

Bad username or bad password !

Trang web cho phép nhập vào username và password như hình trên.

You are connected as : test

Tìm hiểu về noSQL ta có thể thêm toán tử ở sau parameter như hình trên và dùng nó để exploit db.

Ví dụ như query trên là chọn ra username khác admin và password khác admin.

Kết quả login với user là test.

You are connected as : admin

Thử tương tự với username = test. Ta login vào với username là admin.

Phân tích yêu cầu bài là có 1 user nữa bị ẩn và cần login với user đó.

You are connected as : flag{nosql_no_secret_4_you}

Ta có thể dùng regex để lọc ra 2 trường hợp trên. Ý nghĩa của câu query trên hình là username khác admin và test.

Kết quả thu được flag như hình và hoàn thành challenge.