Z'vonty Flugence (zaf17)

Passwords:

- EkijXyKhJRcnpCOKHhWyjjDEHgpq
- 3.141593
- (Couldn't find it) - Algorithm

Write ups:

- At first i attempted to simply find the password by just doing a hexdump or using mystrings, and later the actual strings, but none of them worked (or so I thought, I later found that the password was in the strings output, but I couldn't tell until after i found it by stepping through the program). I found the first password by simply using gdb with the `set disassemble-next-line on` command, and stepped through the code line by line until the program exited the first fgets to get the user's string and returns to the main method to do a comparison. I tested the value at the address returned from the chomp function call, and it gave me the password. Due to the password coming up in strings, it leads me to believe that the password is a static fixed password.
- I attempted the same things as above, using hexdump and strings, but those still did not help. I also used gdb to step through the code, but after going through the code one full time and not making any progress, I used objdump -d -Mintel [file] command which allowed me to find the instructions which outputted the "Sorry"/"Congratulations" message, which I then used those addresses to stop through the code again setting breakpoints for the printf function that was called after their respective lines, then from that function I noticed that the code was continually gathering digits and one of the registers kept holding onto a '.' character. After stepping through the code once again, keeping a closer eye on all the registers, I finally found the password in $esi. However, unlike password 1, password 2 is actually created by an algorithm which
- I wasn't able to get the third password, however from what I did notice it seems to be an algorithm based approach which has a different password based on the input that it receives. I tried using strings, hexdump, and objdump on it but nothing seemed to give away anything. Additionally, when I tried to step through the program, it doesn't have a main function to enter into, so i couldn't run it initially. So i went back to the objdump and used the data from that to get a function name that is used (I used getchars) and set a breakpoint at that function, so i could start stepping through the code.