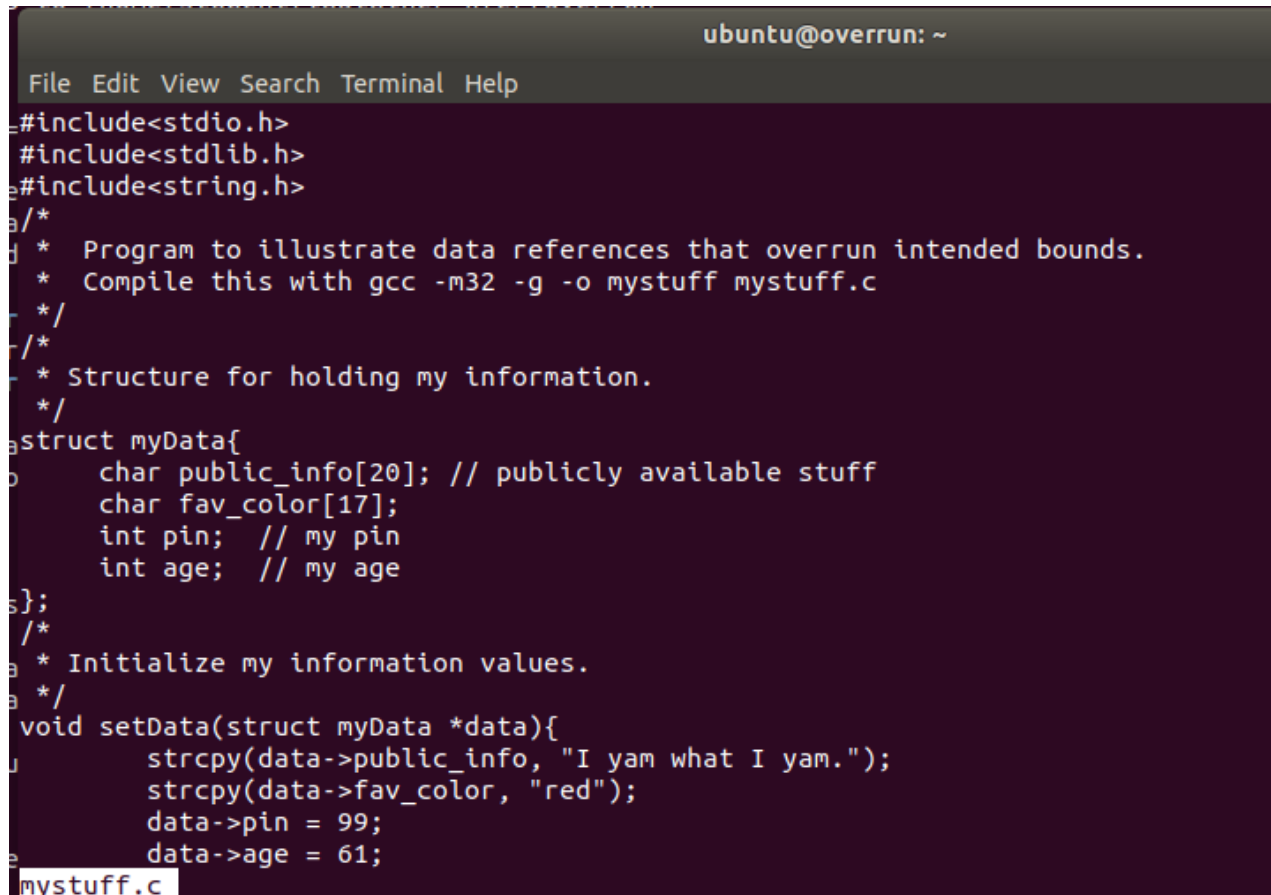


1. BÀI THỰC HÀNH: OVERRUN

Tại terminal mở ra, hãy xem chương trình mystuff.c. Sử dụng vi hoặc nano, hoặc chỉ nhập

less mystuff.c



```
ubuntu@overrun: ~
File Edit View Search Terminal Help
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
/*
 * Program to illustrate data references that overrun intended bounds.
 * Compile this with gcc -m32 -g -o mystuff mystuff.c
 */
/*
 * Structure for holding my information.
 */
struct myData{
    char public_info[20]; // publicly available stuff
    char fav_color[17];
    int pin; // my pin
    int age; // my age
};
/*
 * Initialize my information values.
 */
void setData(struct myData *data){
    strcpy(data->public_info, "I yam what I yam.");
    strcpy(data->fav_color, "red");
    data->pin = 99;
    data->age = 61;
}
mystuff.c
```

Nhìn vào struct myData. Trong chương trình khai báo biến my_data là một struct kiểu myData. Lưu ý rằng mảng ký tự public_info có 20 phần tử. Ta có thể tham chiếu đến các phần tử của mảng bằng cách sử dụng chỉ mục. Ví dụ: my_data.public_info[4] đề cập đến ký tự thứ 5 trong mảng và my_data.public_info[19] đề cập đến ký tự cuối cùng trong mảng.

-> Sau khi chương trình khởi tạo biến my_data kiểu struct, nó sẽ hiển thị địa chỉ của phần bắt đầu trường public_data và trường pin, đồng thời nó hiển thị các giá trị bộ nhớ của các trường đó.

Sử dụng lệnh này để biên dịch chương trình:

gcc -m32 -g -o mystuff mystuff.c

Lưu ý rằng -m32 tạo ra một mã nhị phân 32 bit và -g sẽ chứa các ký hiệu trong file nhị phân, cho phép khám phá quá trình thực thi của chương trình bằng cách sử dụng gdb.

Chạy chương trình:

./mystuff