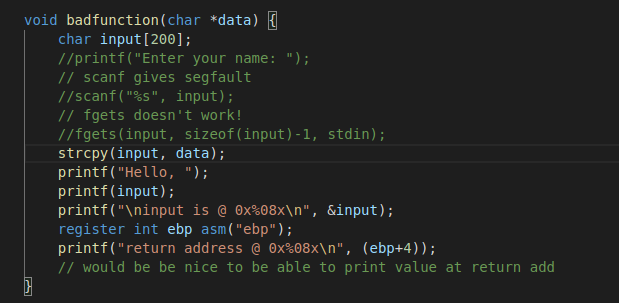
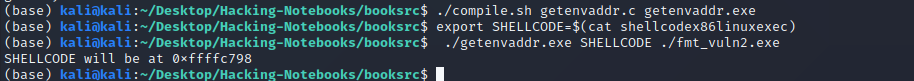
Kimlong Seng

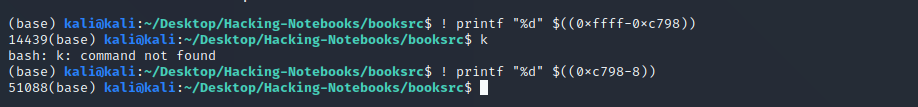
Project 01

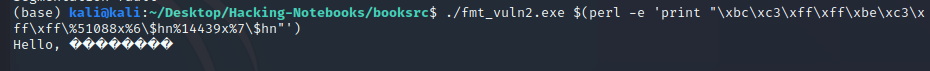
1. Vulnerability
2. Prinf(input) in the badfuntion, Format String Vulnerability happen when u write printf without a proper parameter (%) i.e. printf(string) instead of printf(“%s”, string).



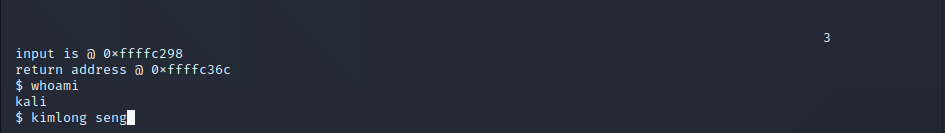
1. Stash shellcode

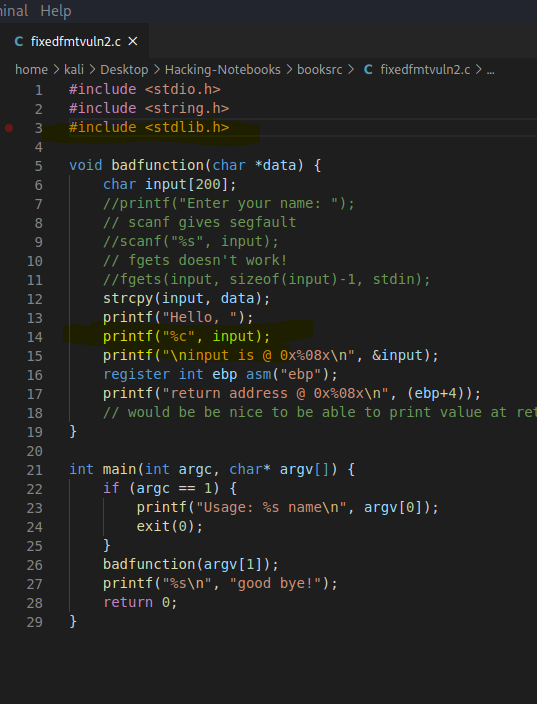


1. Calculate the width by taking the shellcode address 
2. Using the width and shellcode





1. After following the book and calculating the width of the input memory address and plug it in. it did not give me a shellcode but it prints out a new set of input memory and return address (0xffffc36c). So, I redo the process with the new set of memory address, and it work.  
2. Fixing the vulnerability at “%C” to the print and #include <stdlib.h> to clear warning sign



b. after fixing it, I can no longer inject the shellcode to the input

