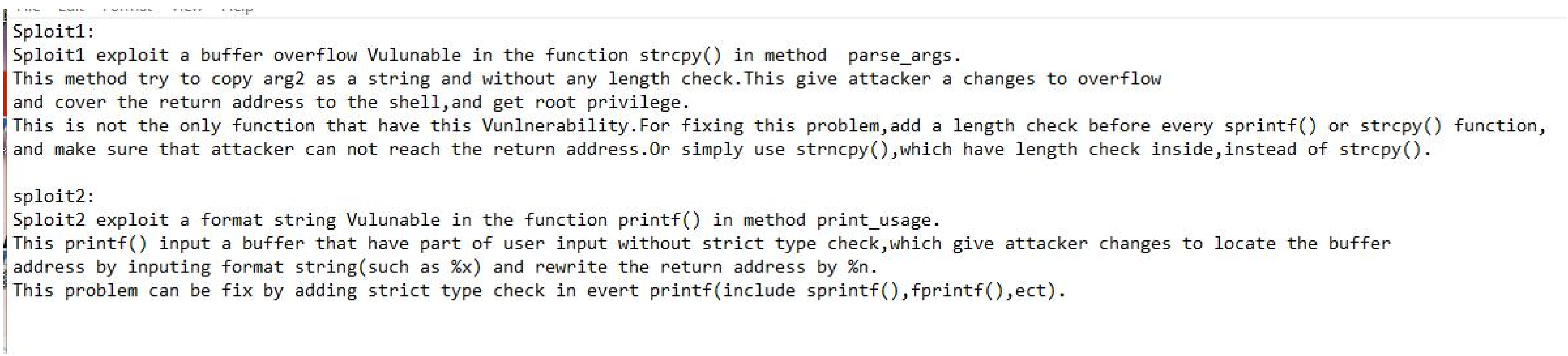

Sploit1:
Sploit1 exploit a buffer overflow Vulunable in the function strcpy() in method parse_args.
This method try to copy arg2 as a string and without any length check.This give attacker a changes to overflow
and cover the return address to the shell,and get root privilege.
This is not the only function that have this Vunlnerability.For fixing this problem,add a length check before every sprintf() or strcpy() function,
and make sure that attacker can not reach the return address.Or simply use strncpy(),which have length check inside,instead of strcpy().

sploit2:
Sploit2 exploit a format string Vulunable in the function printf() in method print_usage.
This printf() input a buffer that have part of user input without strict type check,which give attacker changes to locate the buffer
address by inputing format string(such as %x) and rewrite the return address by %n.
This problem can be fix by adding strict type check in evert printf(include sprintf(),fprintf(),ect).