CS 458/658
Assignment 1 (part 2)
Hanzhang Chen
ID: 20574275

Sploit2.c:

This is a TOCTOU attack, known as race condition attack. The state of the system changed between the check for permission and the execution of the operation. And there is a gap between the changing so that we can make use of it and do our attack.
When we do submit, we got the permission to write to submit.log. If we symlink it with /etc/passwd, we can even modify that file with different forks doing thing at the same time.
root:x:0:0:root:/root:/bin/bash ➔root::0:0:root:/root:/bin/bash
The missing x means require password for /etc/shadow. If we remove it, we can be root without password.

This attack can be solved: When performing a privileged action on behalf of another party, make sure all information relevant to the access control decision is constant between the time of the check and the time of the action (“the race”). Use something like locks to prevent this.