Attack plan

The idea is exploit the overflow in `gets()` to write a `G` character in the `permtd` array. This will allow the attacker to pass an arbitrary pattern to `grep` and thus read the flag, e.g., by passing the `.` wildcard, or some string known to be contained in the flag (e.g., `SNH`).

For example, we can overflow `buffer` with the following: