Module Two Buffer Overflow

Jordan Whitney

CS-405 Secure Coding

Professor: Alan Spencer

7/11/2025

The goal for this code is to prevent a buffer overflow that could overwrite the nearby “account\_number” variable in memory when the user inputs more than 19 characters. I replaced “std::cin >> user\_input” with “std::cin.get(user\_input, sizeof(user\_input))” allowing to safely read at most 19 characters and adds a null terminator. I checked for extra characters by using “std::cin.peek() != ‘\n’” to detect input that exceeded the buffer size, while using “std::xin.ignore()” to discard those remaining characters in the input buffer, ensuring a clean state for further input if needed. This works because the approach avoids overflow constraining the input to the array size, using “sizeof(user\_input)” as the limit.

A screenshot of a computer

AI-generated content may be incorrect.