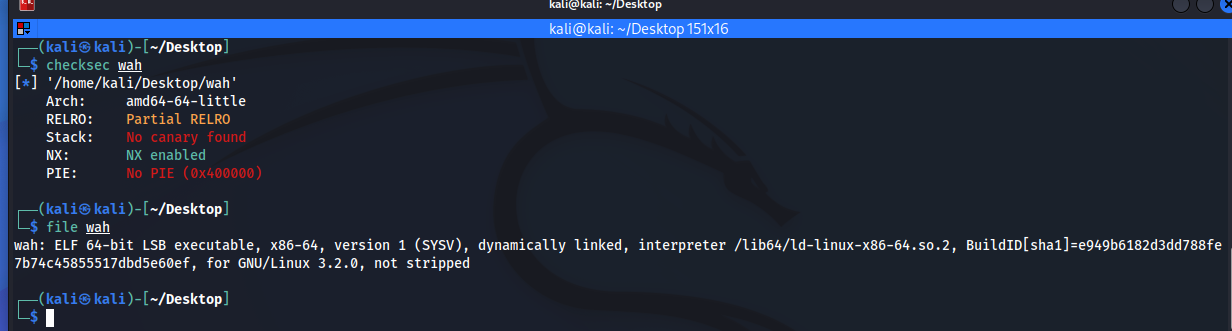
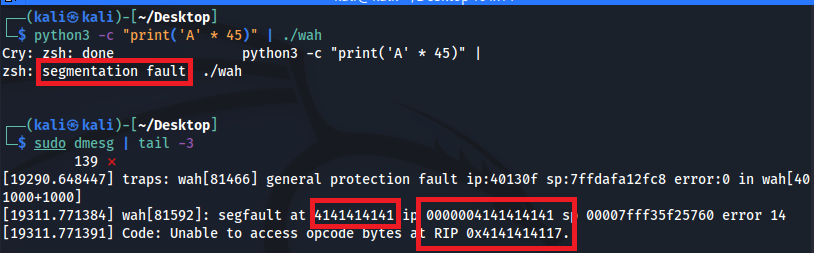
**Wah – Angstorm 2022**



We were provided with a 64 bit architecture ELF file with a buffer overflow vulnerability.  
It has no ASLR or Canary integer, stack is not executable therefore we conclude a shellcode could not be used to solve this challenge.



As you can see in the photo we flood the buffer with 'A' which has ASCII code 0x41

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

Using pwntools we we're able to understand that after 40 bytes we are writing directly to the program's return address, going thru the assembler code we noticed there's a function called flag.

We've used Ghidra to view the function and understand the code easily, as you can see in the photo it opens a flag.txt file and then print out its contents.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

At this point we had everything we need to solve the challenge, we wrote a script using pwntools  
to remotely connect to the server and send the payload that overrides the return address with flag function address, it doesn't require any parameters so the payload as follows:

תמונה שמכילה טקסט, מסך, צילום מסך

התיאור נוצר באופן אוטומטי