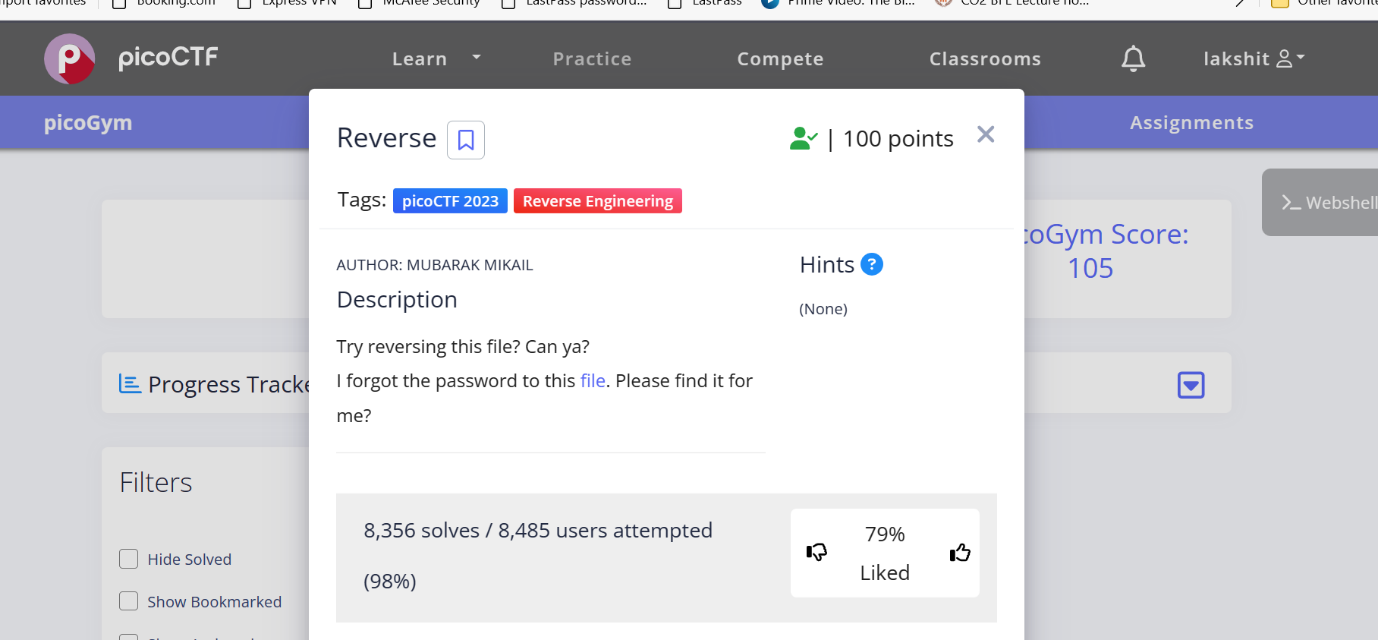
Reverse Engineering

The screenshots of the task have been attached in the fold er

1.Reverse – this task had a file , I downloaded the file ,opened it in the notepad .I easily found the flag picoCTF{3lf\_r3v3r5ing\_succe55ful\_9ae85289}.



2.ASCII FTW-this task had a file .it was a elf file . I used the command readelf –symbols asciiftw.i used chatgtp which said there is a high chance that the flag is in the main part of the file , then I used an online file disassembler Binary Ninja to disassemble the file ,in the main part of the file I found the flag.

