Pico CTFs Write Ups week 5:

1. Picker III:
    a. Downloaded the python file and used "cat picker-III.py" to read the code.
    b. This time the code had a function table established from which it read the functions and called them, these functions were reset_table, read_variable, write_variable and getRandomNumber. They were accessed by numbers 1, 2, 3 and 4 (0, 1, 2, 3 by index).
    c. This function table was a string consisting of the name of the functions mentioned with spaces in between to reach a length of 128 characters, it had to be this length since if it wasn't the program would crash and say that the table was corrupted. In addition, the program used an offset to locate the name in the string, for example, if the user entered the number 2 it would multiply 1*32 = 32 and it will search for a nonspace character at that location and continue until a space is found, that's how it would grab the function name read_variable.
    d. In the program there was a function named win that gave the flag; however, it wasn't on the table. To access the function, modify the func_table variable with the function write_variable and change the string to "print_table read_variable write_variable win ". This string has 128 characters to avoid table corruption.
    e. This way the table won't be corrupted and when one selects the number 4 then 3*32 = 96 and that's where the "w" of win is located.
    f. After accessing the win function, it will give this hex numbers "7069636f4354467b376831355f31355f776834375f77335f6733375f773137685f75353372355f316e5f6368347267335f32323664643238357d" and in text it's the flag.
    g. picoCTF{7h15_15_wh47_w3_g37_w17h_u53r5_1n_ch4rg3_226dd285}