1. Điều kiện tiên quyết

Bài tập Quản lí tài khoản người dùng và xác thực.

2. Giới thiệu

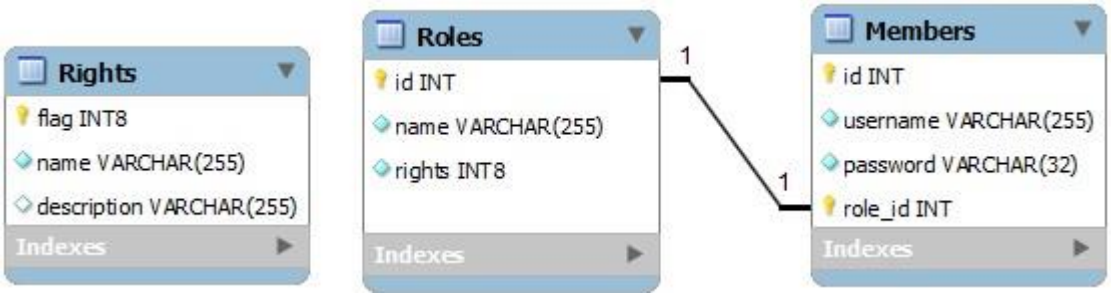
2.1. Phân quyền người dùng

Sau khi người dùng đăng nhập thành công, nhiệm vụ tiếp theo của ứng dụng web là xác định những tài nguyên mà người dùng được phép truy cập.
Thao tác này được gọi là phân quyền người dùng (users authorization). Như đã biết, có ba mô hình phân quyền truy cập điển hình là: *phân quyền truy cập tùy quyền* (discretionary access control), *phân quyền truy cập bắt buộc* (mandatory access control) và *phân quyền truy cập dựa trên vai trò* (role-based access control). Đối với ứng dụng web, mô hình phân quyền thường được sử dụng là phân quyền dựa trên vai trò. Bên cạnh đó, các ngôn ngữ lập trình web khác nhau có thể có hỗ trợ riêng trong vấn đề này.

Trong phân quyền dựa trên vai trò, người dùng được gán một vai nhất định trong hệ thống. Mỗi vai như thế được cấp những quyền nhất định. Để xác định một người dùng có một quyền nào đó hay không, trước hết cần xác định vai của người dùng đó, tiếp theo là xác định xem vai đó có được cấp quyền nói trên hay không. Có thể có nhiều kỹ thuật khác nhau để triển khai mô hình phân quyền này, trong số đó kỹ thuật được sử dụng phổ biến và hiệu quả hiện nay là sử dụng cờ. Mỗi cờ là một bít nào đó trong một dãy bít. Nếu cờ được bật (bít tương ứng có giá trị bằng 1) thì quyền được cấp, còn ngược lại (bít tương ứng có giá trị bằng 0) thì quyền không được cấp. Trên thực tế, nếu số lượng quyền không quá lớn, cụ thể là không vượt quá 64, thì người dùng một số nguyên để biểu diễn dãy bít. Kiểu số nguyên lớn nhất hiện nay được hỗ trợ trên các hệ thống thông thường là 8 byte, tức 64 bít.

Mỗi nhóm thường được phần nhiều quyền khác nhau, tức là sẽ có nhiều bít khác nhau được bật.

Tất nhiên, các thông tin trên đây thường được lưu trong cơ sở dữ liệu. Cụ thể, để lưu thông tin phần quyền người dùng, cần sử dụng hai bảng. Bảng thứ nhất là bảng vai trò (Roles) và bảng thứ hai là bảng người dùng (Members) như trên Hình 2.11. Ngoài ra cũng nên sử dụng thêm bảng Rights để định nghĩa các cờ tương ứng với các quyền.



Hình 2.1. Lưu thông tin phân quyền người dùng

Việc tổ hợp quyền có thể được thực hiện bằng phép cộng thông thường hoặc áp dụng phép logic hoặc trên từng bít (bitiwse OR). Ví dụ, tổ hợp hai quyền ViewThread và DeleteThread có thể được xác định bởi:
0000.0000.0000.0001 + 0000.0000.0000.1000 = 0000.0000.0000.1001 = 9 hoặc
0000.0000.0000.0001 | 0000.0000.0000.1000 = 0000.0000.0000.1001 = 9

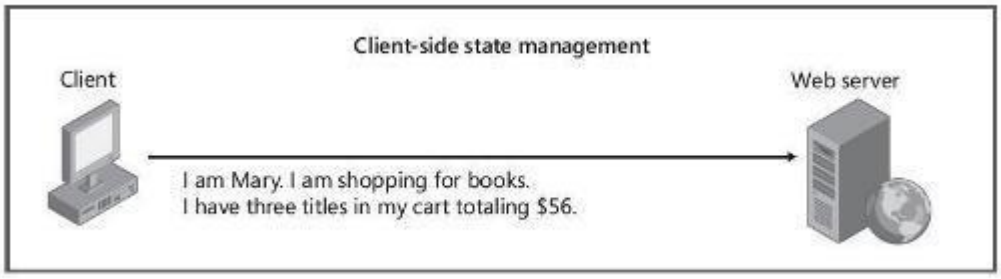
Còn để xác định một người dùng (một vai) có quyền nào đó hay không, có thể sử phép logic và trên từng bít (bitiwise AND). Nếu kết quả khác 0 (cụ thể là bằng đúng giá trị cờ của quyền được kiểm tra) thì câu trả lời là Có, còn nếu kết quả bằng 0 thì câu trả lời là Không.

2.2. Quản lí trạng thái phiên làm việc

Vì bản thân giao thức HTTP là giao thức không trạng thái mà hầu hết các ứng dụng web cần có cơ chế để ghi nhớ kết quả các thao tác của người dùng qua nhiều lần thực hiện truy vấn khác nhau. Cơ chế như thế được gọi là cơ chế quản lý trạng thái (State Managment). Nhìn chung, có hai lựa chọn trong việc quản lý trạng thái:

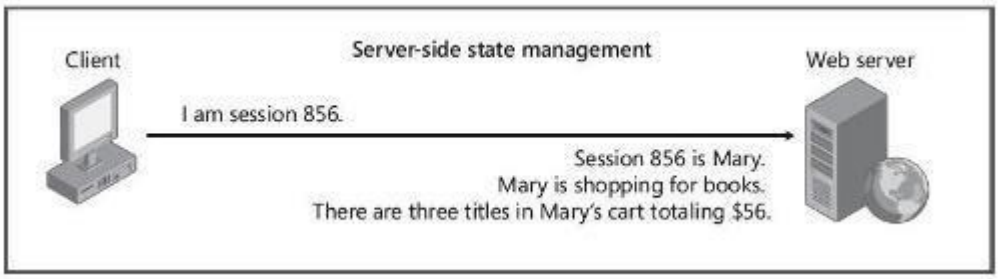
- Quản lý trạng thái ở phía client
- Quản lý trạng thái ở phía server

Khi thực hiện quản lý trạng thái ở phía client, mọi thông tin liên quan đến trạng thái sẽ được lưu tại client. Các thông tin này sẽ được client gửi cho server mỗi khi thực hiện truy vấn. Cách quản lý trạng thái này có thể được diễn tả như trên Hình 2.2. Cần lưu ý rằng các thông tin trạng thái này được lưu giữ ở client nhưng do server tạo ra; và việc sửa đổi hay xóa bỏ các thông tin đó cũng do server quyết định. Server sẽ gửi thông báo cho client (trong phần tiêu đề của phản hồi HTTP) mỗi khi tạo mới, sửa đổi hoặc hủy bỏ một thông tin nào đó.



Hình 2.2. Quản lý trạng thái ở phía client

Còn nếu thực hiện quản lý trạng thái ở phía server thì các thông số của trạng thái được lưu trữ và xử lý trên server. Giữa client và server chỉ cần duy trì một mã số cho phép xác định duy nhất bộ thông tin trạng thái trên server. Cách quản lý trạng thái này có thể được diễn ta như trên Hình 2.3.



Hình 2.3. Quản lý trạng thái ở phía server

Các ngôn ngữ lập trình web hiện nay (PHP, ASP, ASP.NET, JSP) đều hỗ trợ quản lý trạng thái ở phía client thông qua cookie và hỗ trợ quản lý trạng thái ở phía server thông qua session. Ngoài ra, các ngôn ngữ lập trình khác nhau có thể hỗ trợ những kỹ thuật khác để thực hiện quản lý trạng thái trong cả hai trường hợp trên.

3. Kịch bản Xây dựng thêm các chức năng cơ bản để phân quyền người dùng và quản lý phiên cho ứng dụng web trong bài tập Quản lí tài khoản người dùng và xác thực:

- Chức năng Quản lí sách đối với thủ thư: thêm, sửa, xóa Sách (Mã số sách, tên sách, tác giả, năm xuất bản, nhà xuất bản, Thể loại, mô tả nội dung, số lượng, đơn giá); thêm, sửa, xóa Thể loại (tên thể loại, mô tả).
- Chức năng Mượn sách đối với sinh viên, cán bộ, giảng viên: xem và lựa chọn các sách để mượn (có thể thêm, xóa, sửa các sách trong phiếu mượn); thêm, sửa, xóa phiếu mượn. Tuy nhiên khi đã gửi phiếu mượn thì sẽ không thay đổi được nữa.

- Chức năng Quản lí người dùng đối với Quản trị viên: thêm, sửa, xóa người dùng, quyền người dùng.

4. Mục tiêu bài thực hành

Bài tập này nhằm giúp sinh viên:

- Hiểu về cơ chế phân quyền người dùng và quản lí trạng thái phiên làm việc trong an toàn ứng dụng web.
- Biết cách thực thi các cơ chế an toàn trong phân quyền người dùng và quản lí trạng thái phiên làm việc trong ứng dụng web.

5. Tổ chức thực hành

Yêu cầu thực hành: thực hành độc lập

Thời gian: 120 phút

6. Môi trường thực hành

6.1. Phần cứng, phần mềm

- Yêu cầu phần cứng:
  - 01 máy tính
  - Cấu hình tối thiểu: Intel Core i3, 4GB RAM, 50 GB ổ cứng
- Yêu cầu phần mềm trên máy (tùy từng ngôn ngữ lựa chọn để phát triển ứng dụng mà cài đặt môi trường tương ứng):
  - Phần mềm xây dựng web server: Xampp v3.2.2/IIS/…
  - Phần mềm dùng để code: Sublime Text hoặc Visual Studio Code/...
- Yêu cầu kết nối mạng Internet: có

7. Các nhiệm vụ cần thực hiện

Trên giao diện của ứng dụng web có cấu trúc tối thiệu gồm các mục như trong bảng phía dưới:

Ảnh của sinh viên	Thông tin về: Số thứ tự của sinh viên trong danh sách lớp Họ và tên sinh viên Mã số sinh viên

Menu	Nội dung chính
Thông tin bản quyền của sinh viên	

Các chức năng sẽ nằm ở phần "Nội dung chính".

Nhiệm vụ 1. Tạo chức năng Quản lí người dùng

Quản trị viên: thêm, sửa, xóa người dùng, quyền người dùng.

Thông tin của người dùng giống như trong bài Quản lí tài khoản người dùng và xác thực.

Có áp dụng các chính sách an toàn đối với định danh và mật khẩu.

Áp dụng chính sách lưu trữ mật khẩu an toàn trong cơ sở dữ liệu.

Nhiệm vụ 2. Tạo chức năng Quản lí sách

Thủ thư: thêm, sửa, xóa Sách (Mã số sách, tên sách, tác giả, năm xuất bản, nhà xuất bản, Thể loại, mô tả nội dung, số lượng, đơn giá); thêm, sửa, xóa Thể loại (tên thể loại, mô tả).

Nhiệm vụ 3. Tạo chức năng Mượn sách

Sinh viên, cán bộ, giảng viên: xem và lựa chọn các sách để mượn (có thể thêm, xóa, sửa các sách trong phiếu mượn); thêm, sửa, xóa phiếu mượn. Tuy nhiên khi đã gửi phiếu mượn thì sẽ không thay đổi được nữa.

8. Đánh giá bài tập

TT	Tiêu chí đánh giá	Trọng số
1	Chức năng đã cài đặt	70%
2	Thiết kế: Logic, dễ sử dụng, đẹp	10%
3	Tổ chức mã: Tách biệt mã tạo giao diện và mã xử lý nghiệp vụ, tổ chức thư viện, lớp và kế thừa lớp, mô hình MVC	10%
4	Phong cách lập trình: Trình bày mã, chú thích mã, …	10%
	Tổng	100%