Daniel Coffey

2-3 Activity: Buffer Overflow Coding

CS 405 Secure Coding

01/30/21

For this assignment, the user was able to type more than 20 characters and overflow the buffer, resulting in account\_number being replaced, even though it is a constant and the compiler buffer checks are on. I was tasked with modifying the method to prevent buffer overflow without changing the account\_order variable and its position in the declaration. It must always be directly before the variable used for input. For this, I modified the existing method to limit the size of variable input to prevent buffer overflow. I used setw, with an argument of 20 for the user input to accomplish this. Setw sets the field width to be used on output operations. Shape

Description automatically generated