**Bài 1: Nêu các ưu điểm, hạn chế của Cookies và Session, liệt kê các ví dụ có sử dụng Cookie và Session trong ứng dụng web thực tế.**

**Bài làm**

**1) Cookies**

**Ưu điểm**:

* + Lưu trữ dữ liệu trên phía client: Cookies được lưu trữ trong trình duyệt của người dùng, giúp giảm tải cho server vì không cần phải lưu trữ thông tin người dùng mỗi lần yêu cầu.
  + Dễ dàng sử dụng cho các thông tin không nhạy cảm: Cookies có thể lưu trữ các giá trị như sở thích của người dùng, thông tin giỏ hàng, hoặc trạng thái đăng nhập.
  + Tồn tại lâu dài: Cookies có thể được cấu hình với thời gian sống lâu dài (có thể là nhiều tháng hoặc năm), giúp duy trì trạng thái người dùng qua các lần truy cập khác nhau.
  + Dễ dàng gửi thông tin từ client đến server: Cookies có thể gửi kèm thông tin trong mỗi yêu cầu HTTP mà không cần sự can thiệp thêm từ server.

**Nhược điểm**:

* + Giới hạn về kích thước lưu trữ: Mỗi cookie chỉ có thể chứa tối đa khoảng 4 KB dữ liệu, điều này có thể gây hạn chế khi cần lưu trữ dữ liệu lớn.
  + Vấn đề bảo mật: Nếu không được mã hóa hoặc thiết lập đúng cách, cookies có thể bị đánh cắp và gây nguy cơ về bảo mật. Cookies có thể bị sửa đổi bởi người dùng nếu không có bảo vệ tốt.
  + Yêu cầu phải bật cookie trên trình duyệt: Nếu người dùng tắt cookies trong trình duyệt, ứng dụng có thể gặp vấn đề trong việc duy trì trạng thái của người dùng.
  + Cookies có thể bị chặn hoặc bị sửa đổi: Người dùng có thể dễ dàng chỉnh sửa hoặc xóa cookies, gây mất mát thông tin trong ứng dụng.

**Ví dụ sử dụng Cookies**:

* + Giỏ hàng khi mua sắm online: Cookies có thể lưu trữ các sản phẩm đã thêm vào giỏ hàng, ngay cả khi người dùng chưa đăng nhập.
  + Trạng thái đăng nhập: Sau khi đăng nhập, một cookie có thể lưu trữ thông tin nhận dạng người dùng, giúp họ duy trì phiên làm việc khi quay lại trang web.
  + Lựa chọn ngôn ngữ: Cookies có thể lưu trữ thông tin về ngôn ngữ mà người dùng chọn để duy trì sự phù hợp trong các lần truy cập sau.

**2) Sessions**

**Ưu điểm**:

* + An toàn hơn Cookies: Dữ liệu của session được lưu trữ trên server, giảm thiểu nguy cơ bị đánh cắp bởi các hacker. Cookies chỉ chứa ID phiên, không lưu trữ dữ liệu nhạy cảm.
  + Dễ dàng quản lý: Sessions cho phép quản lý trạng thái người dùng và dữ liệu phiên một cách dễ dàng trên server, không bị giới hạn về dung lượng như cookies.
  + Hỗ trợ đăng nhập và bảo mật cao: Các thông tin nhạy cảm như mật khẩu hoặc thông tin thanh toán có thể được lưu trữ trong session, không cần phải lưu trữ trực tiếp trên client, giúp bảo mật tốt hơn.
  + Giảm tải cho client: Vì dữ liệu không cần phải gửi đi trong mỗi yêu cầu HTTP, session giúp giảm tải cho client khi lưu trữ nhiều thông tin hơn.

**Nhược điểm**:

* + Dễ bị mất nếu đóng trình duyệt: Mặc dù session có thể duy trì dữ liệu trong suốt phiên làm việc của người dùng, nhưng khi người dùng đóng trình duyệt hoặc hết thời gian, session sẽ bị mất. Tuy nhiên, có thể cấu hình session để kéo dài thêm thời gian sống.
  + Tải trên server: Server phải lưu trữ dữ liệu của session, điều này có thể gây tải cao nếu ứng dụng có nhiều người dùng. Việc quản lý session cũng có thể tốn tài nguyên.
  + Yêu cầu duy trì session ID: Session ID phải được truyền qua các yêu cầu HTTP (thường là qua cookies hoặc URL). Nếu không có session ID, server không thể nhận diện người dùng và mất trạng thái phiên làm việc.
  + Mất session khi server lỗi hoặc reset: Nếu server gặp sự cố hoặc bị reset, session có thể bị mất, ảnh hưởng đến trải nghiệm người dùng.

**Ví dụ sử dụng Sessions**:

* + Thanh toán trực tuyến: Khi người dùng thực hiện thanh toán trực tuyến, session lưu trữ thông tin giỏ hàng, thông tin thanh toán và các bước trong quy trình checkout.
  + Quản lý quyền truy cập: Sessions có thể được sử dụng để kiểm tra quyền truy cập vào các phần của website, ví dụ: chỉ cho phép người dùng đã đăng nhập truy cập vào trang quản trị.
  + Trạng thái đăng nhập: Session lưu trữ thông tin người dùng sau khi đăng nhập, để người dùng không phải nhập lại mật khẩu trong suốt phiên làm việc của họ.