Pico CTFs Write Ups week 6:

1. Picker IV:
    a. Downloaded the binary and used "chmod +x picker-IV" to add executable permissions.
    b. Used "./picker-IV" and the program asked for a memory location to move to.
    c. I opened the program on Ghidra to read the code and found a win function that was not used that gave the flag that started on 0x0040129e.
    d. Ran the program again and entered that memory location to get the flag.
    e. picoCTF{n3v3r_jump_t0_u53r_5uppl13d_4ddr35535_b8de1af4}
2. bloat.py:
    a. Downloaded both files and ran the program with "python3 bloat.flag.py"
    b. The program asked for a password, as a result, I used "cat bloat.flag.py" to read the code and found that every string used inside the code was made up from this characters: "!\"#$%&'()*+,-
    ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ"+
    \"[\\]^_`abcdefghijklmnopqrstuvwxyz{|}~ "
    c. To understand the strings that were being used I used an online python compiler and copy and pasted the strings to be able to see what they formed until I found the section that asked for the password in an if statement.
    d. In the if block the password was used to compare the string that the user used as input and it was represented as "a[71]+a[64]+a[79]+a[79]+a[88]+a[66]+a[71]+a[64]+a[77]+a[66]+a[68]", a being the characters string.
    e. After printing the password was "happychance"
    f. picoCTF{d30bfu5c4710n_f7w_b8062eec}
3. Vigenere:
    a. Downloaded the cipher.txt and used "cat cipher.txt" to get the string "rgnoDVD{O0NU_WQ3_G1G3O3T3_A1AH3S_2951c89f}" and from the problem the key "CYLAB"
    b. After reading about the Vigenere cipher to get the flag I have to move each letter backwards by the position of the letter in the alphabet of the key. For example, the letter "C" from the key is the letter number 2 in the alphabet starting from 0, as a result, I have to move the letter "r" in the string 2 positions back, this results in the letter "p", to speed up the process I used an online decoder and got the flag.
    c. picoCTF{D0NT_US3_V1G3N3R3_C1PH3R_2951a89h}
4. Forbidden Paths:
    a. Entered the website and after inspecting it, its function was to read files, however, no absolute paths were able to be used like the problem stated.
    b. the website was located in "/usr/share/nginx/html/" and the flag in "/flag.txt" to reach the root one could use ".." to climb up the directories and reach the flag
    c. As a result, "../../../../flag.txt" would result in the flag since it would climb up the root and then open the text file with the flag.

d. picoCTF{7h3_p47h_70_5ucc355_e5fe3d4d}