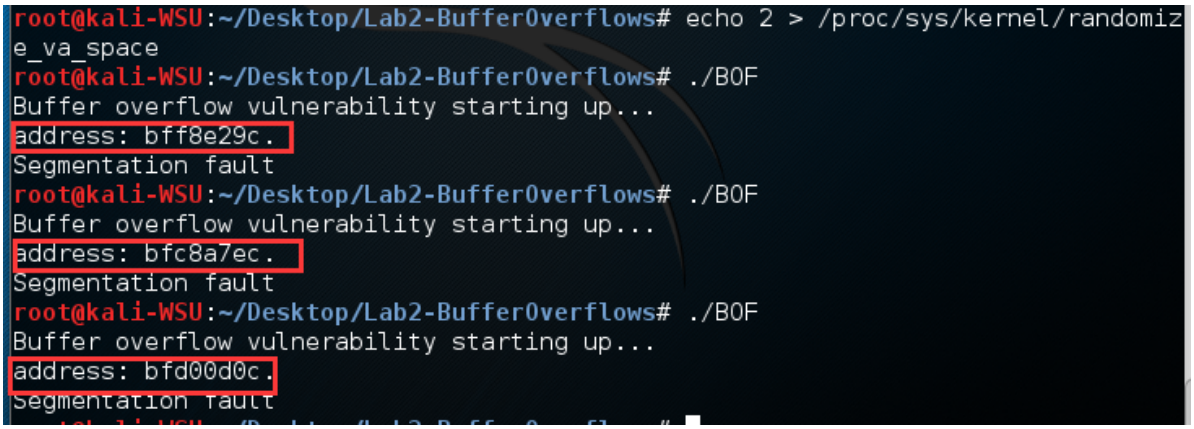
a. What happens when you compile without "-z execstack"?

Since "-z execstack" turns off the NX protection to make the stack executable. So when I turn on it, it all reports a segement fault as follows.



b. What happens if you enable ASLR? Does the return address change?

Definitely yes. When I enable the ASLR, the return address changes each time. So if I don't change my code, I would get a segment fault.

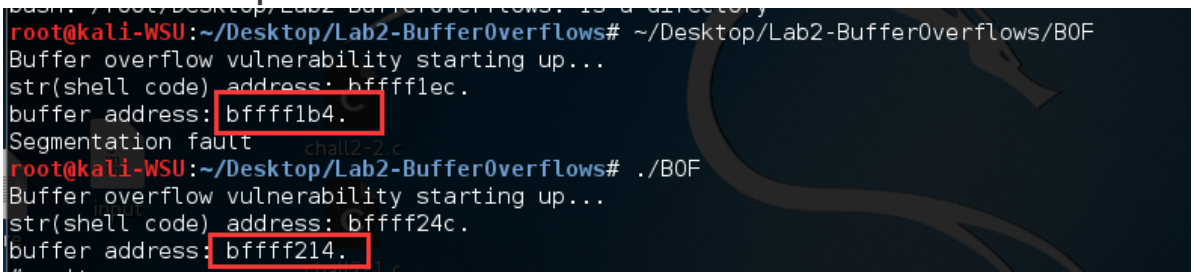


c. Does the address of the buffer[] in memory change when you run BOF using GDB, /home/root/Desktop/Lab2-BufferOverflows/BOF, and ./BOF?

They are all different.

GDB:

/home/root/Desktop/Lab2-BufferOverflows/BOF and **./BOF**



The reasons are as follows:

The contents of the environment variable are changed. When the program is run directly, the \variable holds the execution path of the program, butwhen the program is run through GDB, the variable holds the execution path of GDB. So the address of the variable will change due to different environment.