# CS458a1-milestone

Bo Liu
b69liu
20521697

September 2017

## 1 sploit1

The buffer in main function to store path is only 200 long, and it did not limit the length of path. So we can use buffer overflow to overwrite the return address near it in memory.
Fix: check the second input and limit it length.

## 2 sploit2

The ls command uses a embedded shell script stored somewhere in the system. So we can overwrite it.
Fix: check the directory of the ls file.