Lab2

Name: 黎诗龙

SID: 11811407

4.

(a) It will occur segmentation fault.

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gcc -g -fno-stack-protector BOF.c -o BOF
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ./BOF
Buffer overflow vulnerability starting up...
Segmentation fault
```

(b) It will occur segmentation fault in the command line, **but** it still can be run in the GDB. The return address changes.

I add a sentence `print("Buffer address: %p", buffer)` in the function `bufferOverflow`, which comes from my classmates Zunyao, Mao, to print the buffer address.

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# echo 2 > /proc/sys/kernel/randomiz
e_va_space
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ./BOF
Buffer overflow vulnerability starting up...
Buffer address: 0xbf952d34
Segmentation fault
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# echo 0 > /proc/sys/kernel/randomiz
e_va_space
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ./BOF
Buffer overflow vulnerability starting up...
Buffer address: 0xbffff274
# exit
```

From the buffer address we can infer that the return address has been **changed**.

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gdb BOF
GNU gdb (Debian 7.7.1+dfsg-5) 7.7.1
Copyright (C) 2014 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 "i586-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"...
Reading symbols from BOF...done.
(gdb) run
Starting program: /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...
process 6475 is executing new program: /bin/dash
#
```

(c) They are not the same.

method	buffer[] address
gdb BOF	0xbffff204
/root/Desktop/Lab2-BufferOverflows/BOF	0xbffff214
./BOF	0xbffff274

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# ./BOF
Buffer overflow vulnerability starting up...
Buffer address: 0xbffff274
# exit
```

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# gdb BOF
GNU gdb (Debian 7.7.1+dfsg-5) 7.7.1
Copyright (C) 2014 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 "i586-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"...
Reading symbols from BOF...done.
(gdb) run
Starting program: /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...
Buffer address: 0xbffff204
process 6553 is executing new program: /bin/dash
# exit
```

```
root@kali-WSU:~/Desktop/Lab2-BufferOverflows# /root/Desktop/Lab2-BufferOverflows/BOF
Buffer overflow vulnerability starting up...
Buffer address: 0xbffff214
Segmentation fault
```