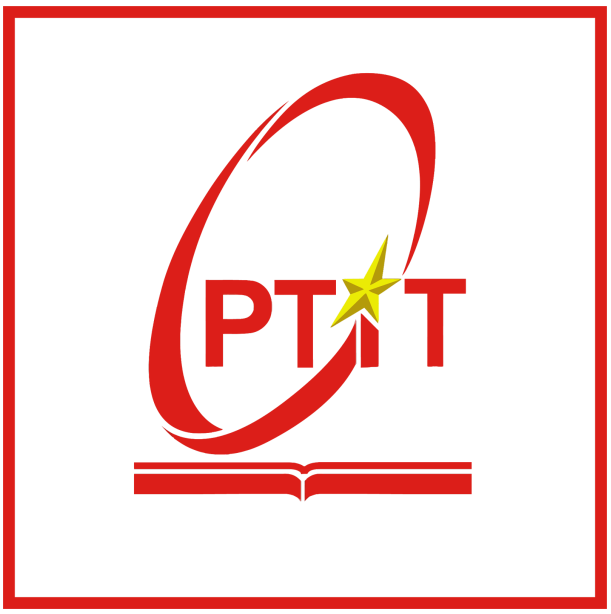
BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO THỰC TẬP CƠ SỞ TUẦN 3

XÁC THỰC VÀ BẢO MẬT THÔNG TIN TRONG WEBSITE

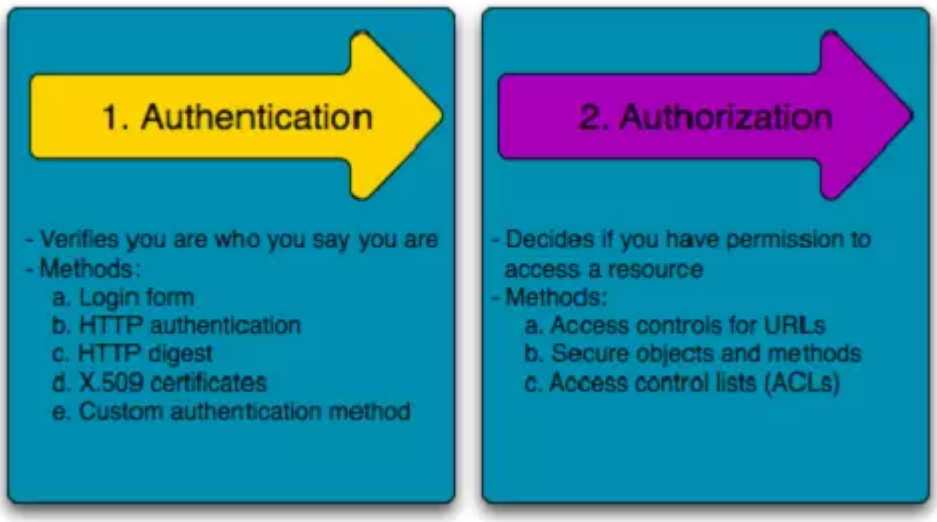
Giảng viên hướng dẫn: TS. Kim Ngọc Bách

Sinh viên thực hiện:

- Nguyễn Quang Trung - B22DCDT321

MỤC LỤC

I. Authorization và Authentication



Authentication là gì? Authentication (tạm dịch: xác thực) là quá trình kiểm tra danh tính một tài khoản đang vào hệ thống hiện tại thông qua một hệ thống xác thực.

Đây là bước ban đầu của mọi hệ thống có yêu cầu về nhận biết người dùng hoặc có yêu cầu lưu trữ các hành động cá nhân hoá của từng người dùng riêng. Hiểu đơn giản, Authentication là quá trình đi tìm câu trả lời cho câu hỏi "Bạn là ai?"

Authorization là quá trình để xác định người dùng có được xác thực có quyền truy cập vào các tài nguyên cụ thể hay không. Nó xác minh quyền của bạn để cấp cho bạn quyền truy cập vào các tài nguyên như thông tin, cơ sở dữ liệu, file,…

Authorization thường được đưa ra sau khi xác thực xác nhận các đặc quyền thực hiện của bạn. Nói một cách đơn giản hơn, nó giống như cho phép ai đó chính thức làm điều gì đó hoặc bất cứ điều gì.

Authentication khác gì so với Authorization ?

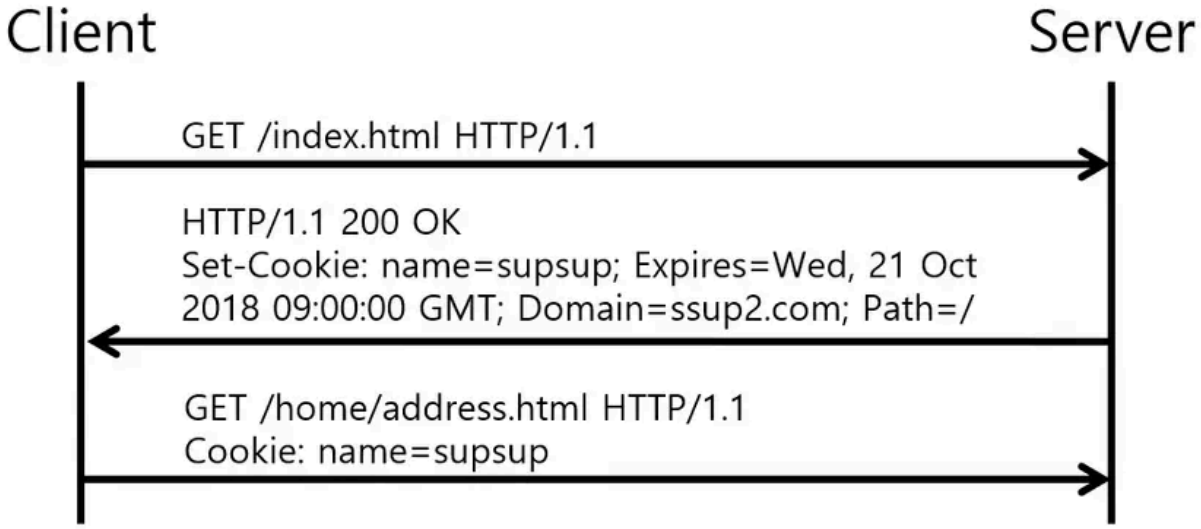
Tiêu chí	Xác thực (Authentication)	Ủy quyền (Authorization)
Định nghĩa	Là quá trình xác minh danh tính của người dùng trước khi cho phép họ truy cập hệ thống, tài khoản hoặc tệp tin.	Là quá trình xác minh mức độ truy cập của người dùng vào hệ thống, tài khoản hoặc tệp tin.
Mục đích	Xác nhận danh tính người dùng và ngăn chặn những người dùng đáng ngờ hoặc độc hại.	Đảm bảo chỉ những người dùng được ủy quyền mới có thể truy cập vào tài nguyên cần thiết.
Cách hoạt động	Dựa trên xác minh thông tin xác thực (username, password, OTP, câu hỏi bảo mật).	Dựa trên chiến lược ủy quyền như Kiểm soát truy cập dựa trên vai trò (RBAC).
Công nghệ áp dụng	So sánh thông tin đăng nhập với dữ liệu lưu trữ trong cơ sở dữ liệu để xác nhận danh tính.	Ánh xạ quyền truy cập với vai trò của người dùng, không phải với từng cá nhân.
Kết quả	Nếu xác thực thành công, người dùng có thể truy cập vào hệ thống.	Nếu được ủy quyền, người dùng chỉ có thể truy cập vào các thông tin phù hợp với vai trò của họ.

Mặc dù, cả hai thuật ngữ thường được sử dụng kết hợp với nhau, chúng có các khái niệm và ý nghĩa hoàn toàn khác nhau. Trong khi cả hai khái niệm này đều quan trọng đối với cơ sở hạ tầng dịch vụ web, đặc biệt là khi cấp quyền truy cập vào hệ thống, hiểu từng thuật ngữ liên quan đến bảo mật là chìa khóa. Trong khi hầu hết chúng ta nhầm lẫn một thuật ngữ này với một thuật ngữ khác, hiểu được sự khác biệt giữa chúng là điều quan trọng thực sự rất đơn giản. Nếu authentication là bạn là ai thì authorization là những gì bạn có thể truy cập và sửa đổi. Nói một cách đơn giản, authentication là xác định xem ai đó là người mà anh ta tuyên bố là. Mặt khác, Authorization xác định quyền của mình để truy cập tài nguyên.

II. Cookies

Cookie HTTP là một phần dữ liệu mà máy chủ gửi đến trình duyệt web. Sau đó, trình duyệt web lưu trữ cookie HTTP trên máy tính của người dùng và gửi nó trở lại cùng một máy chủ trong các yêu cầu sau này.

Cookie HTTP còn được gọi là web cookie hoặc browser cookie. Và nó thường được gọi là cookie.



Như ta biết HTTP request chỉ là stateless, vì khi ta gửi hai yêu cầu HTTP tuần tự đến máy chủ, không có liên kết nào giữa chúng. Nói cách khác, máy chủ không thể biết liệu hai yêu cầu có phải từ cùng một trình duyệt web hay không.

Do đó, Cookie được sử dụng để cho biết liệu hai yêu cầu có đến từ cùng một trình duyệt web hay không.

Trên thực tế, cookie phục vụ các mục đích sau:

- Quản lý Session - cookie cho phép bạn quản lý bất kỳ thông tin nào mà máy chủ cần ghi nhớ. chẳng hạn như thông tin đăng nhập, giỏ hàng, v.v.
- Cá nhân hóa - cookie cho phép bạn lưu trữ thông tin người dùng, chủ đề và cài đặt cụ thể cho người dùng.
- Theo dõi - cookie giúp ghi lại và phân tích các hành vi của người dùng trong quảng cáo.

Có bao nhiêu loại cookies?

1. Session Cookies:

Session cookies (cookies phiên) là cookies tạm thời chỉ được lưu trữ trên thiết bị của người dùng trong phiên duyệt web của họ. Sau khi đóng trình duyệt, cookies này sẽ tự động bị xóa.

Chúng thường được sử dụng để theo dõi các hoạt động của người dùng trong một lần truy cập trang web, chẳng hạn như duy trì trạng thái đăng nhập hoặc theo dõi các mặt hàng trong giỏ hàng trực tuyến.

2. Permanent Cookies:

Không giống như session cookies, permanent cookies (còn được gọi là cookies liên tục hoặc cookies lưu trữ) không bị xóa sau khi đóng trình duyệt.

Chúng vẫn còn trên thiết bị của người dùng trong một khoảng thời gian cụ thể hoặc cho đến khi người dùng xóa chúng theo cách thủ công. Cookies này thường được sử dụng để ghi nhớ các tùy chọn của người dùng và thông tin đăng nhập trong nhiều lần truy cập vào một trang web.

3. First-Party Cookies:

First-Party cookies của bên thứ nhất được đặt theo miền trang web mà người dùng hiện đang truy cập.

Chúng được sử dụng để lưu trữ dữ liệu liên quan đến các chức năng riêng của trang web và thường được coi là ít xâm phạm hơn về mặt quyền riêng tư.

4. Third-Party Cookies:

Third-Party cookies được đặt bởi các miền khác với miền mà người dùng đang truy cập.

Các cookies này thường được các bên quảng cáo sử dụng để theo dõi hành vi của người dùng trên các trang web khác nhau, cho phép các bên quảng cáo được nhắm mục tiêu và lập hồ sơ người dùng.

5. Flash Cookies (Đối tượng chia sẻ cục bộ):

Flash cookies là các tệp dữ liệu được lưu trữ bởi Adobe Flash Player trên thiết bị của người dùng.

Chúng tương tự như cookies thông thường nhưng có thể lưu trữ lượng dữ liệu lớn hơn và không được quản lý thông qua trình duyệt. Flash cookies thường được sử dụng để theo dõi và được biết đến với khả năng liên tục tạo lại các cookies truyền thống ngay cả khi người dùng đã xóa chúng.

6. Zombie Cookies:

Zombie cookies, còn được gọi là everCookies, được thiết kế để tự động tạo lại các cookies ngay khi bị người dùng xóa, được quản lý thông qua trình duyệt. Họ sử dụng nhiều kỹ thuật khác nhau, chẳng hạn như lưu trữ dữ liệu ở nhiều vị trí hoặc tự tạo lại bằng cách sử dụng các loại lưu trữ khác như flash cookies.

Người dùng có thể quản lý và xóa cookies thông qua cài đặt trình duyệt, đảm bảo một số quyền kiểm soát về quyền riêng tư.

Cookies hoạt động bằng cách thiết lập một kênh liên lạc quan trọng giữa trình duyệt web của người dùng và máy chủ. Quá trình này bắt đầu khi người dùng truy cập một trang web, yêu cầu máy chủ gửi hướng dẫn đến trình duyệt một tệp văn bản nhỏ chứa dữ liệu theo cặp khóa-giá trị.

Những cookies này sau đó được trình duyệt lưu trữ cục bộ trên thiết bị của người dùng. Khi người dùng truy cập lại cùng một trang web trong tương lai, trình duyệt sẽ tự động đưa các cookies có liên quan vào các yêu cầu đối với máy chủ. Thông qua cơ chế này, máy chủ có thể xác định và nhận ra người dùng, tạo ra một trải nghiệm duyệt web cá nhân hóa hơn.

Các cookies được lưu trữ trên thiết bị của người dùng cho phép máy chủ truy cập và truy xuất dữ liệu liên quan đến các tương tác trước đây của người dùng với trang web. Dữ liệu này giúp tùy chỉnh trải nghiệm của người dùng dựa trên các tùy chọn và hành động trước đây của họ.

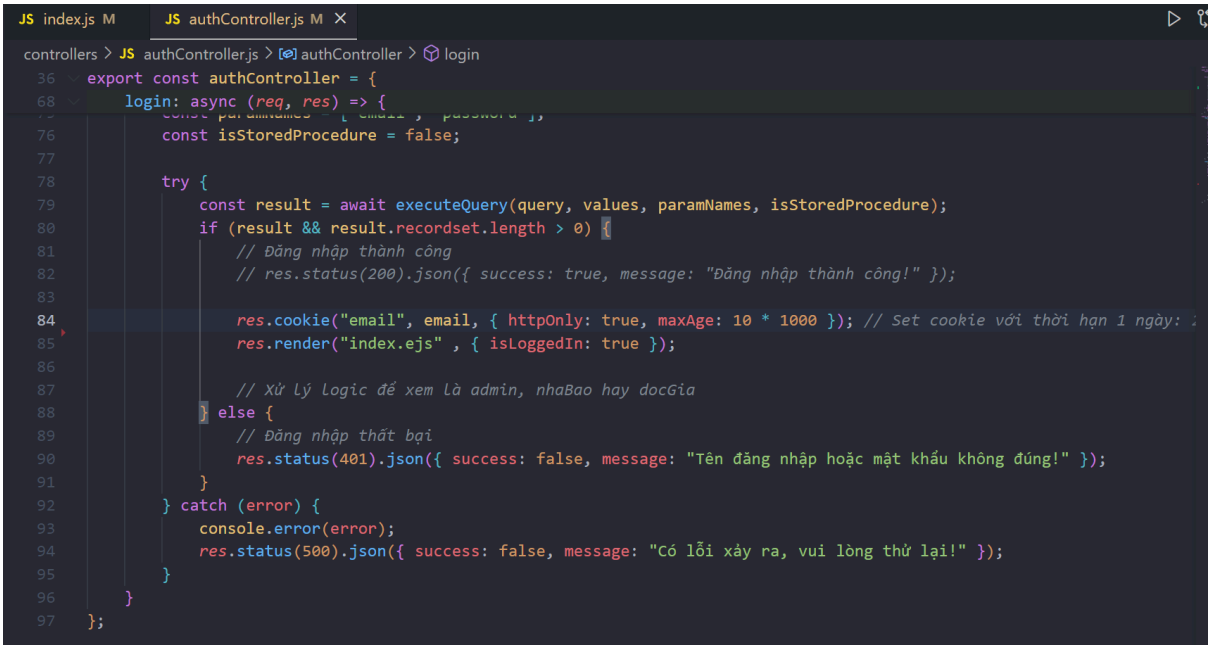
Điều quan trọng cần lưu ý là các cookie có thể có thời gian tồn tại khác nhau, một số cookies dựa trên phiên và hết hạn khi người dùng đóng trình duyệt, trong khi một số khác tồn tại cho đến ngày hạn định (được cài đặt trước) hoặc bị xóa thủ công.

Mọi cookies được liên kết với một miền và đường dẫn cụ thể. Do đó, trình duyệt sẽ gửi cookies dành riêng cho máy chủ ban đầu và trỏ tới các URL trong đường dẫn đã chỉ định. Việc này đảm bảo rằng các cookies chỉ liên quan đến trang web đã tạo ra chúng, ngăn chặn truy cập trái phép vào dữ liệu được lưu trữ và tăng cường bảo mật và phân chia dữ liệu tổng thể.

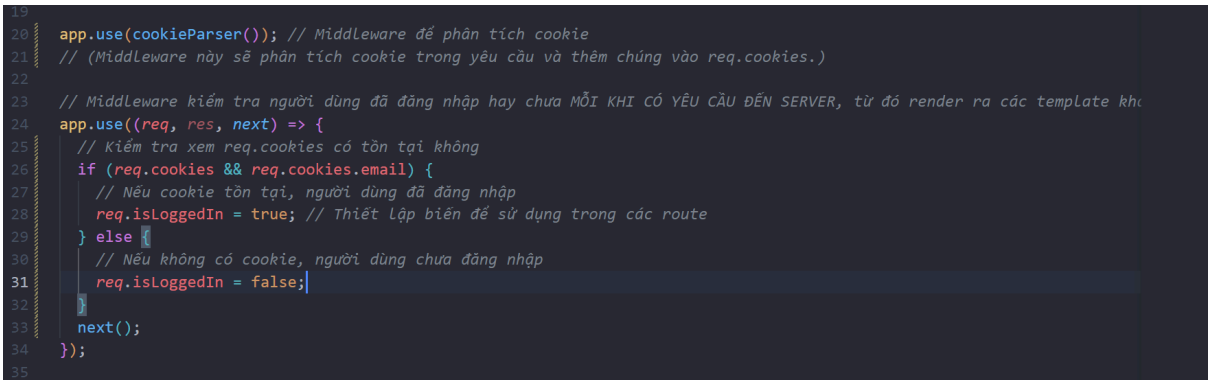
Cách tiếp cận này nhằm bảo vệ quyền riêng tư của người dùng và đảm bảo rằng cookies không vô tình tương tác với dữ liệu của các trang web khác hoặc tạo ra các lỗ hổng bảo mật tiềm ẩn.

→ Thực hành sử dụng cookies:

Tạo route và controller handle việc xác thực đăng nhập, sau khi kiểm tra trong database nếu thành công sẽ tạo ra cookies lưu trữ trạng thái đăng nhập. Sau đó mỗi khi client gửi request đến server sẽ đều qua middleware kiểm tra trạng thái đăng nhập để lấy tài nguyên tương ứng.

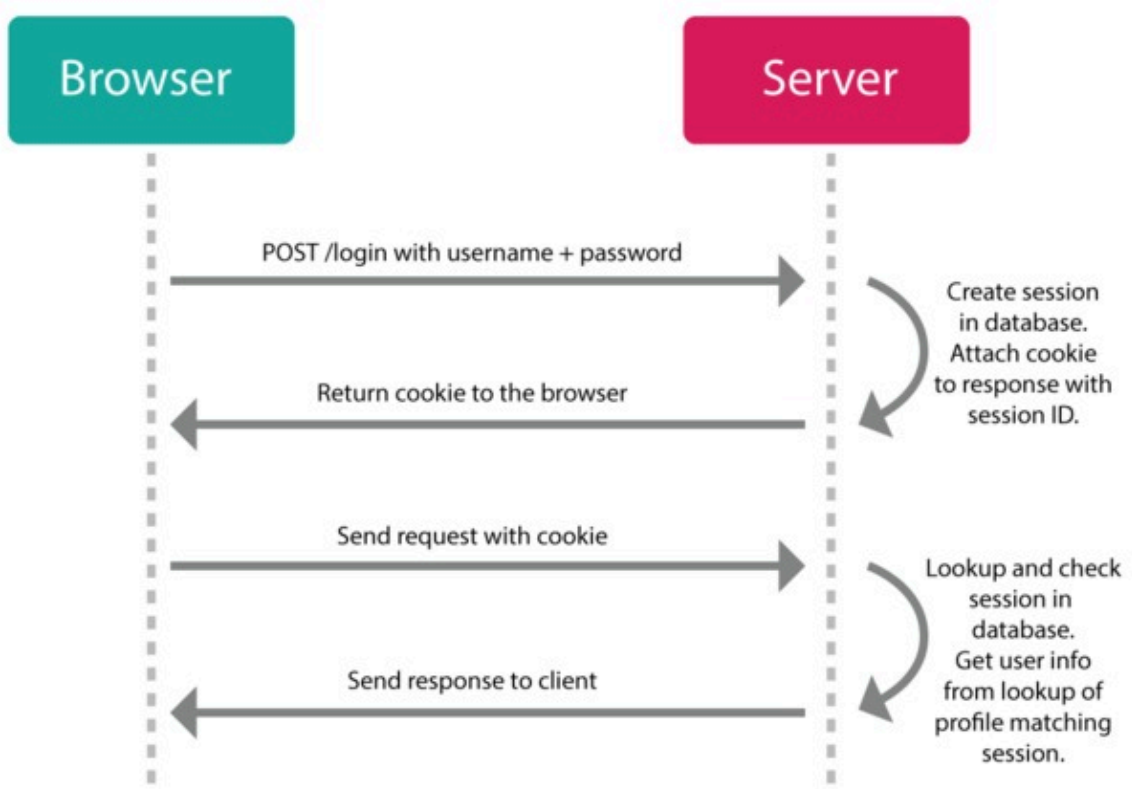


Sau khi đăng nhập thành công sẽ tạo cookie lưu trữ trạng thái đăng nhập



Middleware kiểm tra trạng thái đăng nhập trước khi request tới server

III. Session



Session là một khái niệm phổ biến được dùng trong lập trình các website có kết nối với cơ sở dữ liệu database. Đặc biệt các chức năng như đăng nhập, đăng xuất người dùng sẽ khó có thể thực hiện được nếu không sử dụng session.

Session đơn giản là 1 cách để chúng ta lưu lại dữ liệu của người dùng sử dụng website. Giá trị của session được lưu trong một tập tin trên máy chủ. Ví dụ khi bạn đăng nhập vào một trang web và đăng nhập với tài khoản đã đăng ký trước đó. Máy chủ sau khi xác thực được thông tin bạn cung cấp là đúng nó sẽ sinh ra một tập tin (hay chính là session của trình duyệt của bạn) chứa dữ liệu cần lưu trữ của người dùng.

Bạn có thể tùy ý quyết định xem nên lưu trữ những thông tin nào vào Session. Nhưng thông thường chúng ta chỉ nên lưu những thông tin tạm thời trong session ví dụ như số lượng sản phẩm người dùng đã thêm vào giỏ nhưng chưa mua, hay những nhật xét đang được viết và lưu dưới dạng nháp nhưng chưa gửi

đi. Những dữ liệu sử dụng lâu dài như nội dung nhận xét đã được gửi đi hay số sản phẩm đã được mua thì nên được thực hiện ở máy chủ chứa cơ sở dữ liệu.

→ Cách phân biệt session của các trình duyệt khác nhau

Sau khi tạo ra một tập tinh session trên máy chủ để lưu trữ dữ liệu tạm thời của người dùng, chúng ta cần phải phân biệt được session nào là của người dùng nào. Để làm điều này thì với mỗi session tạo ra cần phải tạo một cookie tương ứng với nó. Cookie là một mẩu tin nhỏ có thể được trình duyệt tạo ra khi người dùng truy cập vào web và dùng để lưu trữ thông tin của người dùng ở phía trình duyệt (client).

So sánh giữa Cookie và Session

Cookie	Session
Cookie được lưu trữ trên trình duyệt của người dùng.	**Session** không được lưu trữ trong trình duyệt của người dùng.
Dữ liệu **cookie** được lưu trữ ở phía máy khách.	Dữ liệu **session** được lưu trữ ở phía máy chủ.
Dữ liệu **cookie** dễ dàng sửa đổi khi chúng được lưu trữ ở phía khách hàng.	Dữ liệu **session** không dễ dàng sửa đổi vì chúng được lưu trữ ở phía máy chủ.
Dữ liệu **cookie** có sẵn trong trình duyệt của chúng ta đến khi hết hạn.	Dữ liệu **session** có sẵn cho trình duyệt chạy. Sau khi đóng trình duyệt sẽ mất thông tin **session**.