John Munguia

CS 499 – Module 2 – Buffer Overflow Activity

July 13, 2025

In this buffer overflow activity, I identified that the vulnerability was caused by allowing the user to input more characters than the fixed char user\_input[20] buffer could handle. If the input exceeded the buffer, it would overwrite adjacent memory, including the account\_number variable declared before it.

To fix this, I replaced the unsafe cin >> with std::cin.get(user\_input, sizeof(user\_input)), which limits input to 19 characters plus a null terminator. I also added a check with std::cin.fail() to detect if the input was too long and then cleared the error state and discarded the remaining input. This fix prevents buffer overflow and ensures the account\_number remains unchanged. The program also alerts the user if they exceed the allowed input length, demonstrating both input validation and secure defensive coding practices.

Screenshot of output using less than 20 characters:

A screenshot of a computer

AI-generated content may be incorrect.

Screenshot of output using more than 19 characters:

A screenshot of a computer

AI-generated content may be incorrect.