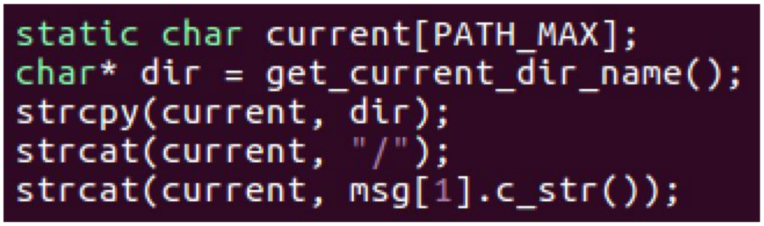
CS527 Project Bug Hunting Report

Team 8:

Team 1

1. Stack Overflow

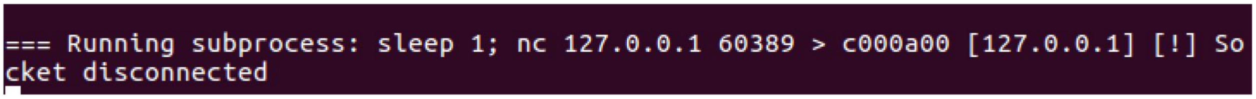


```
static char current[PATH_MAX];
char* dir = get_current_dir_name();
strcpy(current, dir);
strcat(current, "/");
strcat(current, msg[1].c_str());
```

PATH_MAX=4096. When the length of current directory path plus the length of the first argument (msg[1]) of cd command, the length of current can exceed its bound.

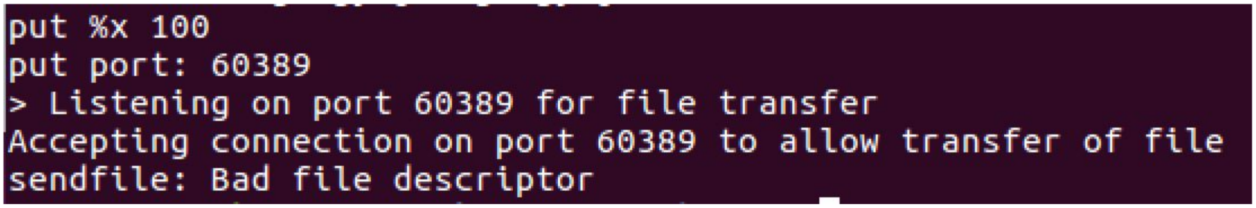
2. Format String

Common.cpp line 35: fprintf(stderr, msg.c_str());
When client executes put command with file name including format string such as “put %x 100”, server will output memory information, and client will be disconnected.
Server output:



```
=== Running subprocess: sleep 1; nc 127.0.0.1 60389 > c000a00 [127.0.0.1] [!] So
cket disconnected
```

Client output:



```
put %x 100
put port: 60389
> Listening on port 60389 for file transfer
Accepting connection on port 60389 to allow transfer of file
sendfile: Bad file descriptor
```

3. Misc

- cd command does not support path length larger than 100 characters.
- Get a empty file from server will cause both server and client crashed.
- When the client is run within the base directory of server, get or put will crash both server and client.