James Soto

7/4/2023

CS-405 Secure Coding

2-3 Activity: Buffer Overflow

To fix the buffer overflow issue in the code snippet I had to limit the size of the user's input to the size of the buffer it is being stored in. I achieved this by using the `std::cin.width(sizeof(user\_input));` before the `std::cin >> user\_input;` operation. This line ensures that the maximum number of characters read from the input is limited to the size of `user\_input`, thereby preventing an overflow. It truncates any input longer than the buffer size. For this assignment I had to use Clion on Mac to get the code to work properly since Visual Studio does not work with C++. The screenshots included below show what happens when an overflow occurs and what happens when the code is protected from an buffer overflow.

A screenshot of a computer program

Description automatically generated with medium confidence

A screenshot of a computer program

Description automatically generated with medium confidence