Format String Vulnerability

Name: Alizeh Jafri

Task 1.1

First I created the file called ‘vul_prog.c’ and entered the code which was provided to us in that file as shown in the screen shot below:

```
root@VM:/home/seed# nano vul_prog.c
root@VM:/home/seed# cat vul_prog.c
/* vul_prog.c */
#include<stdio.h>
#include<stdlib.h>
#define SECRET1 0x44
#define SECRET2 0x55int 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("secret[0]'s address is 0x%8x (on heap)\n", (unsigned int)&secret[0]
);
```

Next in root, I compiled (vul_prog.c) file as shown:

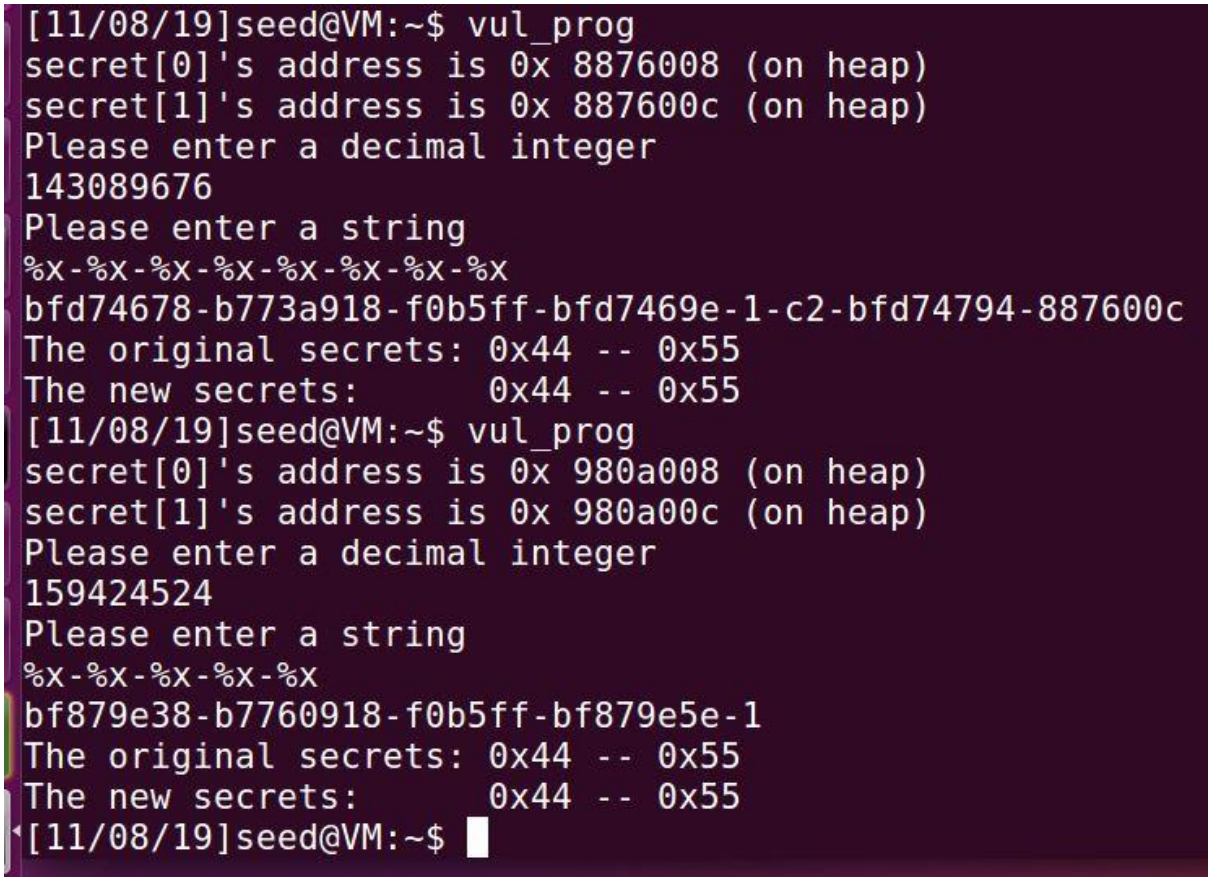
```
root@VM:/home/seed# gcc -o vul_prog vul_prog.c
vul_prog.c: In function ‘main’:
vul_prog.c:28:12: warning: format not a string literal and no format arguments [
-Wformat-security]
     printf(user_input);
            ^
root@VM:/home/seed# chmod 4755 vul_prog
root@VM:/home/seed# su seed
```

Then in seed, I ran the program, and I crashed it by entering the format strings with several ‘%s’ characters to crash the program. You can see the ‘Segmentation fault’ which shows that the program has been crashed successfully. As shown below:

```
[11/08/19]seed@VM:~$ vul_prog
secret[0]'s address is 0x 8706008 (on heap)
secret[1]'s address is 0x 870600c (on heap)
Please enter a decimal integer
3456
Please enter a string
%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
Segmentation fault
[11/08/19]seed@VM:~$
```

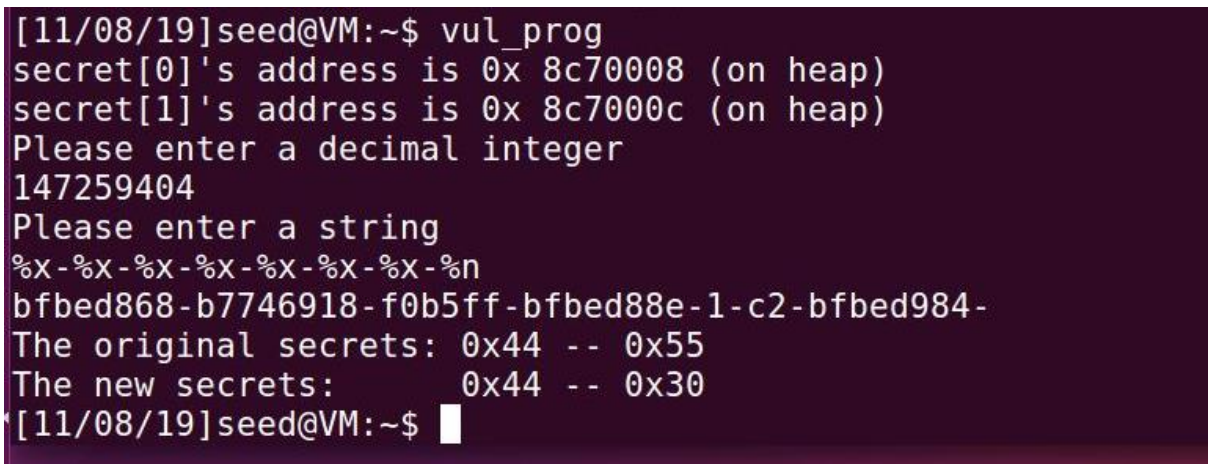
Task 1.2

I entered 'vul_prog' and it gave me secret [0] and secret [1]. I converted secret [1] into decimal and entered the decimal integer. Then I entered the string as shown below:



Task 1.3

Now, I modified the secret [1] and the value of secret [1] has been changed to 0x30:



Task 1.4

Then, I modified the secret [1] value to a pre-determined value by entering another string. You can see that value of secret [1] is modified to the pre-determined value (0x50). Here, I entered 32 bytes to get the new secret value 0x50 as shown below.