Heap overflow challenge

In this challenge I have created a hole using the strcpy which allows the buffferoverflow in the heap memory so the actual goal for them to find the flag is by making the address overflow and make another variable called safe var to take the value as overflowed which would allow the user to read the flag

in order to do so they first should get the address of the variables and difference between the address and then give input as per the requirement

but here is where a challenge is the address wont be known until the code is excecuted and run as I used malloc which dynamically allocates memory which will let them have the offset size and to solve this I have used GDB and made the program run until a point and have read the address of the heap and found the offset and it will work successfully

A screenshot of a computer screen

AI-generated content may be incorrect.A screenshot of a computer program

AI-generated content may be incorrect.