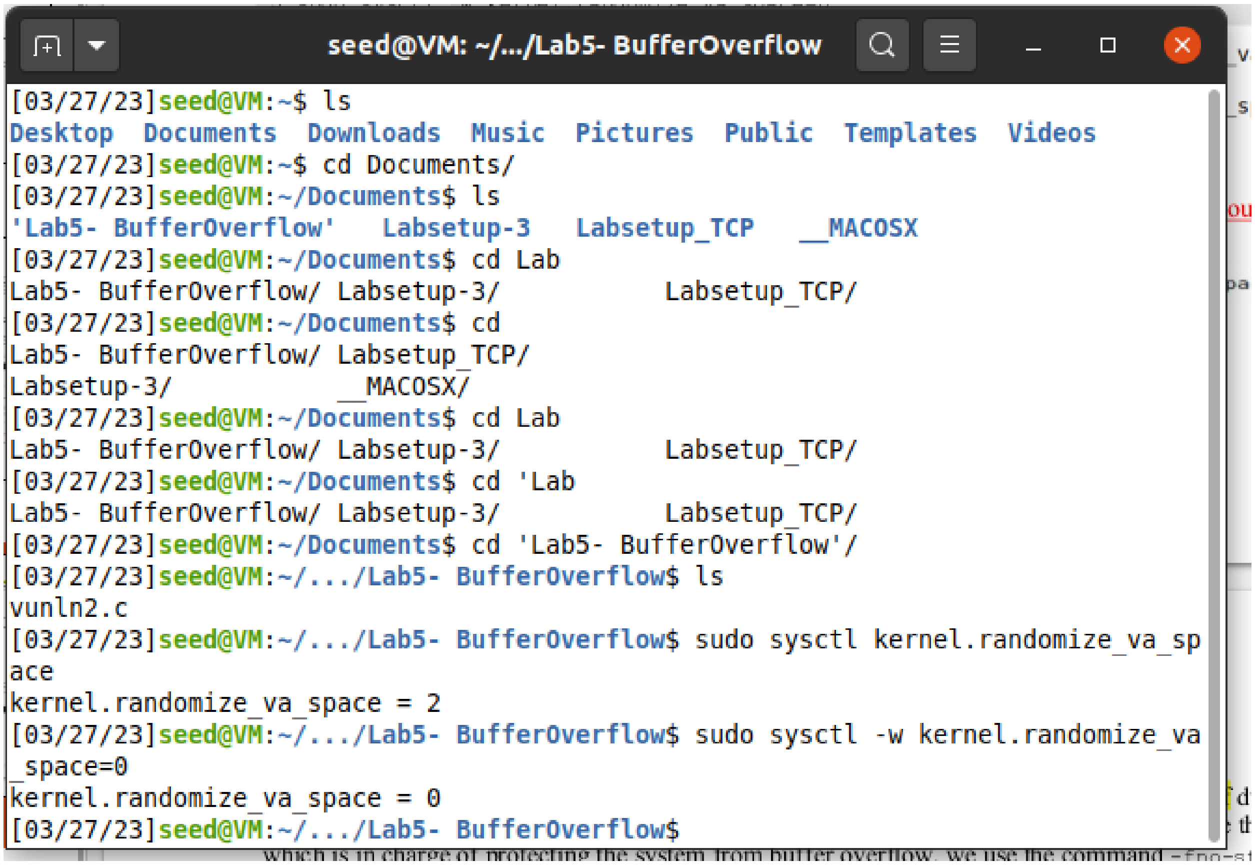
Lab #05 – Buffer Overflow

Lab Group 13
Kalid Ajibade (100660188)
Walid Ayub (100695612)
Zain Butt (100751676)
Konrad Herbus (100768380)

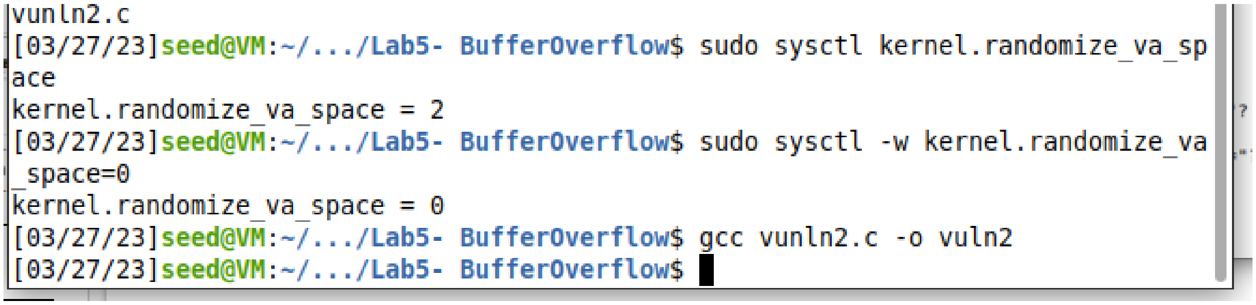
2.1 Initial setup

Address Space Randomization

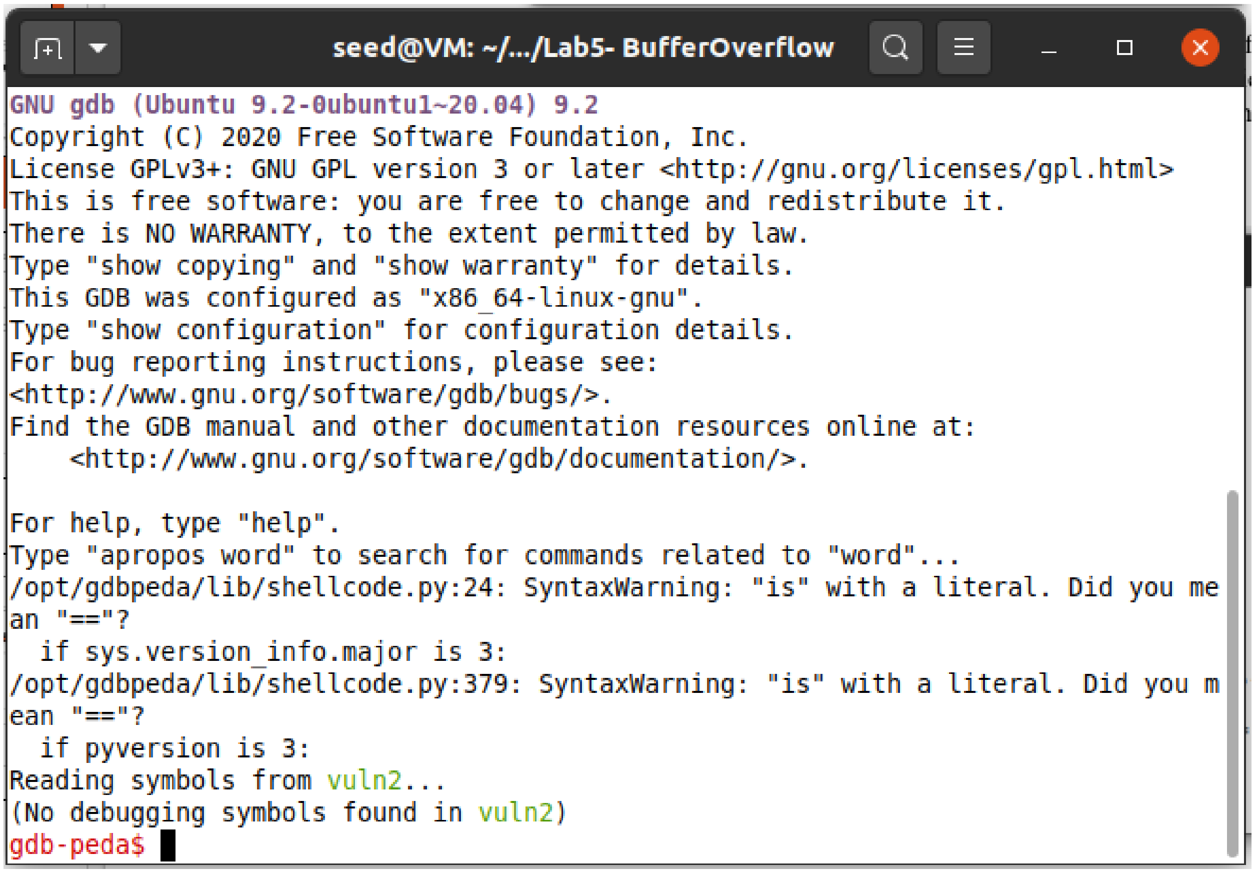


```
[03/27/23]seed@VM:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[03/27/23]seed@VM:~$ cd Documents/
[03/27/23]seed@VM:~/Documents$ ls
'Lab5- BufferOverflow'   Labsetup-3   Labsetup_TCP   __MACOSX
[03/27/23]seed@VM:~/Documents$ cd Lab
Lab5- BufferOverflow/ Labsetup-3/           Labsetup_TCP/
[03/27/23]seed@VM:~/Documents$ cd
Lab5- BufferOverflow/ Labsetup_TCP/
Labsetup-3/            __MACOSX/
[03/27/23]seed@VM:~/Documents$ cd Lab
Lab5- BufferOverflow/ Labsetup-3/           Labsetup_TCP/
[03/27/23]seed@VM:~/Documents$ cd 'Lab
Lab5- BufferOverflow/ Labsetup-3/           Labsetup_TCP/
[03/27/23]seed@VM:~/Documents$ cd 'Lab5- BufferOverflow'/
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ ls
vunln2.c
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ sudo sysctl kernel.randomize_va_sp
ace
kernel.randomize_va_space = 2
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ sudo sysctl -w kernel.randomize_va
_space=0
kernel.randomize_va_space = 0
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$
```

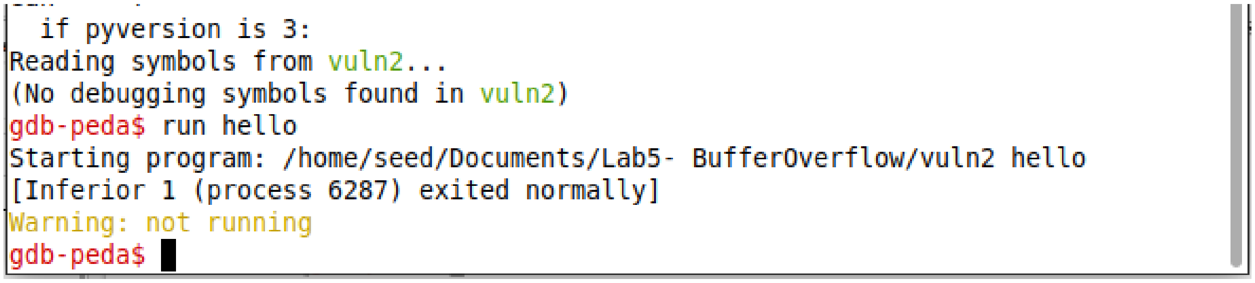
2.2 The Vulnerable Program



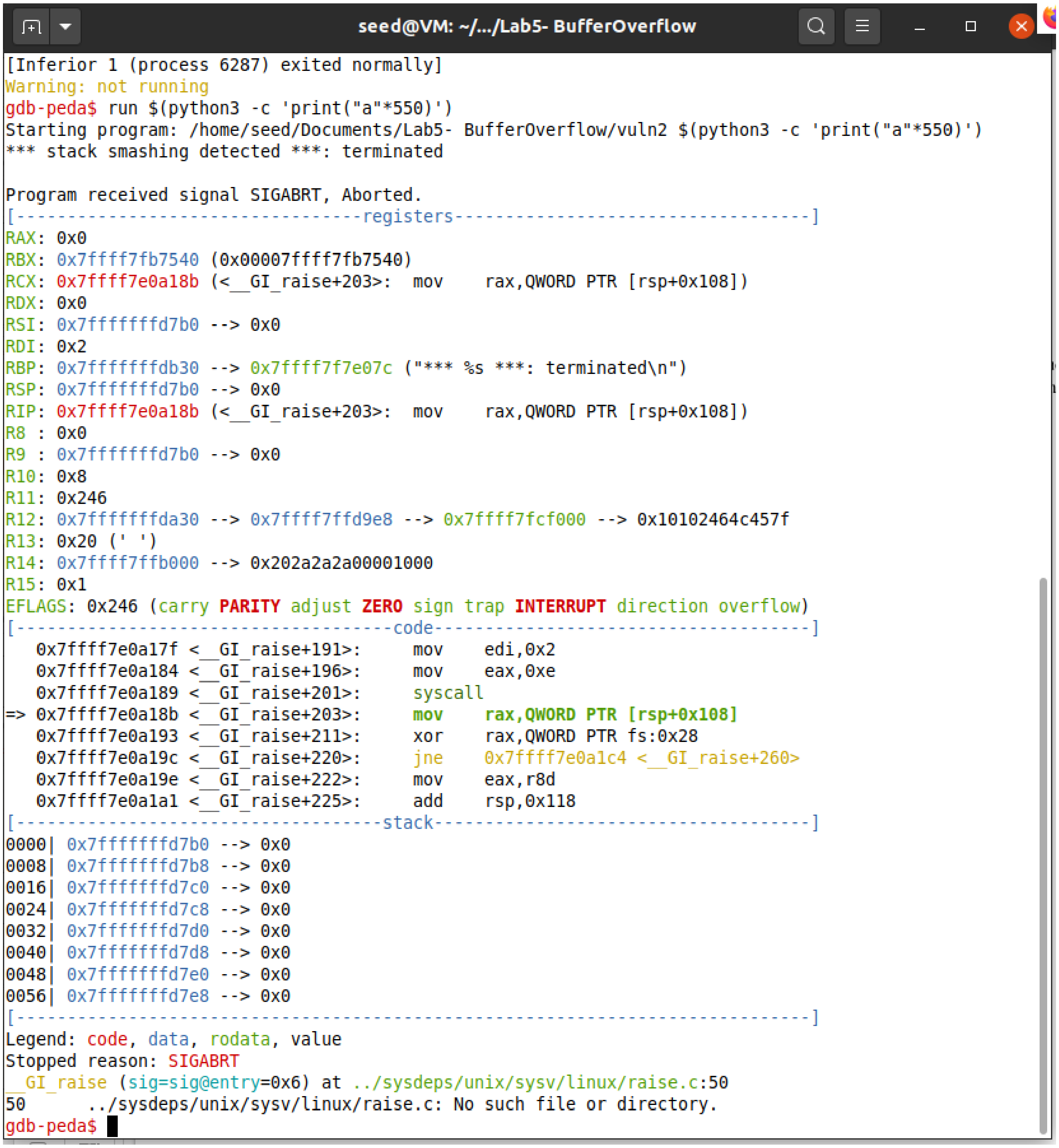
```
vunln2.c
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ sudo sysctl kernel.randomize_va_sp
ace
kernel.randomize_va_space = 2
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ sudo sysctl -w kernel.randomize_va
_space=0
kernel.randomize_va_space = 0
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ gcc vunln2.c -o vuln2
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ 
```



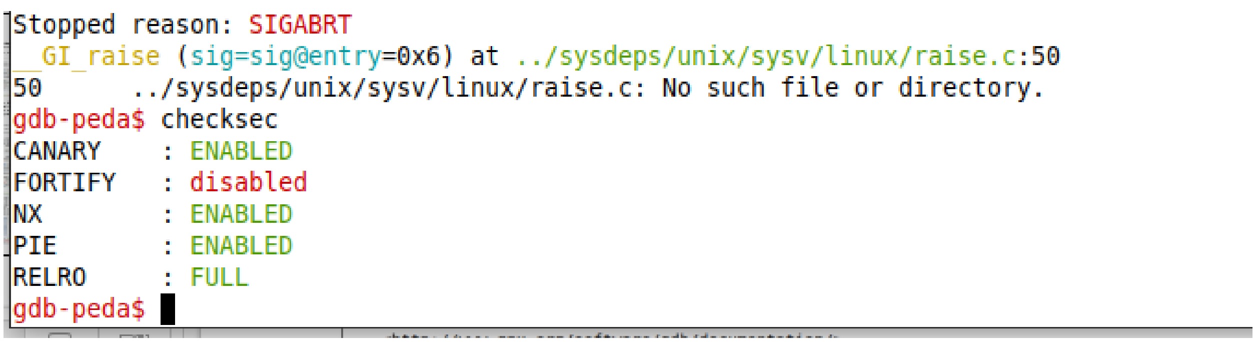
```
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
/opt/gdbpeda/lib/shellcode.py:24: SyntaxWarning: "is" with a literal. Did you me
an "=="?
  if sys.version_info.major is 3:
/opt/gdbpeda/lib/shellcode.py:379: SyntaxWarning: "is" with a literal. Did you m
ean "=="?
  if pyversion is 3:
Reading symbols from vuln2...
(No debugging symbols found in vuln2)
gdb-peda$ 
```



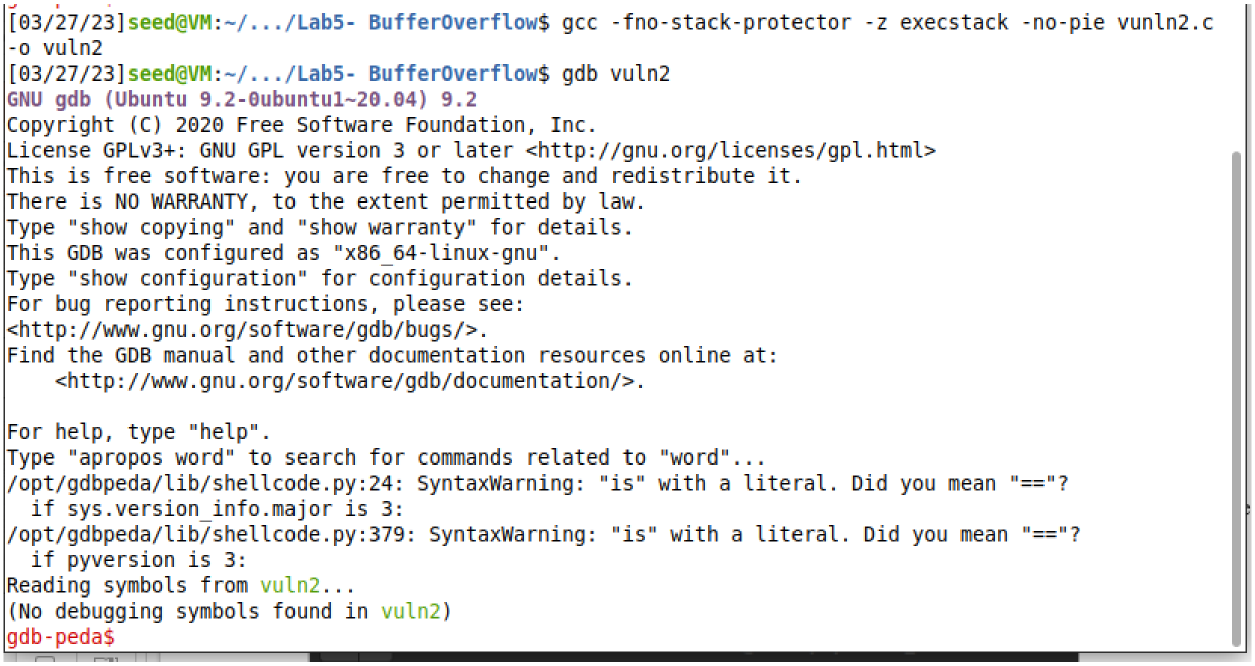
```
  if pyversion is 3:
Reading symbols from vuln2...
(No debugging symbols found in vuln2)
gdb-peda$ run hello
Starting program: /home/seed/Documents/Lab5- BufferOverflow/vuln2 hello
[Inferior 1 (process 6287) exited normally]
Warning: not running
gdb-peda$ 
```



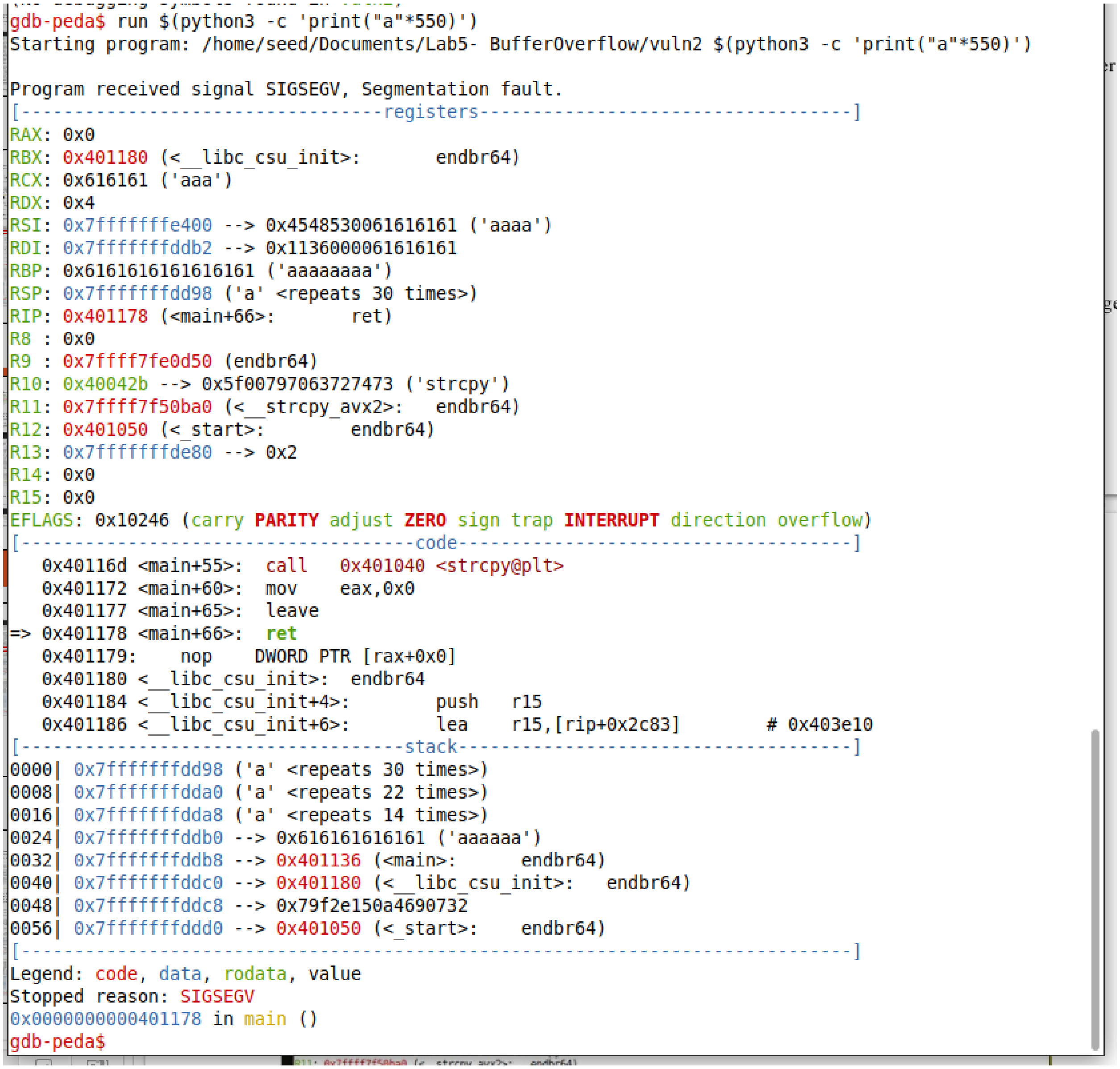
```
[Inferior 1 (process 6287) exited normally]
Warning: not running
gdb-peda$ run $(python3 -c 'print("a"*550)')
Starting program: /home/seed/Documents/Lab5- BufferOverflow/vuln2 $(python3 -c 'print("a"*550)')
*** stack smashing detected ***: terminated

Program received signal SIGABRT, Aborted.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x7ffff7fb7540 (0x00007ffff7fb7540)
RCX: 0x7ffff7e0a18b (<__GI_raise+203>:  mov    rax,QWORD PTR [rsp+0x108])
RDX: 0x0
RSI: 0x7fffffffd7b0 --> 0x0
RDI: 0x2
RBP: 0x7fffffffdb30 --> 0x7ffff7f7e07c ("*** %s ***: terminated\n")
RSP: 0x7fffffffd7b0 --> 0x0
RIP: 0x7ffff7e0a18b (<__GI_raise+203>:  mov    rax,QWORD PTR [rsp+0x108])
R8 : 0x0
R9 : 0x7fffffffd7b0 --> 0x0
R10: 0x8
R11: 0x246
R12: 0x7fffffffda30 --> 0x7ffff7ffd9e8 --> 0x7ffff7fcf000 --> 0x10102464c457f
R13: 0x20 (' ')
R14: 0x7ffff7ffb000 --> 0x202a2a2a00001000
R15: 0x1
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x7ffff7e0a17f <__GI_raise+191>:     mov    edi,0x2
   0x7ffff7e0a184 <__GI_raise+196>:     mov    eax,0xe
   0x7ffff7e0a189 <__GI_raise+201>:     syscall
=> 0x7ffff7e0a18b <__GI_raise+203>:     mov    rax,QWORD PTR [rsp+0x108]
   0x7ffff7e0a193 <__GI_raise+211>:     xor    rax,QWORD PTR fs:0x28
   0x7ffff7e0a19c <__GI_raise+220>:     jne    0x7ffff7e0a1c4 <__GI_raise+260>
   0x7ffff7e0a19e <__GI_raise+222>:     mov    eax,r8d
   0x7ffff7e0a1a1 <__GI_raise+225>:     add    rsp,0x118
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffd7b0 --> 0x0
0008| 0x7fffffffd7b8 --> 0x0
0016| 0x7fffffffd7c0 --> 0x0
0024| 0x7fffffffd7c8 --> 0x0
0032| 0x7fffffffd7d0 --> 0x0
0040| 0x7fffffffd7d8 --> 0x0
0048| 0x7fffffffd7e0 --> 0x0
0056| 0x7fffffffd7e8 --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGABRT
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:50
50      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
gdb-peda$ 
```



```
Stopped reason: SIGABRT
__GI_raise (sig=sig@entry=0x6) at ../sysdeps/unix/sysv/linux/raise.c:50
50      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
gdb-peda$ checksec
CANARY    : ENABLED
FORTIFY   : disabled
NX        : ENABLED
PIE       : ENABLED
RELRO     : FULL
gdb-peda$ 
```

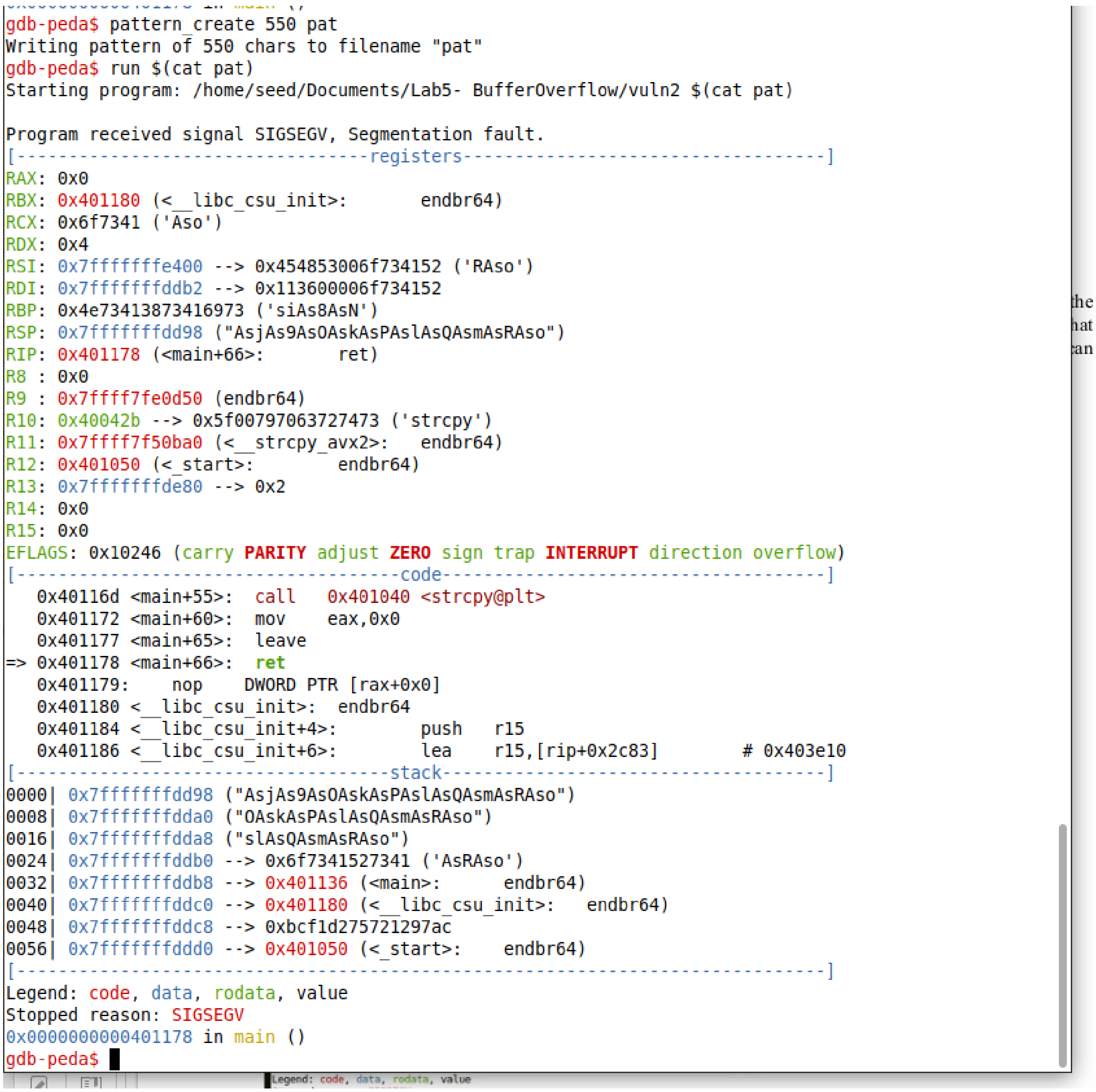


```
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ gcc -fno-stack-protector -z execstack -no-pie vunln2.c
-o vuln2
[03/27/23]seed@VM:~/.../Lab5- BufferOverflow$ gdb vuln2
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
/opt/gdbpeda/lib/shellcode.py:24: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if sys.version_info.major is 3:
/opt/gdbpeda/lib/shellcode.py:379: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if pyversion is 3:
Reading symbols from vuln2...
(No debugging symbols found in vuln2)
gdb-peda$
```



```
gdb-peda$ run $(python3 -c 'print("a"*550)')
Starting program: /home/seed/Documents/Lab5- BufferOverflow/vuln2 $(python3 -c 'print("a"*550)')

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x401180 (<__libc_csu_init>:       endbr64)
RCX: 0x616161 ('aaa')
RDX: 0x4
RSI: 0x7fffffffe400 --> 0x4548530061616161 ('aaaa')
RDI: 0x7fffffffddb2 --> 0x1136000061616161
RBP: 0x6161616161616161 ('aaaaaaaa')
RSP: 0x7fffffffdd98 ('a' <repeats 30 times>)
RIP: 0x401178 (<main+66>:       ret)
R8 : 0x0
R9 : 0x7ffff7fe0d50 (endbr64)
R10: 0x40042b --> 0x5f00797063727473 ('strcpy')
R11: 0x7ffff7f50ba0 (<__strcpy_avx2>:   endbr64)
R12: 0x401050 (<_start>:        endbr64)
R13: 0x7fffffffde80 --> 0x2
R14: 0x0
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x40116d <main+55>:  call   0x401040 <strcpy@plt>
   0x401172 <main+60>:  mov    eax,0x0
   0x401177 <main+65>:  leave
=> 0x401178 <main+66>:  ret
   0x401179:    nop    DWORD PTR [rax+0x0]
   0x401180 <__libc_csu_init>:  endbr64
   0x401184 <__libc_csu_init+4>:        push   r15
   0x401186 <__libc_csu_init+6>:        lea    r15,[rip+0x2c83]        # 0x403e10
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffdd98 ('a' <repeats 30 times>)
0008| 0x7fffffffdda0 ('a' <repeats 22 times>)
0016| 0x7fffffffdda8 ('a' <repeats 14 times>)
0024| 0x7fffffffddb0 --> 0x616161616161 ('aaaaaa')
0032| 0x7fffffffddb8 --> 0x401136 (<main>:      endbr64)
0040| 0x7fffffffddc0 --> 0x401180 (<__libc_csu_init>:   endbr64)
0048| 0x7fffffffddc8 --> 0x79f2e150a4690732
0056| 0x7fffffffddd0 --> 0x401050 (<_start>:    endbr64)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x0000000000401178 in main ()
gdb-peda$
```

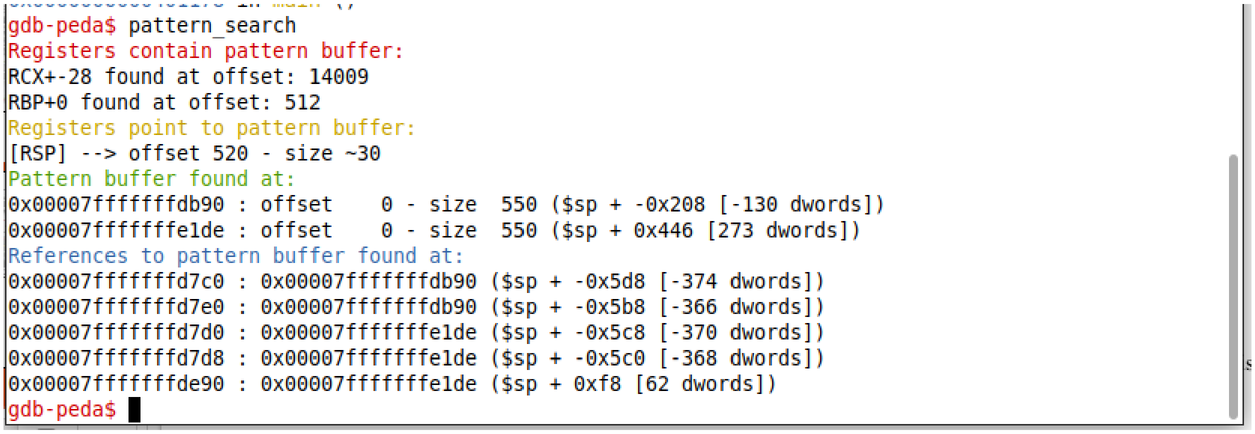
2.3 Observations on Buffer overflow



```
0x0000000000401178 in main ()
gdb-peda$ pattern_create 550 pat
Writing pattern of 550 chars to filename "pat"
gdb-peda$ run $(cat pat)
Starting program: /home/seed/Documents/Lab5- BufferOverflow/vuln2 $(cat pat)

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x401180 (<__libc_csu_init>:       endbr64)
RCX: 0x6f7341 ('Aso')
RDX: 0x4
RSI: 0x7ffffffe400 --> 0x454853006f734152 ('RAso')
RDI: 0x7fffffffddb2 --> 0x113600006f734152
RBP: 0x4e73413873416973 ('siAs8AsN')
RSP: 0x7fffffffdd98 ("AsjAs9AsOAskAsPAslAsQAsmAsRAso")
RIP: 0x401178 (<main+66>:       ret)
R8 : 0x0
R9 : 0x7ffff7fe0d50 (endbr64)
R10: 0x40042b --> 0x5f00797063727473 ('strcpy')
R11: 0x7ffff7f50ba0 (<__strcpy_avx2>:   endbr64)
R12: 0x401050 (<_start>:        endbr64)
R13: 0x7fffffffde80 --> 0x2
R14: 0x0
R15: 0x0
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x40116d <main+55>:  call   0x401040 <strcpy@plt>
   0x401172 <main+60>:  mov    eax,0x0
   0x401177 <main+65>:  leave
=> 0x401178 <main+66>:  ret
   0x401179:    nop    DWORD PTR [rax+0x0]
   0x401180 <__libc_csu_init>:  endbr64
   0x401184 <__libc_csu_init+4>:        push   r15
   0x401186 <__libc_csu_init+6>:        lea    r15,[rip+0x2c83]        # 0x403e10
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffdd98 ("AsjAs9AsOAskAsPAslAsQAsmAsRAso")
0008| 0x7fffffffdda0 ("OAskAsPAslAsQAsmAsRAso")
0016| 0x7fffffffdda8 ("slAsQAsmAsRAso")
0024| 0x7fffffffddb0 --> 0x6f7341527341 ('AsRAso')
0032| 0x7fffffffddb8 --> 0x401136 (<main>:      endbr64)
0040| 0x7fffffffddc0 --> 0x401180 (<__libc_csu_init>:   endbr64)
0048| 0x7fffffffddc8 --> 0xbcf1d275721297ac
0056| 0x7fffffffddd0 --> 0x401050 (<_start>:    endbr64)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x0000000000401178 in main ()
gdb-peda$ 
```

Legend: code, data, rodata, value

the
hat
an



```
gdb-peda$ pattern_search
Registers contain pattern buffer:
RCX+-28 found at offset: 14009
RBP+0 found at offset: 512
Registers point to pattern buffer:
[RSP] --> offset 520 - size ~30
Pattern buffer found at:
0x00007fffffffdb90 : offset    0 - size  550 ($sp + -0x208 [-130 dwords])
0x00007fffffffe1de : offset    0 - size  550 ($sp + 0x446 [273 dwords])
References to pattern buffer found at:
0x00007fffffffd7c0 : 0x00007fffffffdb90 ($sp + -0x5d8 [-374 dwords])
0x00007fffffffd7e0 : 0x00007fffffffdb90 ($sp + -0x5b8 [-366 dwords])
0x00007fffffffd7d0 : 0x00007fffffffe1de ($sp + -0x5c8 [-370 dwords])
0x00007fffffffd7d8 : 0x00007fffffffe1de ($sp + -0x5c0 [-368 dwords])
0x00007fffffffde90 : 0x00007fffffffe1de ($sp + 0xf8 [62 dwords])
gdb-peda$ 
```