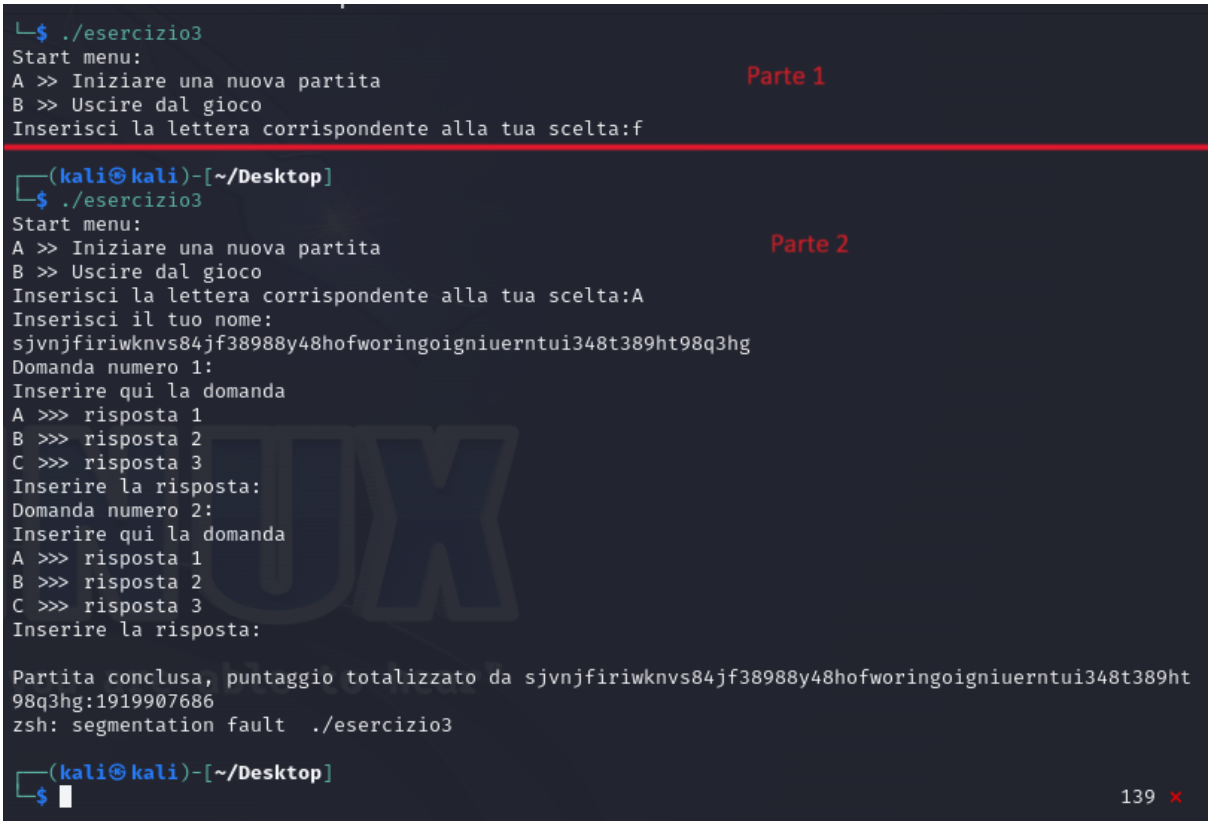

Il programma permette di giocare una partita ad un quiz con risposta multipla e consente di tenere il conto del punteggio del giocatore. Inizialmente abbiamo a disposizione la scelta tra una nuova partita o uscire dal gioco. Poi viene chiesto al giocatore di inserire il suo nome e successivamente parte il quiz.

Nella parte alta della foto possiamo vedere cosa succede se inseriamo una lettera diversa da A o B nella selezione del menù principale; il programma termina perché non è stata inserita, nel codice, un'istruzione che permette di gestire questa casistica.

La variabile del nome del giocatore viene dichiarata con uno spazio di massimo venti caratteri. Nella seconda parte della foto possiamo vedere cosa succede se il nome inserito dal giocatore eccede lo spazio fornito. Questa vulnerabilità viene definita buffer overflow, cioè una condizione di errore in cui, in un determinato buffer di una data dimensione, vengono scritti dati di dimensioni maggiori. I dati extra traboccano (overflow) e vanno a sovrascrivere le variabili adiacenti all'interno del programma, o il suo stesso stack. In conseguenza di ciò, a seconda di cosa è stato sovrascritto e con quali valori, il programma può dare risultati errati o imprevedibili, bloccarsi, o addirittura, bloccare il sistema. Un malintenzionato può inserire una serie di dati malevoli che, inviati per provocare il buffer overflow, gli consentano di prendere il controllo del programma e da questo dell'intero sistema.