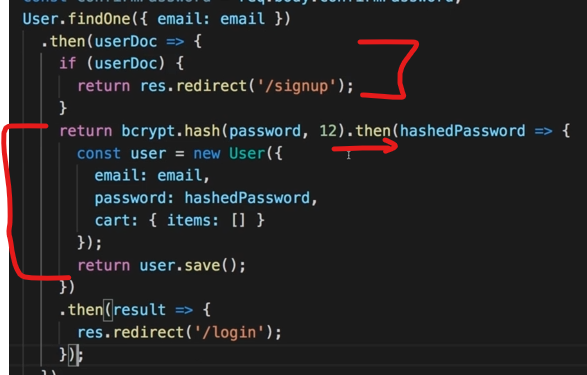
Sử dụng Bcrypt cho password

Npm install bcryptjs

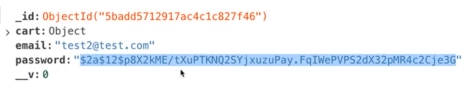


Và trước khi register thì encrypt nó

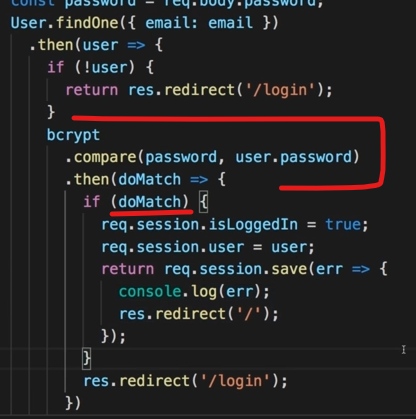


Bcrypt.hash(pwd, salt) : salt càng cao thì round càng nhiều 🡪 ecrypt lâu 🡪 bảo mật hơn

Result



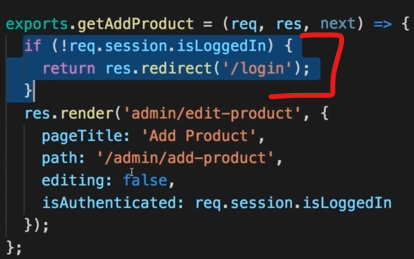
# Sign In Function



Compare trả về promise nhưng err catch không phải khi không match mà là khi lỗi xảy ra

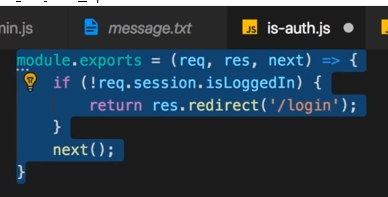
Biến “doMatch” mới là giá trị so sánh

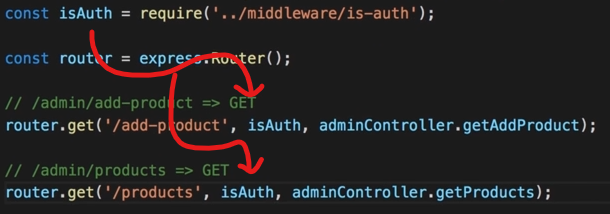
# Route Protection



Xét đã login chưa ở mỗi route

Hoặc sử dụng Middleware(recommended)





Middleware sẽ chạy từ trái sang phải 🡪 và xét duyệt

CSRF

Npm install csurf



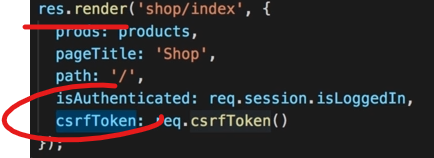


 đặt csrf sau session vì nó sẽ dùng session

Cách hoạt động :

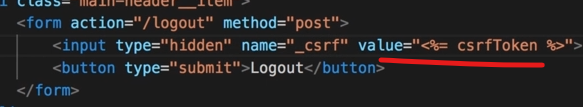
1. ở ^~ **nonGet(POST / PUT / PATCH / DELETE)** request : middleware đều check csrf token ở **requestBody**

Set CSRF token ở view



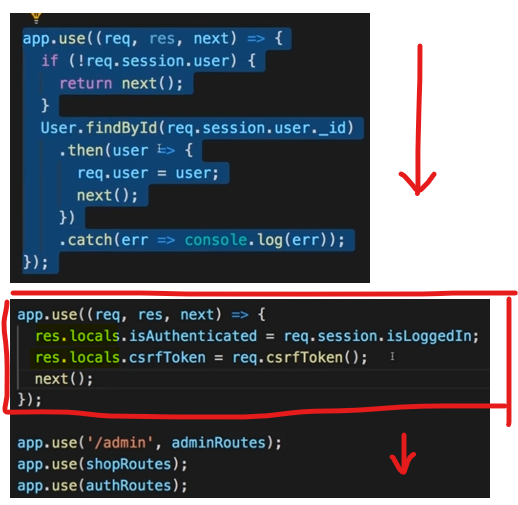
^~ khi cần render view có form cần submit 🡪 truyền csrf token vào

Như này



Input name : must be “\_csrf”

# Sử dụng middleware cho csrf

lưu ý thứ tự : phải add nó trước ~ route

\*\*\*\*\*res.locals : là thuộc tính của middleware chỉ dành cho ~ response nào render view

 Đây là lỗi khi view không có csrf hidden input