# **CS 405 2-3 Activity: Buffer Overflow Coding**

# **Austin Donaubauer**

# **Southern New Hampshire University**

# **CS-405 Secure Coding**

# **Wasim Alim**

# **July 13th, 2025**

# **CS 405 2-3 Activity: Buffer Overflow Coding**

The buffer overflow coding activity deals with detecting a buffer overflow of a variable. To detect an overflow attempt, I because by getting the characters and creating a string from the user input. Then I could test if the string length exceeds 20 because that is the limit. If it is longer than 20 then I output a Buffer Overflow error message to the user and stop the program. If it’s not longer than 20 then I output the account number as needed.

I have an issue with my program due to possible user entries that have spaces. But for this assignment the tests didn’t have spaces in the input so I assume I could ignore spaces.

Detecting and preventing a buffer overflow attack is important because important information could be displayed to a malicious user which is the reason they performed the attack in the first place to get that information. Securely coding for this prevents this attack from being successful.

Screenshot of my output from the program:

A computer screen with a message

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.