BUFFER OVERFLOW

Un "buffer overflow" è una vulnerabilità informatica che si verifica quando un programma, durante la scrittura di dati in un buffer di memoria, supera il limite del buffer, sovrascrivendo così dati nella memoria adiacente. Questa situazione può avere gravi conseguenze, in quanto un attaccante può sfruttare questa vulnerabilità per eseguire codice dannoso o manipolare il comportamento del programma in modi indesiderati.

Questo è il codice standard dato dall’esercizio

A computer screen with yellow text

Description automatically generated

Questo codice legge un nome inserito ma con un max di 30 caratteri, quindi se andiamo a scrivere più di 30 avremo questo output.

cA computer screen with white text

Description automatically generated

questo è l’output di errore perché abbiamo superato i 30 caratteri

la modifica del codice è stata la seguente

A screenshot of a computer screen

Description automatically generated

Abbiamo limitato l’opzione di inserimento di caratteri tramite lo scanf %29s

Cosi facendo se qualcuno inserirà una stringa superiore a 30 (29 perché si comincia a contare da 0)

Verranno stampati solo ii primi 30

A screenshot of a computer

Description automatically generated