

Il compito di oggi è rispondere a dei quesiti.

prima domanda.

Il programma è un gioco di quiz con un menu iniziale che offre due opzioni:

- 1. **Nuova partita (A)**: il giocatore inserisce il proprio nome e risponde a due domande con opzioni A, B o C. Il punteggio viene calcolato in base alle risposte corrette e viene stampato insieme al nome dell'utente alla fine della partita.
- 2. **Uscita (B)**: Se il giocatore sceglie di uscire, il programma mostra un messaggio di ringraziamento e termina.

Il ciclo **while** consente di continuare a giocare finché il giocatore sceglie di iniziare una nuova partita (opzione A). Il giocatore può tornare al menu iniziale dopo ogni partita. Le domande e le risposte sono ipotetiche e possono essere personalizzate. Il codice assume che il giocatore inserisca risposte valide e che il gioco si basi su risposte predefinite.

Seconda domanda

Se il giocatore inserisce una lettera diversa da 'A' o 'B', il programma potrebbe avere un comportamento imprevisto. Attualmente, il ciclo **while** continua ad eseguire il blocco di codice fintanto che la condizione **scelta == 'A'** è vera. Tuttavia, se il giocatore ha inserito una lettera diversa, la condizione rimane vera, portando a un comportamento indesiderato perché non ha inserito 'A'. Infatti il programma termina immediatamente senza dirci *Grazie per aver giocato alla prossima* (cosa che accade se inseriamo 'B').

Terza domanda

In questo caso se il giocatore inserisce un nome che ha più caratteri della dimensione dell'**array nome** dichiarato (20 caratteri), si verificherà un problema noto come "buffer overflow".

Il buffer overflow è una vulnerabilità di sicurezza che si verifica quando un programma scrive dati oltre i limiti di un buffer, cioè un'area di memoria assegnata per memorizzare dati temporanei come stringhe. Questa condizione può portare a comportamenti imprevedibili e, in alcuni casi, può essere sfruttata da attaccanti (Black hat) per compromettere l'integrità del programma e, potenzialmente, dell'intero sistema. Se poniamo l'esempio di inserire 22 caratteri, il buffer "**nome**" non può contenere l'intero nome inserito, e i caratteri extra verranno sovrascritti in aree di memoria adiacenti, potenzialmente causando comportamenti imprevedibili.