The encountered bugs in the buggy.c program are:

1. Segmentation fault (and stack smashing detected) when the length of string entered is greater than MAX\_ALLOWED value i.e. 8.This can be fixed by limiting the size of string that is parsed or accepted by scanf by modifying the scanf code as : scanf("%8s", str); .

2. Incorrect result of swapping of q and r. Using gdb as below the address and values stored at that address where observed (left panel) and changes were made in the program as shown below (right panel). This is due the order in which the parameters of the function are stored in the stack when the function call is made.

