# Set-UID exercises

1. Turn a program into Set-IUD (slide 8): copy /bin/cat to your home folder as mycat and turn it into a set-uid program owned by root. See if you can display the root’s password hash in /etc/passwd.
2. EUID vs RUID (slide 9): copy /bin/id to your home folder as myid. Observe the change of RUID and EUID when you execute the program in normal mode and in set-uid mode.
3. Capability leaking (slide 20): Compile and run cap\_leak.c given in the source code folder to exploit the capability leaking vulnerability.
4. Vulnerable catall (slide 24): Given a vulnerable set-uid program catall.c. Let’s exploit the security hole of the system function call.
5. Safe catall version: Try again with safecatall.c and see if the security hole still exists.
6. PHP system call (slide 31): Write a php program to display the content of a directory given the path name. Name it list.php and put it in folder /var/www/html. Open a browser in your **host** machine and try to display /etc/passwd on your web server.