Buffer OverFlow

Dato il codice “BOF.c”:

Con un nome utente di 7 caratteri (Edoardo) il programma non riporta alcun errore. Il programma continua a funzionare correttamente fino all’inserimento del diciassettesimo carattere. Dopo aver inserito il diciottesimo, tuttavia, il programma mi comunica l’errore: “zsh: segmentation fault .\BOF” .

Ho notato inoltre che se inserisco nome e cognome separati da uno spazio, l’output mi restituisce soltanto i caratteri che precedono lo spazio: questo avviene poiché la funzione “scanf” si interrompe al primo spazio digitato dall’utente.

Soluzione:

Per ovviare ai problemi sopracitati, ho modificato il codice, aumentando la dimensione del vettore a 30 (come da traccia), e sostituendo "scanf("%s, buffer")", con "fgets(buffer, sizeof(buffer), stdin)", dove:

• Stdin, usato argomento di fgets, indica a quest'ultimo di leggere l'input dalla tastiera;

• Fgets legge l'input digitato dalla tastiera e lo memorizza nell'array buffer;

• Sizeof(buffer), usato come argomento di fgets, indica a quest'ultimo che in questo caso deve leggere un massimo di 29 caratteri, in quanto l'ultimo è riservato al terminatore di stringa). Dopo la modifica è possibile inserire tranquillamente nome e cognome separati da uno spazio.