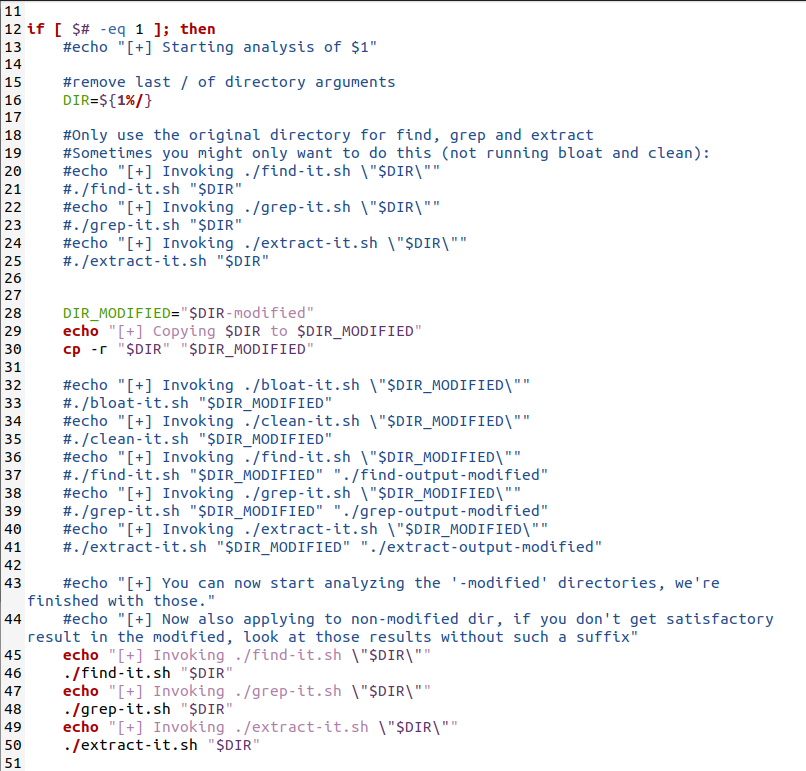
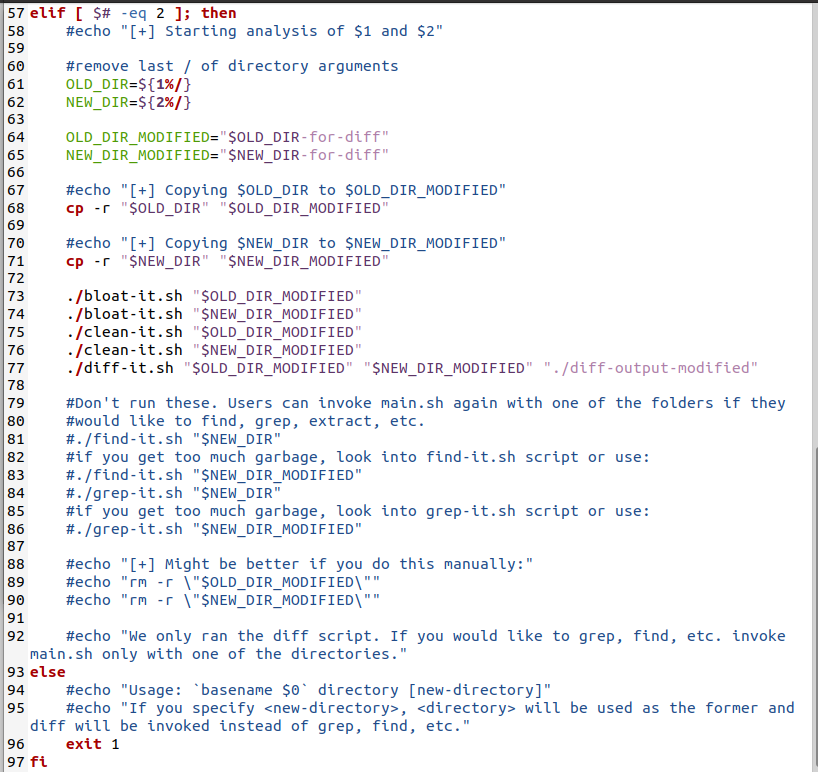
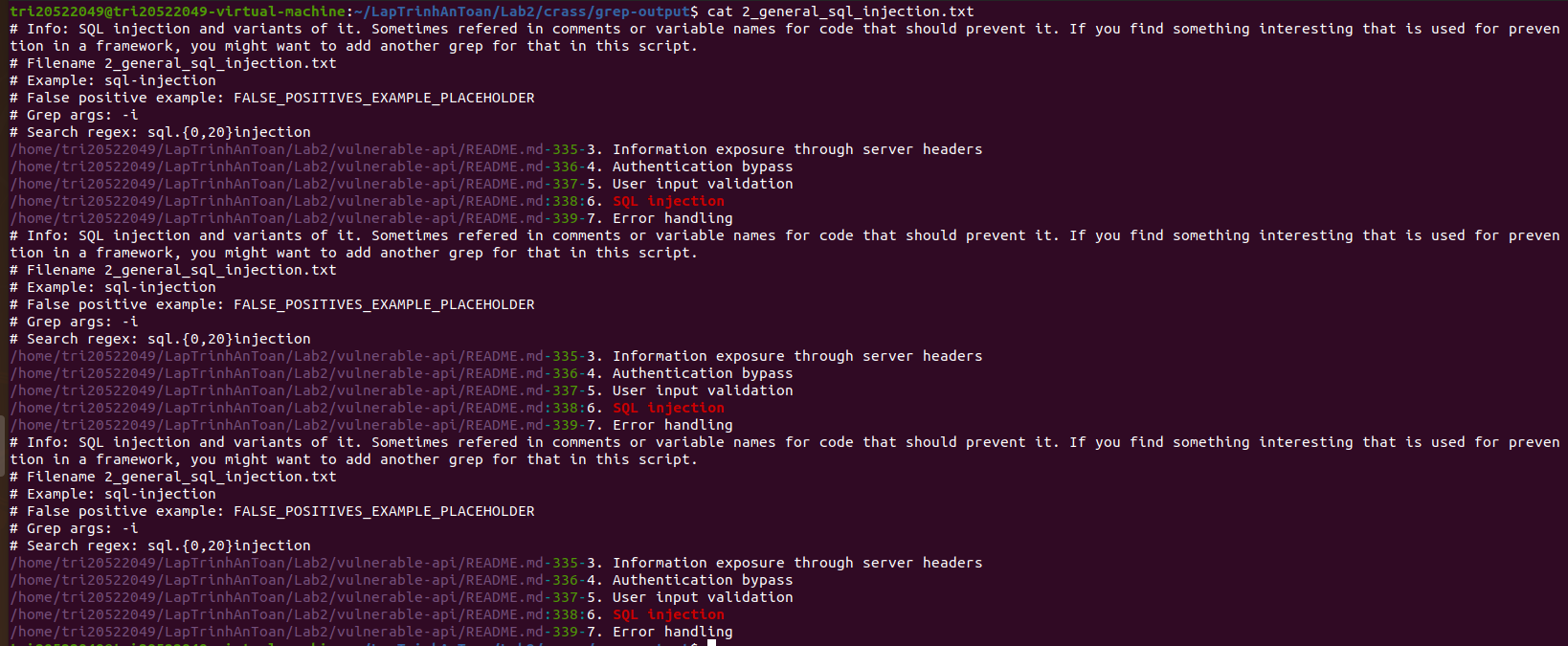
**Yêu cầu 1.1:** Sinh viên chỉnh sửa file **main.sh** trong thư mục của CRASS để đảm  
bảo ***chỉ*** chạy các chức năng bên dưới khi quét **1 thư mục mã nguồn**





**Yêu cầu 1.2:** Dựa vào kết quả sau khi quét, sinh viên tìm và giải thích ngắn gọn **01**nguy cơ bảo mật có thể thấy trong mã nguồn của ứng dụng.

Sau khi quét ta thấy được cái lỗi bảo mật SQL injection

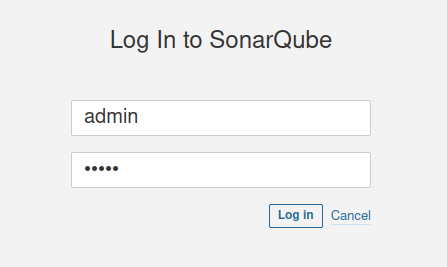
SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng.

Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database.

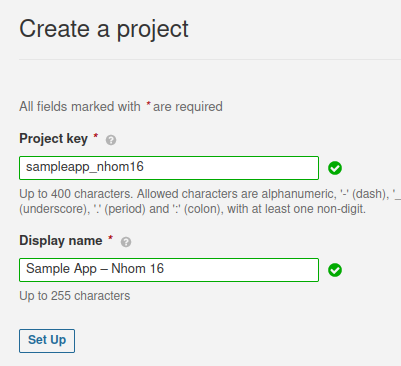
SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

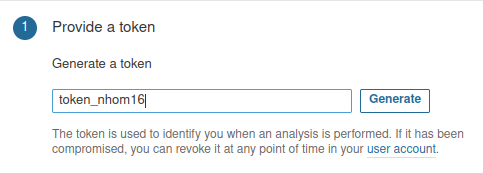
**Yêu cầu 1.3:** Sinh viên sử dụng SonarQuabe để quét mã nguồn của ứng dụng  
Sample App đã chạy ở Lab 1. Trình bày kết quả quét mã nguồn.

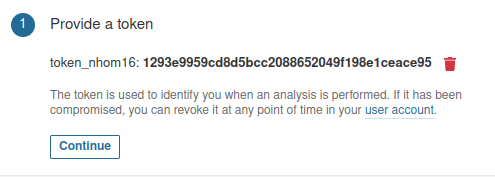
Đầu tiên ta tải sonarqube theo hướng dẫn và khởi chạy sonarqube ở localhost với port mong muốn, sau đó ta vô locolhost với port đã chạy trước đó đăng nhập với mật khẩu mặc định là admin/admin

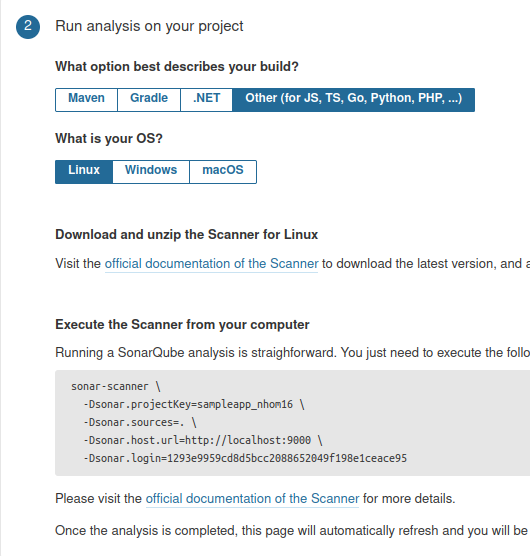


Sau khi ta đã đăng nhập vào, ta tạo project để kiểm thử 1 ứng dụng nào đó (trong trường hợp này là sample app)

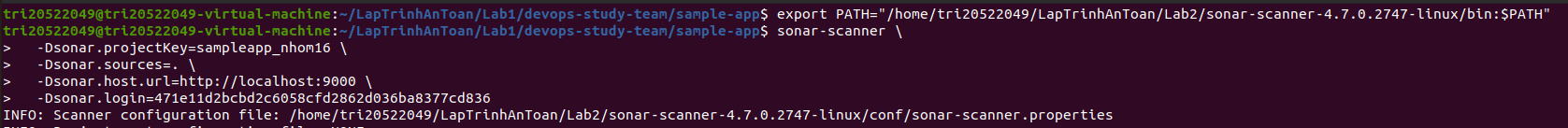




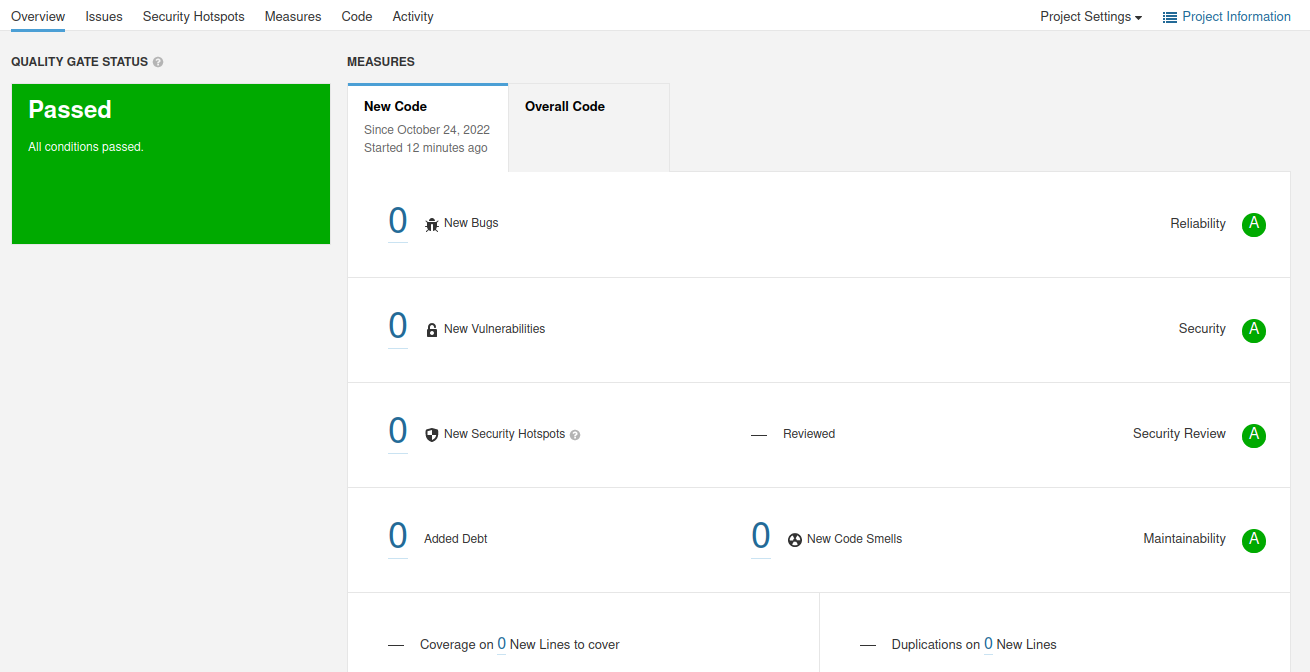


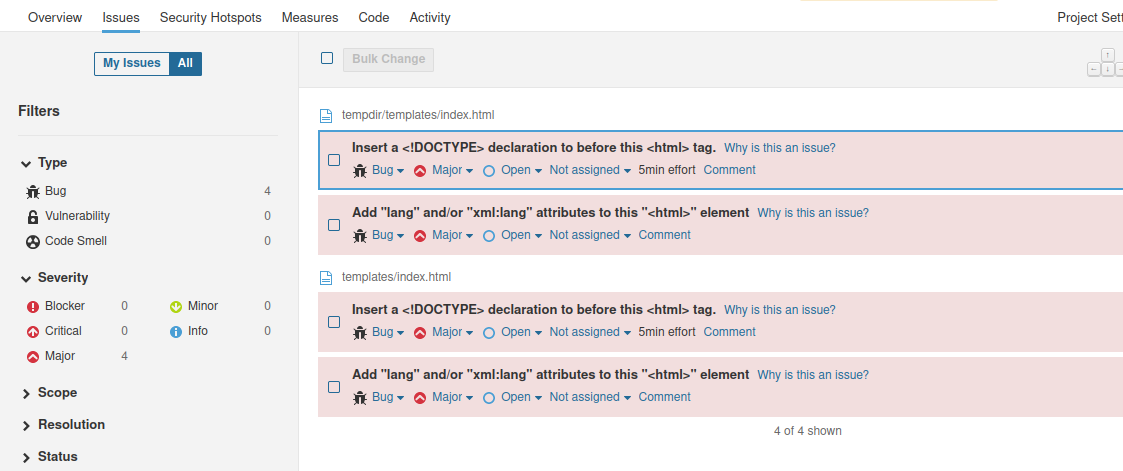


Khi đã làm xong các bước trên, ta chạy lệnh dưới ở thư mục của app cần kiểm thử

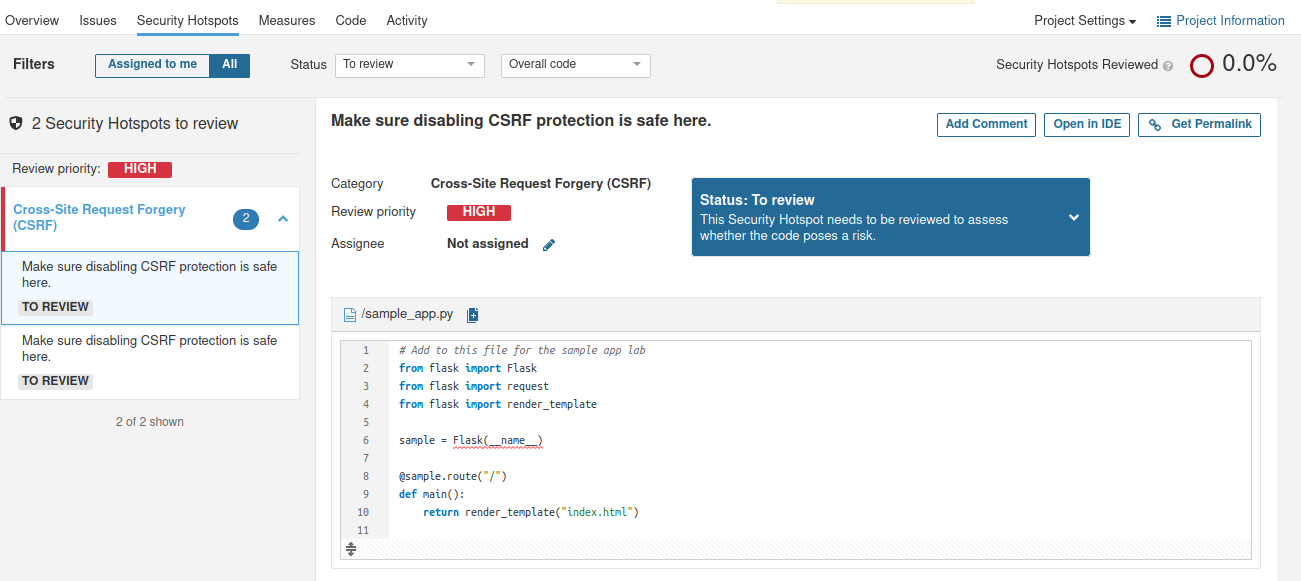


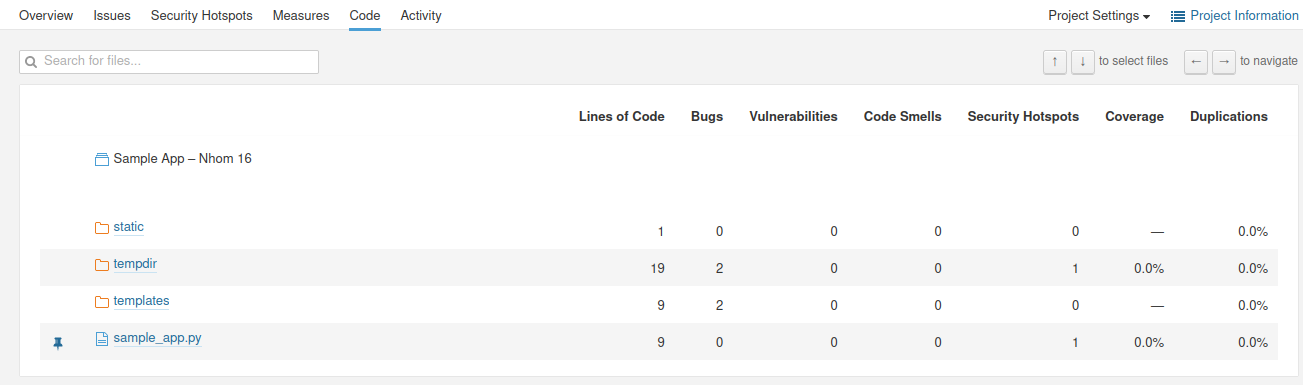
Sau khi chạy thử xong, web vào giao diện này cho ta thấy các thông tin của lần kiểm thử này có những lỗi gì và nhiều thức khác





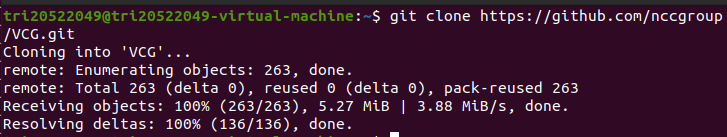
Như hình dưới, ta có thể thấy web thông báo cho ta lỗi CSRF nếu vẫn để như thế



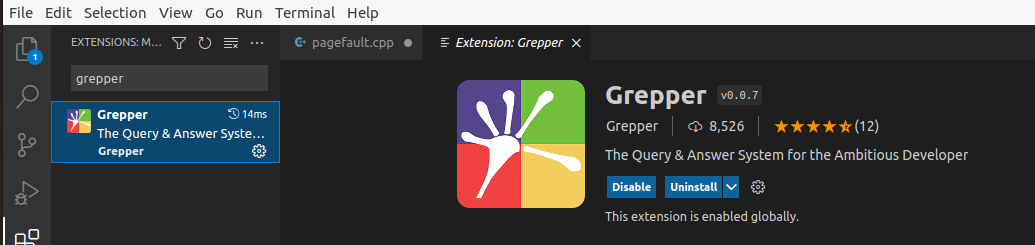


Yêu cầu 1.4: Sinh viên tự tìm hiểu, cài đặt và đưa ra 1 ví dụ quét mã nguồn với VCG

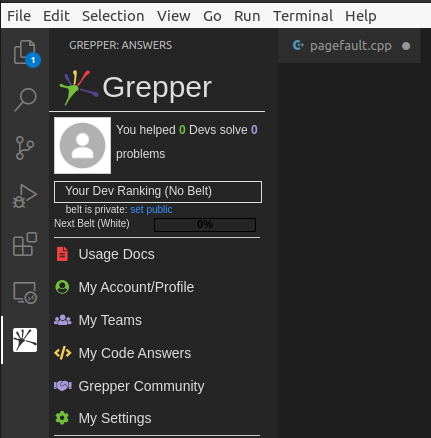
Đầu tiên ta tải VCG về



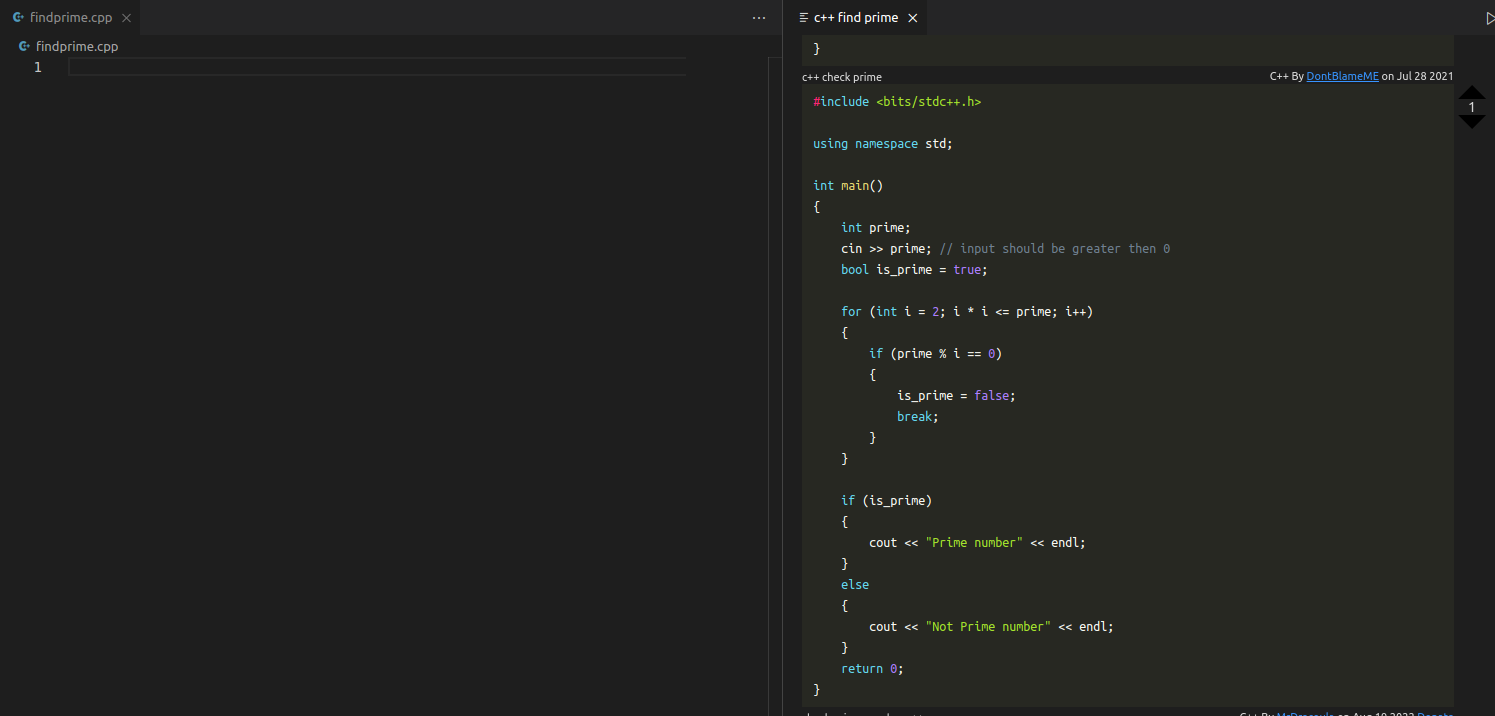
Tiếp theo ta vào công vụ visual studio để cài tiện ịch “Grepper”



Khi đã tải về ta cần đăng nhập vào với vài thao tác tạo tài khoản đơn giảns



Như ví dụ dưới đây ta cần code ra 1 chương trình kiểm tra số nguyên tố thì ta có thể nhờ công cụ vừa tải về để tìm mã nguồn có sẵn 1 cách nhanh chóng mà không tốn nhiều thời gian



Ta cũng có thể đóng góp cho cộng đồng bằng cách thêm vào code do chính bản thân viết ra bằng cách tô đen code cần đóng góp rồi bấm vào thêm câu trả lời cho tiện ích (Add Grepper Answer)

