1. **Cookie**

**Ưu điểm:**

* Cookie được lưu trữ trên máy khách, cho phép server truy cập vào đó để lưu trữ thông tin về người dùng, giúp cho việc xác thực và lưu trữ thông tin phiên làm việc trở nên dễ dàng hơn.
* Cookie cho phép các ứng dụng Web tự động đăng nhập, cung cấp cho người dùng trải nghiệm đăng nhập thuận tiện hơn.
* Cookie có thể được sử dụng để lưu trữ các thông tin tùy chỉnh của người dùng như ngôn ngữ, cài đặt trang, vị trí, giúp tăng trải nghiệm người dùng.

**Nhược điểm**

* Cookie chỉ lưu trữ được một số lượng nhỏ thông tin, do đó không phù hợp cho việc lưu trữ các thông tin nhạy cảm.
* Cookie có thể bị xâm phạm, đánh cắp, cho phép người khác truy cập vào thông tin cá nhân của người dùng.
* Cookie không phải là giải pháp tuyệt đối cho việc xác thực người dùng, một số kẻ tấn công vẫn có thể tạo ra các cookie giả mạo và đánh lừa hệ thống.

**Ví dụ sử dụng Cookie trong ứng dụng Web thực tế**

Một trong những ví dụ sử dụng Cookie phổ biến nhất trong ứng dụng Web là việc lưu trữ thông tin đăng nhập của người dùng. Khi người dùng đăng nhập vào một trang web, trang web sẽ tạo ra một cookie trên máy tính của người dùng và lưu trữ thông tin đăng nhập. Khi người dùng truy cập trang web lần sau, cookie sẽ được đọc và xác thực người dùng mà không cần phải đăng nhập lại.

1. **Session**

**Ưu điểm :**

* Bảo mật: Session là một cách để lưu trữ thông tin liên quan đến người dùng một cách an toàn. Dữ liệu session được lưu trữ trên server thay vì trên trình duyệt của người dùng, ngăn chặn người dùng khác xâm nhập và sửa đổi dữ liệu.
* Phân cấp quyền truy cập: Dữ liệu session cho phép phân cấp quyền truy cập, vì vậy các người dùng khác nhau có thể truy cập vào các phần khác nhau của trang web, tùy thuộc vào quyền truy cập của họ.
* Hiệu suất tối ưu: Dữ liệu session được lưu trữ trên server, giúp giảm tải cho trình duyệt của người dùng và giúp trang web hoạt động nhanh hơn.
* Dễ sử dụng: Session là một cách dễ sử dụng để lưu trữ dữ liệu liên quan đến người dùng, và có thể được sử dụng để lưu trữ thông tin tạm thời hoặc dữ liệu có thể tái sử dụng trên nhiều trang web.

**Nhược điểm :**

* Tính bảo mật bị đe dọa khi bị tấn công Cross-Site Scripting (XSS): Nếu dữ liệu được lưu trữ trong session không được xác thực đúng cách, nó có thể dẫn đến tấn công Cross-Site Scripting (XSS) và mất bảo mật dữ liệu của người dùng.
* Tài nguyên máy chủ có thể bị chiếm dụng: Nếu không được xác thực đúng cách, session có thể dẫn đến chiếm dụng tài nguyên máy chủ, do đó làm giảm hiệu suất của trang web.
* Không thể chia sẻ giữa các ứng dụng khác nhau: Dữ liệu session chỉ có thể sử dụng trên cùng một ứng dụng web và không thể chia sẻ giữa các ứng dụng khác nhau.
* Chi phí lưu trữ: Lưu trữ dữ liệu session tốn chi phí.
* Tăng tải cho server khi có nhiều người dùng: Khi có nhiều người dùng truy cập trang web cùng một lúc, dữ liệu session sẽ tăng và ảnh hưởng đến hiệu suất của server.

**Ví dụ về cách sử dụng Session trong các ứng dụng web thực tế:**

* Sử dụng session để lưu trữ thông tin đăng nhập của người dùng, giúp họ không cần phải đăng nhập lại sau khi đăng nhập thành công.
* Sử dụng session để lưu trữ thông tin giỏ hàng của khách hàng trong một trang web bán hàng.
* Sử dụng session để lưu trữ thông tin phiên làm việc của người dùng trong một ứng dụng web.
* Sử dụng session để lưu trữ thông tin ngôn ngữ được chọn của người dùng trong một trang web đa ngôn ngữ.
* Sử dụng session để lưu trữ thông tin các sản phẩm đã được xem bởi người dùng trong một trang web bán hàng.