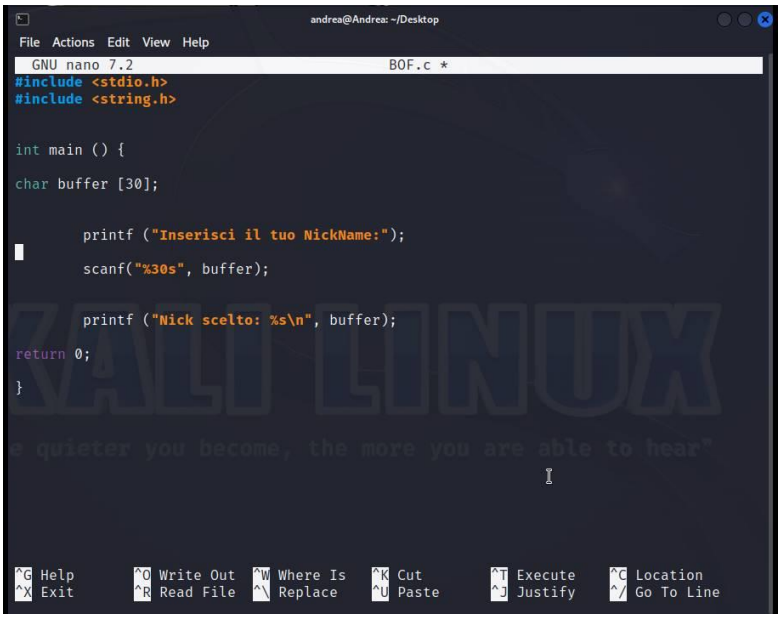
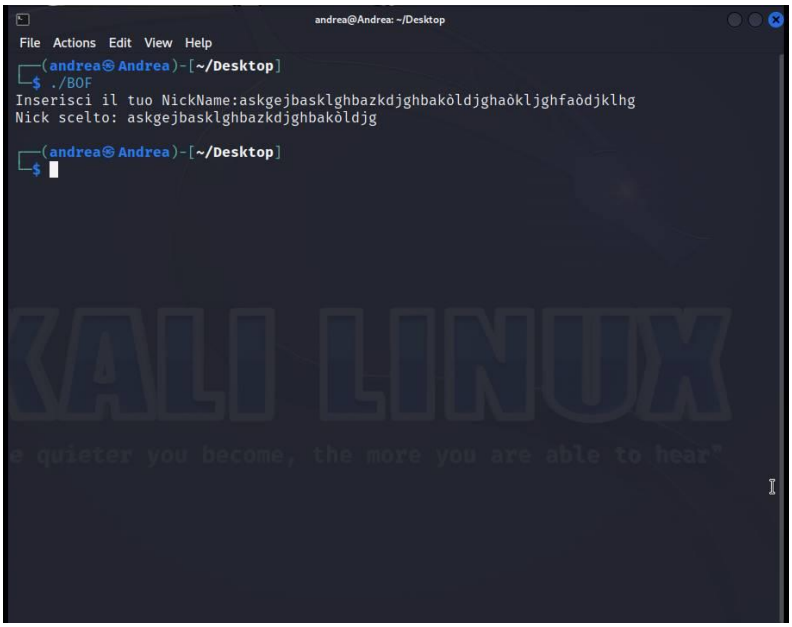
Esercizio 4 Settimana 7

Buffer Overflow

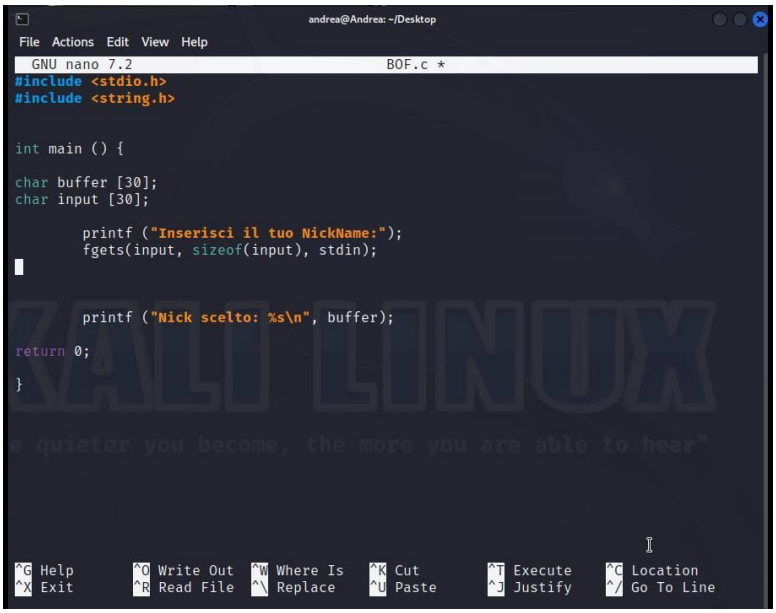
Il Buffer Overflow è una vulnerabilità che implica la mancanza di un controllo sull'input dell'utente.
Nel nostro caso il programma dato accetta una stringa di 10 caratteri in input, ma senza alcun controllo nel caso in cui l'utente inserisca una stringa più lunga: proprio in questo caso il programma tenterà di scrivere una parte di memoria a cui non ha accesso causando problemi e, in alcuni casi, lasciando la possibilità all'attaccante di iniettare puntatori o codici malevoli.
Per poter sanare il codice dobbiamo inserire dei parametri che vadano a limitare l'inserimento:



Una delle soluzioni più semplici sarebbe inserire *'%30s'* per indicare la formattazione a 30 caratteri che andrà a sostituire i caratteri mancanti con spazi vuoti e/o andrà a eliminare i caratteri superiori a 30:



In alternativa si può andare a modificare il codice inserendo una nuova variabile *'char input [30]'* e nuove funzioni come *'fgets'*: il primo inserisce un array di caratteri dato dall'utente e limitato, mentre il secondo legge l'input utente e lo memorizza nell'array di input con la lunghezza fissata (30).



Questi, infine, sono i due risultati con e senza modifiche: