**Bài tập thực hành 1. Lỗi tràn bộ đệm**

1. **Mục tiêu:**

* Giúp sinh viên hiểu rõ hơn về vấn đề tràn bộ đệm;
* Rèn luyện kỹ năng lập trình, tư duy code tránh được lỗi tràn bộ đệm.

1. **Nội dung thực hành:**
2. ***Program 1.***

Cho đoạn code sau:

#include

using namespace std;

const int inputSize=10;

string inputString();

void copyStrs(string, char[] );

void subStrs(char[],char[]);

void getStrs(int,int,char[],char[]);

int main()

{

char strs[inputSize];

char sub[inputSize];

string s1 = inputString();

copyStrs(s1,strs);

subStrs(strs,sub);

cout << "sub string: " << sub << endl;

return 0;

}

string inputString()

{

cout << "Type a string: ";

string s;

getline(cin,s);

return s;

}

void copyStrs(string s, char strs[])

{

int i=0;

for (i = 0; i < s.length(); i++)

strs[i] = s.at(i);

strs[i] ='\0';

}

void subStrs(char strs[],char newStrs[])

{

int start;

int end;

cout << "Starting point: ";

cin >> start;

cout << "Ending point: ";

cin >> end;

getStrs(start,end,strs,newStrs);

}

void getStrs(int start,int end,char strs[],char newStrs[])

{

int len = end-start+1;

int i=0;

for (i=0; i < len - 1; i++)

newStrs[i] = strs[start + i];

newStrs[i] = '\0';

}

Yêu cầu:

* Gõ, biên dịch và chạy chương trình trên.
* Liệt kê các lỗi tràn bộ đệm tiềm ẩn trong chương trình trên.
* Chỉ ra ví dụ đầu vào có thể gây ra lỗi tràn bộ đệm.
* Trình bày giải pháp có thể sử dụng để loại bỏ lỗ hổng tràn bộ đệm tiềm ẩn trong chương trình.
* Sửa lại chương trình để loại bỏ các vấn đề tràn bộ đệm tiềm ẩn (sử dụng cấp phát bộ nhớ động).

1. ***Program 2***

Viết một hàm cho phép sao chép một dãy tùy ý của một mảng các số nguyên sang mảng khác. Hàm sao chép này có 7 tham số đầu vào:

* Mảng nguồn các số nguyên.
* Chiều dài mảng nguồn.
* Điểm bắt đầu sao chép trong mảng nguồn.
* Điểm kết thúc trong mảng nguồn.
* Mảng đích các số nguyên.
* Chiều dài của mảng đích.
* Vị trí bắt đầu thêm vào các dữ liệu trong mảng đích.

*Để tránh lỗi tràn bộ đệm:*

* Chỉ sao chép những giá trị tồn tại trong mảng nguồn đến các vị trí sẵn có trong bản đích.
* Nếu không đủ không gian trong mảng đích, chỉ copy không gian đích đến khi không gian trống đã đầy.
* Hàm trả về số giá trị được sao chép.