Setup instruction:

```
$ cd lab05_exercise/exercise/
$ make
```

Tasks:

- Use gdb to examine the stack
- Break into the function that calls the vulnerable strcpy
- Locate the current stack frame
- Locate the buffer buf1 in the stack
- Locate the return address in the stack
- Cause a segmentation fault
- Hint: Overflow the buffer until the function return address is overwritten

Submission:

Please submit a detailed report in pdf with descriptions of how you finished each task above. For each task, please include screenshots of commands you used with explanations.