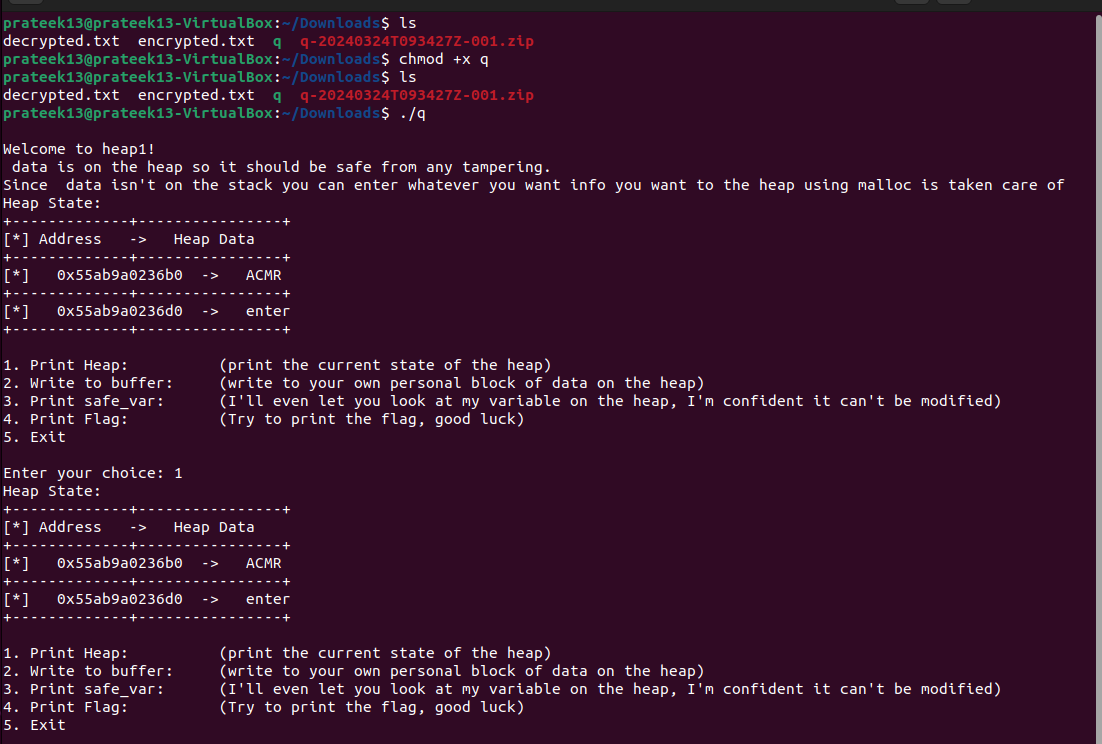
Q2. CAPTURE THE FLAG FROM A BINARY ELF FILE

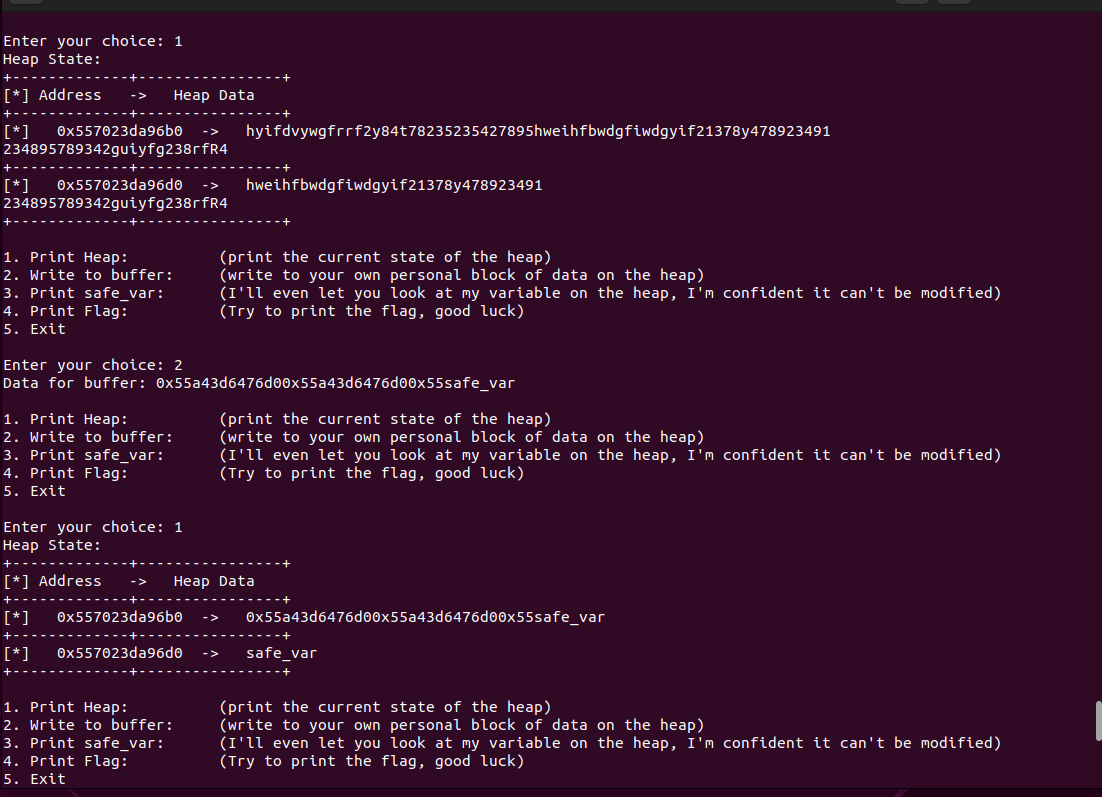
First I opened the file using cat q, where I found a mix of binary and human readable texts. So I ran file q. There I found the file to be of ELF format.

This is the output which I got “q: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=54cd3f5563708722f75088fe855b71cc1a7788c2, for GNU/Linux 3.2.0, not stripped”.

Then I ran chmod +x q followed by ./q toget access to the info in the file.



Here I was provided with some instructions to perform. I tried the 2nd option many a times where I noticed there is a change in heap data. The ACMR got replaced by the entered block of heap. If I entered something with spaces then the program terminated. So I thought of buffer overflowing to see any other change. And I entered long heap of data and found that there was a change of data in the section where enter is there. Below are the result I got



A screenshot of a computer

Description automatically generated