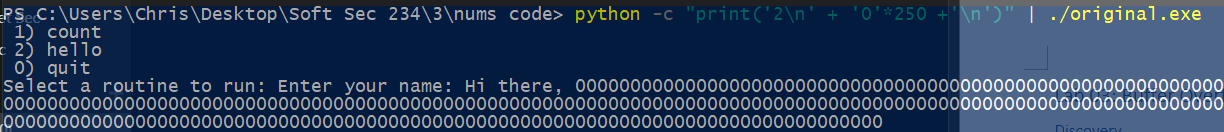
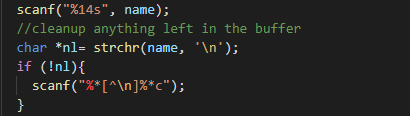
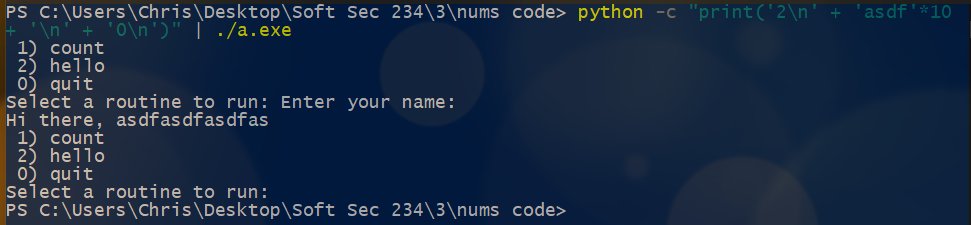
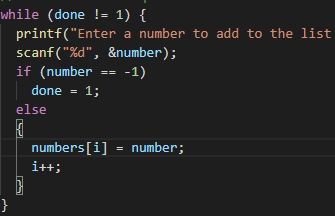
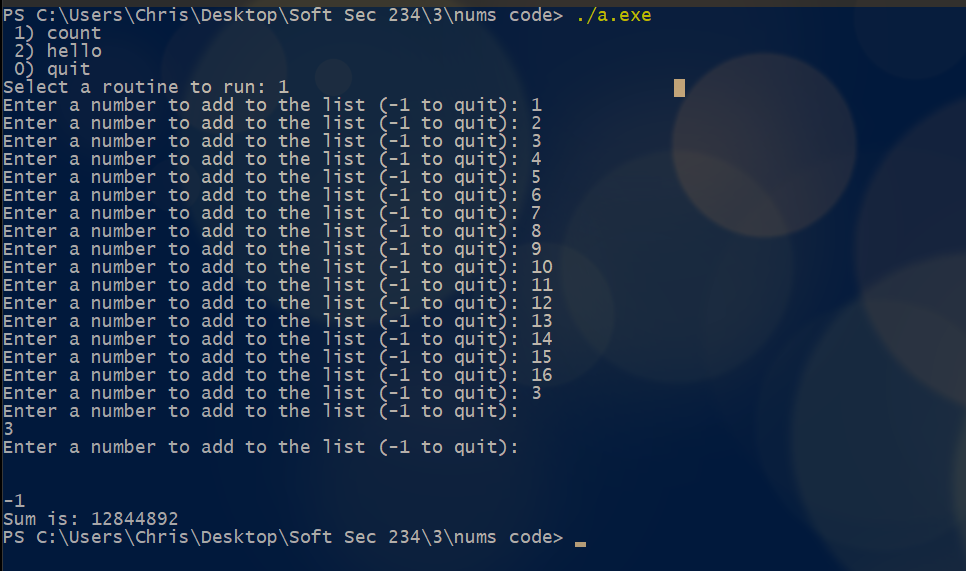
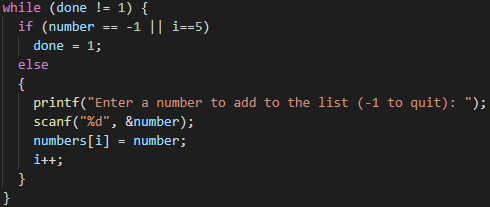
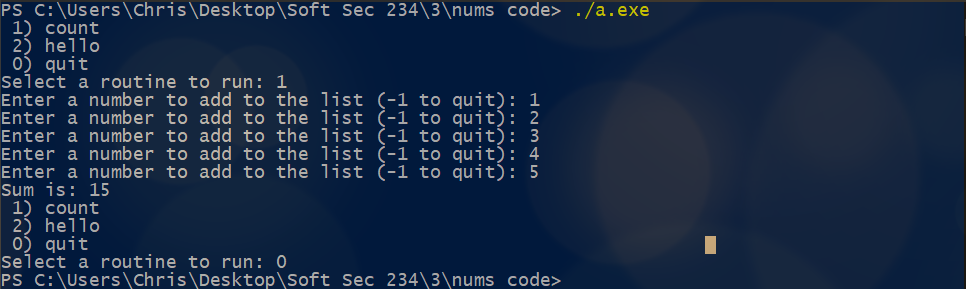
Lab 03: Buffer Overflows

# Discovery

This program has several flaws including some which could result in overflow of a memory buffer. Identify changes you’d make and why.

1. The initial scanf %d in main leaves a newline character which meddles with later scans. There is a getchar() to catch it in the hello() function but it should be in main, so I cut and dropped it into main after the scanf() it is cleaning up.  
   
2. Hello() uses a gets() call to fetch the user’s input string, and doesn’t perform checks on the 15 character boundary  
     
   I fix this by explicating the buffer size - changing gets() to scanf(), with a 14 character limit (+ the newline) on the scan, followed by a stdin flush.  
     
   
3. The loop in count() does not perform any checks on the boundaries of the int array.  
     
   I add a boundary check to the control flow logic, and then move the prompt/scan into the else statement to avoid confusion of inputting that gets dropped when I reaches the 5th index.  
     
   we could probably change it to a do{…}while(number==1 || i==5) loop as well, which would eliminate the need for the ‘done’ variable, and the nested control flow, to improve readability, but this works for now.  
   

# Remediation

After confirming the vulnerability, use your knowledge and available resources to modify the source to follow best practices and avoid integer overflows.

1. Modify the source code to gracefully handle overflows and remove any other flaws.
   1. Document your resulting source code with a screenshot

Included the screenshots and elaborations on the protections used above – wasn’t aware this was a separate question – it seemed right in line with the other one

1. Test your changes
   1. Are your attempts at entering further oversized input successful? Why or why not?

Same thing. As above

* 1. Provide screenshots documenting proper handling of invalid / oversized input.

Also included above

I’ll be sure to read ahead next time, to make sure my answers aren’t organized out of order from the answer sheet. Please forgive me this time .



# Scoring

The rubric will be published at scoring time. Each portion of the assignment has the following points assigned.

|  |  |
| --- | --- |
| **Section Points** | |
| **1** | 6 |
| **2** | 2 |
| **3** | 6 |
| **4** | 6 |
| **Total** | **20** |