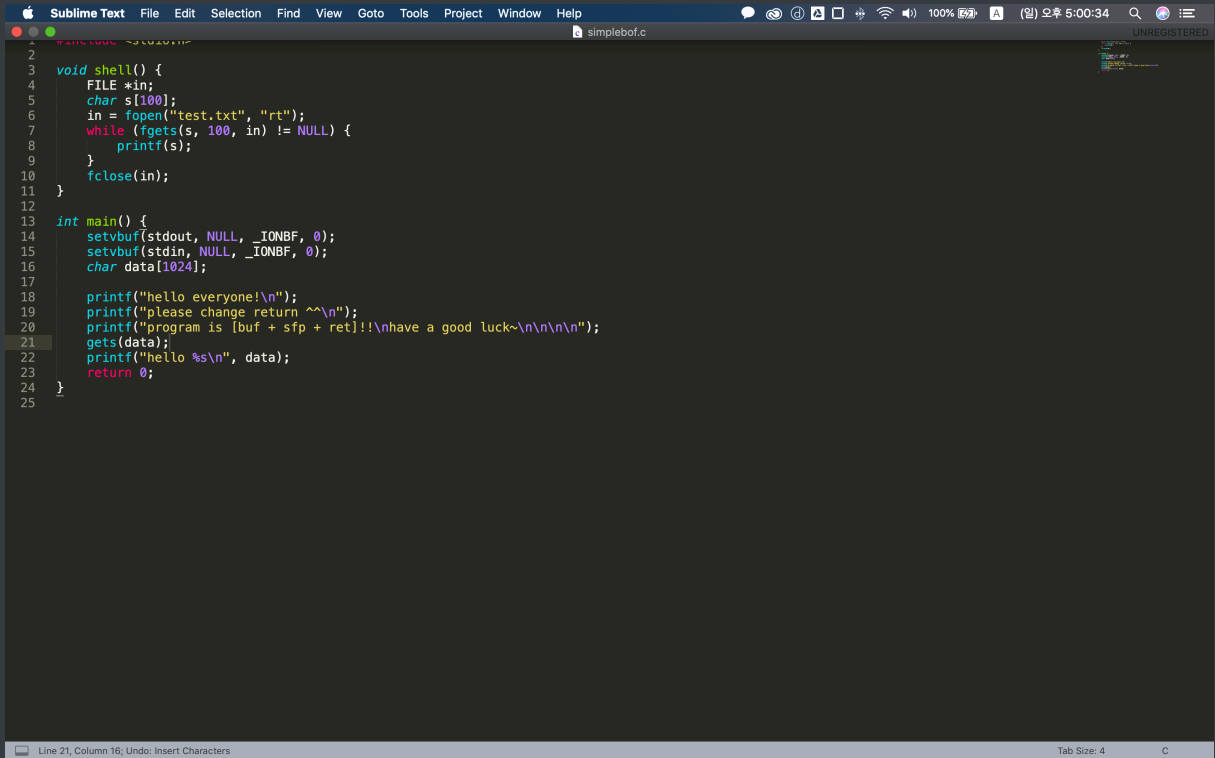


2019_06_01_9차시

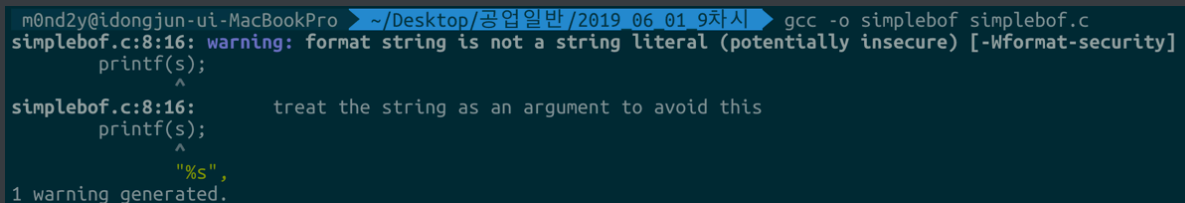
BOF취약점을 이용해서 문제 만들기

1. 입력을 받는 부분에서 배열의 최대값을 넘기게 만들기.



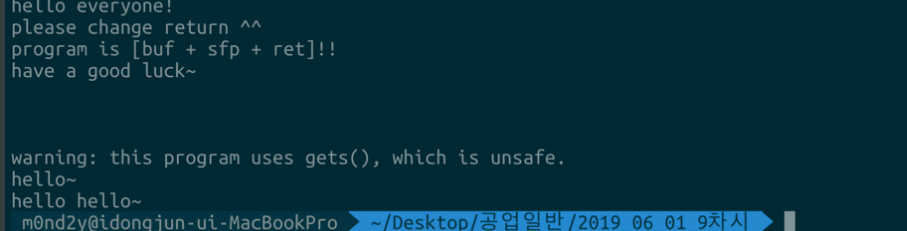
```
1 #include <stdio.h>
2
3 void shell() {
4     FILE *in;
5     char s[100];
6     in = fopen("test.txt", "rt");
7     while (fgets(s, 100, in) != NULL) {
8         printf(s);
9     }
10    fclose(in);
11 }
12
13 int main() {
14     setvbuf(stdout, NULL, _IONBF, 0);
15     setvbuf(stdin, NULL, _IONBF, 0);
16     char data[1024];
17
18     printf("hello everyone!\n");
19     printf("please change return ^^ \n");
20     printf("program is [buf + sfp + ret]!! \nhave a good luck~ \n \n \n");
21     gets(data);
22     printf("hello %s \n", data);
23     return 0;
24 }
25
```

3. Gcc 컴파일하기



```
m0nd2y@idongjun-ui-MacBookPro ~/Desktop/공업일반/2019_06_01_9차시$ gcc -o simplebof simplebof.c
simplebof.c:8:16: warning: format string is not a string literal (potentially insecure) [-Wformat-security]
    printf(s);
               ^
simplebof.c:8:16:      treat the string as an argument to avoid this
    printf(s);
               ^
               "%s",
1 warning generated.
```

4. 실행하기



```
m0nd2y@idongjun-ui-MacBookPro ~/Desktop/공업일반/2019_06_01_9차시$ ./simplebof
hello everyone!
please change return ^^
program is [buf + sfp + ret]!!
have a good luck~

warning: this program uses gets(), which is unsafe.
hello~
hello hello~
m0nd2y@idongjun-ui-MacBookPro ~/Desktop/공업일반/2019_06_01_9차시$
```

5. 실행하기