**Module Two Buffer Overflow**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

March 17, 2024

**Module Two Buffer Overflow**

**Summary:**

Originally the file used *std::cin* to read input with no bounds checking which could lead to overwriting the password. The change implemented was to instead utilize *getline* and specify the number of characters to read (Cplusplus.com, n.d.). This method will ensure that a buffer overflow does not happen as it stops reading at user\_input – 1 characters leaving space for the null terminator. As shown in several test cases below, empty strings, very long nonsense input, as well as python injections are unsuccessful in unexpectedly modifying the account number.

A screenshot of a computer program

Description automatically generated

**References**

Cplusplus.com. (n.d.). *istream::getline – C++ Reference.* <https://cplusplus.com/reference/istream/istream/getline/>