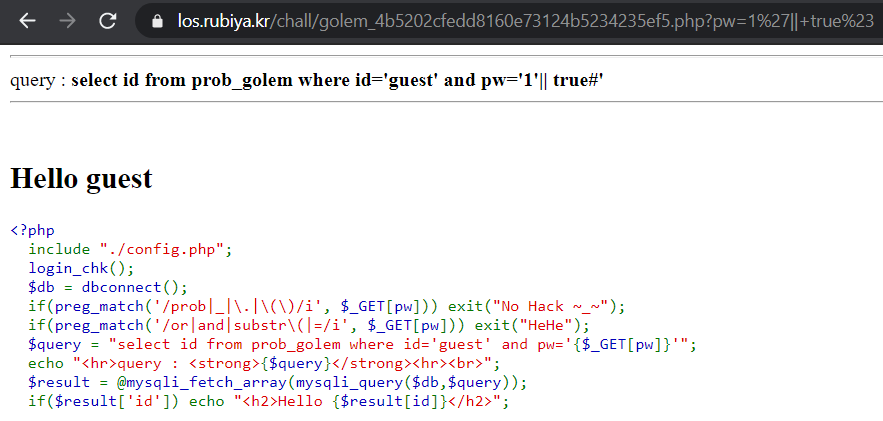


Xem code để biết cách hoạt động của filter. Em thấy được không thể dùng or, and, substr. Tìm hiểu thì có thể thay thế or bằng ||, and bằng && và substr() bằng mid()

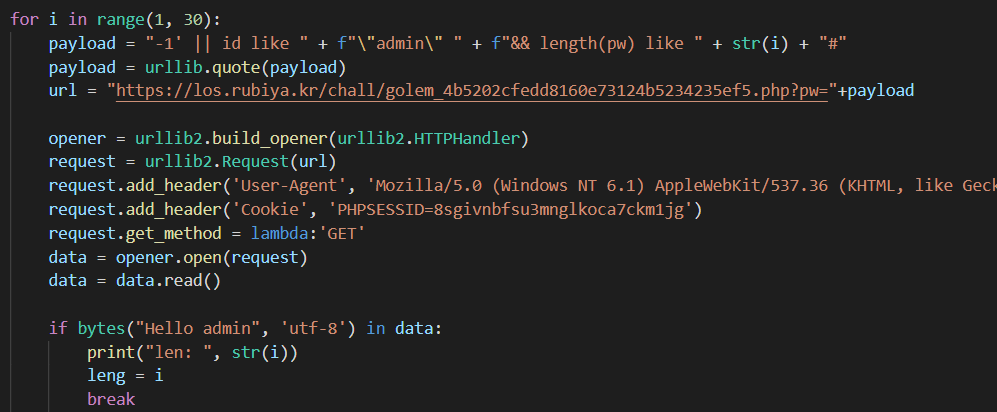
Đầu tiên cần tạo một query hợp lệ. Sau khi thử các cách thì query có dạng: ‘||+true%23. Trong đó %23 là dấu # để comment phần sau của query. Sử dụng || thay cho or.



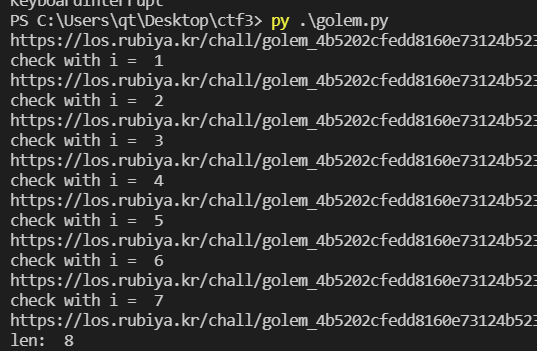
Tiếp theo cần đổi id thành admin bằng cách thêm || id like “admin”. Dùng like thay cho = vì = đã bị block



Như bài trước đây là kiểu blind sql trong đó cần tìm ra pw. Mỗi lần query thành công sẽ hiện ra Hello admin.



Đoạn code trên kiểm tra độ dài của pw.



Chạy code và được độ dài của pw là 8.



Đoạn code trên brute force từng kí tự của pw. Vì hàm substring() đã bị block nên sẽ dùng hàm mid() thay thế.



Chạy code ta dò ra được pw như trên hình



Nhập pw vào và hoàn thành challenge.