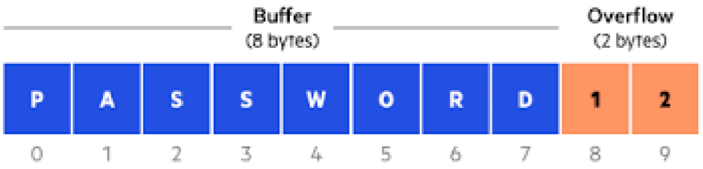
Universidad Rey Juan Carlos

Buffer overflow

Una de las vulnerabilidades más explotadas cuando se desarrollan programas en C es el desbordamiento de buffer o buffer overflow. Esta vulnerabilidad se basa en acceder a posiciones de memoria más allá de las reservadas para un determinado buffer (por ejemplo, un array).



Para evitar este tipo de ataques, vamos a programar un módulo para el compilador que nos avise de si existe el peligro de desbordamiento de buffer en función de un tamaño reservado y una entrada dadas.

Entrada

La entrada contendrá un número $\boldsymbol{N}$ que indicará el tamaño reservado para un buffer. A continuación, aparecerá una serie de datos numéricos que se introducirían en el buffer por parte del usuario durante el flujo de ejecución de la aplicación. La entrada finaliza cuando el usuario introduce un número negativo que no cuenta como elemento de entrada.

Salida

Por cada caso de prueba, se imprimirá "BUFFER OVERFLOW" en caso de que la cantidad de datos introducidos sea mayor al tamaño reservado para el buffer o "OK" en caso contrario.

Ejemplo de entrada	**Ejemplo de salida**
3 1 2 3 -1	OK
Ejemplo de entrada	**Ejemplo de salida**
3 1 2 3 4 -1	BUFFER OVERFLOW

Límites

- $0 \leq N \leq 2000$
- $0 \leq N_i \leq 10000$