Ashton_Wise_adw0082

1. Describe the buffer overflow problem. (5 points)

Buffer overflow is a common vulnerability that occurs when a program tries to write data into a buffer, but the amount of data being written exceeds the buffer's capacity. This can lead to a variety of security issues such as crashing the program, allowing an attacker to execute arbitrary code or bypass security measures, and accessing or modifying sensitive information.

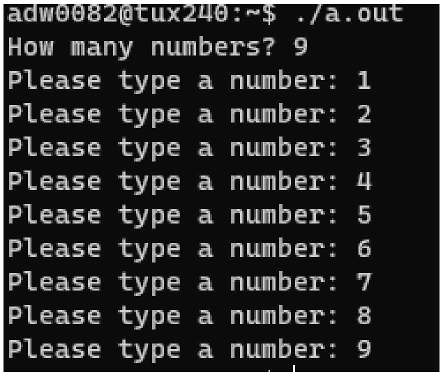
2. How could you prevent a buffer overflow from occurring in your program? (5 points)

checking the size of the input data and the buffer's size and making sure that the data being copied does not exceed the buffer's capacity.

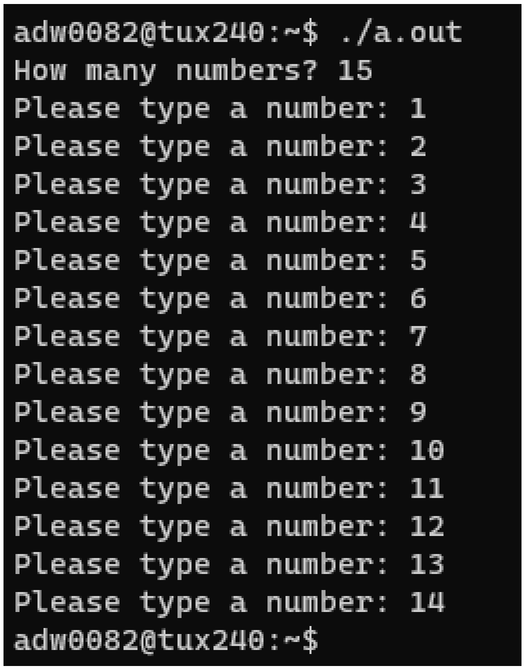
3. A sample code is presented in a picture format (Above). Please create a secure_coding.cpp

and type code with your hands. Compile and Run in AU server(Linux environment). Present

your results with a screenshot. (5 points)



```
adw0082@tux240:~$ ./a.out
How many numbers? 9
Please type a number: 1
Please type a number: 2
Please type a number: 3
Please type a number: 4
Please type a number: 5
Please type a number: 6
Please type a number: 7
Please type a number: 8
Please type a number: 9
```



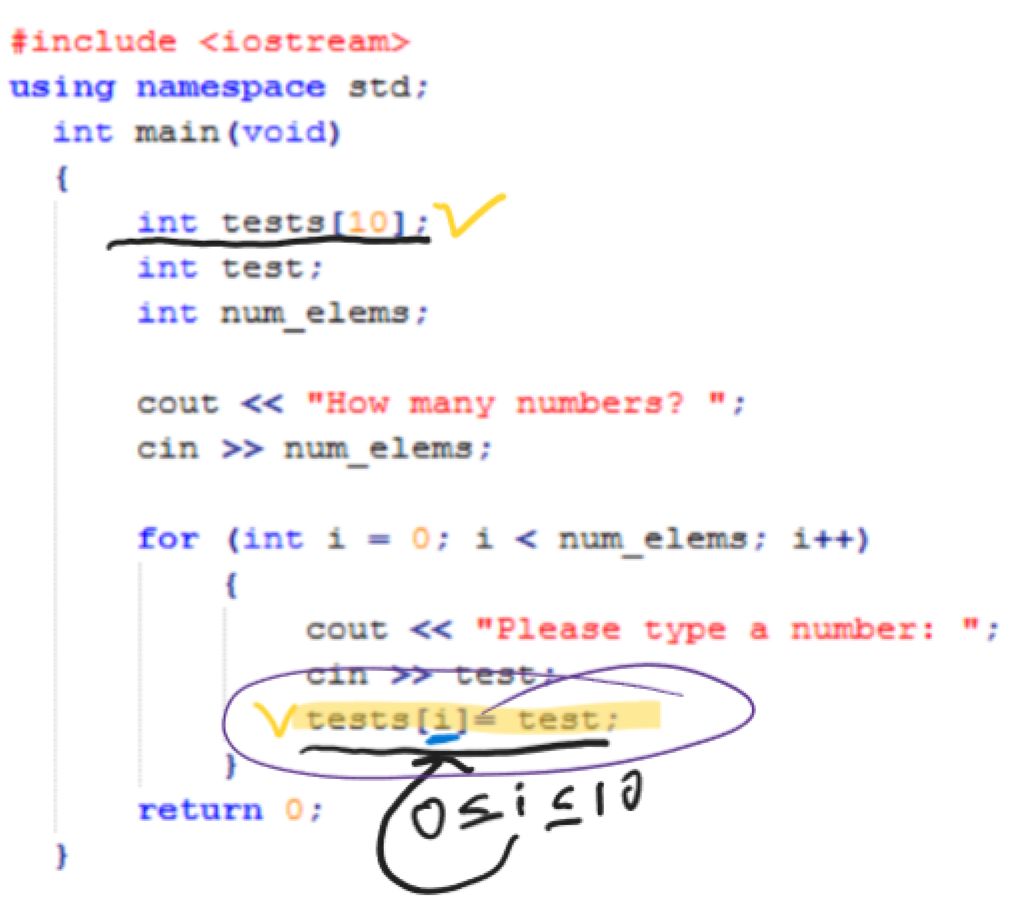
```
adw0082@tux240:~$ ./a.out
How many numbers? 15
Please type a number: 1
Please type a number: 2
Please type a number: 3
Please type a number: 4
Please type a number: 5
Please type a number: 6
Please type a number: 7
Please type a number: 8
Please type a number: 9
Please type a number: 10
Please type a number: 11
Please type a number: 12
Please type a number: 13
Please type a number: 14
adw0082@tux240:~$
```

4. What happened? (5 points) Why? (5 points) Fix the error and run again. (5 points)

There was an overflow C++ doesn’t throw an error for that.

There was an overflow because you tried to store more in the array than the allocated space

5. Complete the security checklist(below) for this program. (30 points. 5 points each)



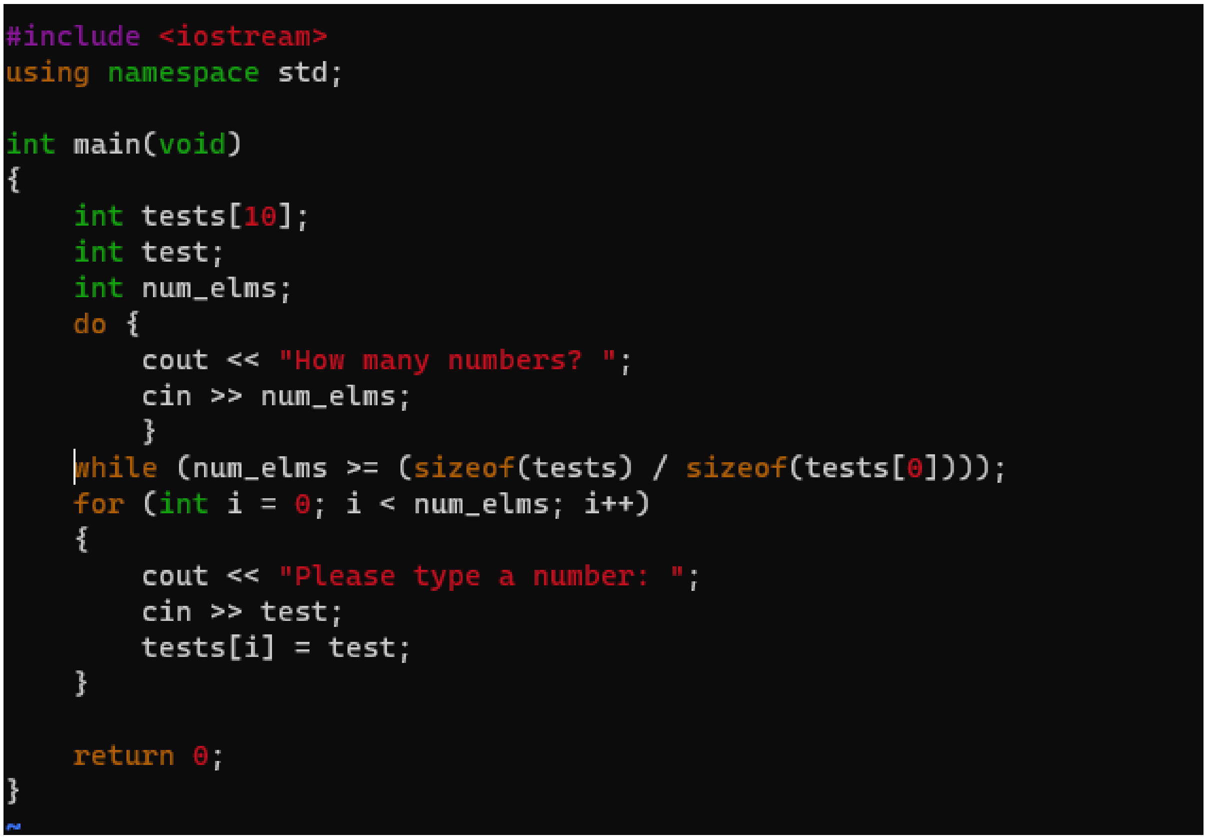
```
#include <iostream>
using namespace std;
  int main(void)
  {
      int tests[10];
      int test;
      int num_elems;

      cout << "How many numbers? ";
      cin >> num_elems;

      for (int i = 0; i < num_elems; i++)
      {
          cout << "Please type a number: ";
          cin >> test;
          tests[i]= test;
      }
      return 0;
  }
```

6. The V indicates where the potential buffer could occur. How could we prevent this? (10

points)

by adding a do-while loop that keeps asking for the input “num_elems” until it is less that or equal to the size of the tests array

7. Revise the program to eliminate potential buffer overflow problems. (10 points)



```cpp
#include <iostream>
using namespace std;

int main(void)
{
    int tests[10];
    int test;
    int num_elms;
    do {
        cout << "How many numbers? ";
        cin >> num_elms;
        }
    while (num_elms >= (sizeof(tests) / sizeof(tests[0])));
    for (int i = 0; i < num_elms; i++)
    {
        cout << "Please type a number: ";
        cin >> test;
        tests[i] = test;
    }

    return 0;
}
~
```