The milestone exploits the class B, in particular we are exposing the issue of Incomplete mediation through the environment variables.

When pwgen get user_id, it actually just reads in the value of “HOME” under env, which means if the value is illegally modified to say, “/root”, now the program would mistaken the user as root and when -w option is specified, it write to the shadow file and overwrite the password of root.

In order to fix this, the program should double check if “HOME”’s value is actually user’s id, in particular, C has other function like getuid() that is better suited for the job.