# Secure programming
# Homework 3
## Due: Friday, Nov. 18, 2016

The practice of buffer overflow: Creating a shellcode.

Create a shellcode for Fig. 1 (in Homework 1) to execute an arbitrary program, such as /usr/bin/vi (or other programs) in the Linux system. You should illustrate how to find the function return address and change it to execute your designed malicious code. Again, **you may disable some protections by OS or compilers to make your attack successful** (note that you should disable stack protection and make the shell code executable in stack (-z execstack) as gcc compiling).
*First, you can manually try to attack the program within GDB or in command line. If possible, you may also write some programs (such as C/C++, Python or Perl) to automatically establish the attack scenario instead of manually launching the attacks.