**Windows**

**flag 1, 2, 3**

**flag 1 and 2 is obvious, just ctrl+f and u can see the answers.**

**Now, let’s throw the windows into Ghidra. I use gcc windows to do analysis.**

**Graphical user interface, text, application

Description automatically generatedThis is how the main() function look like after performing decompilation.**

**Text

Description automatically generated**

**For function of flag 1, the password is “NNN”.**

**Graphical user interface, text, application

Description automatically generated**

**For function of flag 2, it is obvious to see pwVar3 is storing the flag value, which is also the password.**

**Graphical user interface, text, application

Description automatically generated**

**Since their algorithm is similar, for function 3, we guess the password is here, but here are just some junk unicode.**

**Therefore, I try to extract the code and throw it to Magic mode. Checking the output, I found that using XOR 4e, it will show the answer**

**Graphical user interface, text, application

Description automatically generated**

**There you go!**

**Graphical user interface, text, application

Description automatically generated**

**Text

Description automatically generated**