BÀI TẬP CHƯƠNG 3

Bài tập 1

Hãy cho biết HQT CSDL đang dùng có những privilege gì trên từng loại đối tượng dữ liệu (table, view, ..)?

Hãy cho biết HQT CSDL đang dùng cung cấp sẵn những role gì? Cho biết với role đó, người dùng có thể thực hiện những privilege gì?

Hãy cho biết HQT CSDL đang dùng sử dụng cơ chế thu hồi quyền dây chuyền hay không dây chuyền? Cho ví dụ minh họa.

Hãy cho ví dụ minh họa về việc điều khiển truy cập dựa trên nội dung (giới hạn dòng, cột) thông qua view. Nếu một user bị thu hồi quyền đọc dữ liệu trên bảng cơ sở (tạo ra view) thì quyền trên view còn hợp lệ hay không? Cho ví dụ minh họa.

Hãy minh họa về:

- Sự ưu tiên của quyền phủ định so với quyền khẳng định khi phân quyền cho một chủ thể.
- Khi rút lại quyền phủ định thì chủ thể có thể sử dụng lại quyền khẳng định.

Bài tập 2

Hãy cho ví dụ kiểm chứng về quyền của 1 user khi user U thỏa mãn những điều kiện sau:

- U thừa hưởng quyền ở các trạng thái granted, denied, revoked trực tiếp từ user khác.
- Hãy gán một số quyền cho role A, B, C, D. Cho U thừa hưởng quyền từ role C và D, role C là thành viên của role A, role D là thành viên của role B. Hãy thực hiện các quyền ở các trạng thài granted, denied, revoked trên A, B, C, D và kiểm chứng quyền cuối cùng của U.
- Hãy rút ra quy luật về quyền cuối cùng của U khi thừa hưởng quyền trực tiếp và gián tiếp qua role ở các trạng thái granted, denied, revoked.

Bài tập 3

Hãy đề ra 3 chính sách bảo mật trong một CSDL cụ thể và dùng VPD để làm các chính sách bảo mật đó có hiệu lực?

Khi áp dụng đồng thời nhiều chính sách cùng một lúc thì ta thực hiện như thế nào? Kết quả ra sao?

Khi một chính sách bảo mật trước đó đã được áp dụng bị thay đổi ta phải làm gì?

Những người dùng nào mới có thể làm cho một chính sách có hiệu lực thông qua việc dùng RLS của VPD?

Cho biết HQT CSDL đang dùng hỗ trợ những ngữ cảnh gì trong quá trình điều khiển truy cập?

Hãy tìm hiểu và cho ví dụ minh họa về việc sử dụng kết hợp RLS và Application context.

Bài tập 4

Cho 3 quan hệ sau:

NHANVIEN(MANV, MAPB, CHUCVU)

LUONG(MANV, THANG, LUONGCB, PHUCAP, TONGLUONG)

TONGHOP(NAM, MAPB, THU, CHI)

Nhân sự trong công ty gồm có:

- 1 giám đốc.
- 3 trưởng phòng.
- 10 nhân viên phòng kế toán.
- 15 nhân viên phòng kế hoạch.
- 10 nhân viên phòng kỹ thuật.

Sau đây là ma trận quyền truy xuất.

	MANV	MAPB	CHUCVU	THANG	LUONGCB	PHUCAP	TONGLUONG	NAM	THU	CHI
Giám đốc	01	01	01	01	01	01	01	11	11	11
Trưởng phòng	11	11	11	11	11	11	11	00	00	00
Nhân viên	01	01	01	00	00	00	00	00	00	00

Bit 1: quyền đọc, bit 2: quyền ghi; 0: không được quyền; 1: được quyền

Câu A: Dùng các lệnh cấp quyền và lấy lại quyền để thực hiện các yêu cầu sau:

1. Hãy cấp quyền cho các người dùng theo ma trận quyền truy xuất trên.
2. Giám đốc cấp quyền Đọc trên quan hệ TONGHOP cho các trưởng phòng.
3. Trưởng phòng cấp quyền Đọc trên quan hệ TONGHOP cho các nhân viên trong phòng.
4. Giám đốc lấy lại quyền đọc trên thuộc tính CHI.
5. Vẽ lại ma trận quyền truy xuất sau khi đã thực hiện các lệnh cấp quyền và lấy lại quyền theo yêu cầu trên.

Câu B: Hãy dùng cơ chế RBAC để thực hiện các yêu cầu trong câu A.

Bài tập 5

Hãy mô tả chi tiết công việc chuẩn bị một phòng máy cho sinh viên thực tập, với các yêu cầu được liệt kê như sau:

- Tạo 40 cơ sở dữ liệu trên sever, đặt tên là sv1, sv2, …, sv40.
- Cho phép 40 sinh viên có thể làm việc trên hệ thống này, mỗi sinh viên được chỉ được toàn quyền trên 1 cơ sở dữ liệu, không được xóa CSDL. Tương ứng, quyền svi chỉ được làm việc trên CSDL tên là svi mà không được nhìn thấy dữ liệu hay làm bất cứ điều gì trên cơ sở dữ liệu khác.

Bài tập 6

Cho lược đồ CSDL sau:

1. NHANVIEN (MANV, HONV, TENLOT, TENNV, PHAI, LUONG, DIACHI, NGAYSINH, MANQL, PHG)
2. PHONGBAN (MAPB, TENPB, TRPHG, NGAYBĐ)
3. DIADIEM_PHG (MAPB, DIADIEM)
4. DEAN (MADA, TENDA, NGAYBD, PHONG, DIADIEM_DA)

5. PHANCONG (MANV, MADA, THOIGIAN)
6. THANNHAN(MANV, TENTN,PHAI,NGSINH,QUANHE)

Giả sử tất cả các quan hệ được tạo ra (và thuộc sở hữu) của user X. X muốn thực hiện cấp các quyền sau cho các account A, B, C, D, E:

i. A có thể tìm kiếm và cập nhật trên tất cả các quan hệ trừ quan hệ THANNHAN. A có thể cấp tất cả những quyền này cho những user khác.
ii. B có thể tìm kiếm trên tất cả các thuộc tính của quan hệ NHANVIEN và PHONGBAN ngoại trừ các thuộc tính LUONG, MANQL, NGAYBĐ.
iii. C có thể tìm kiếm và cập nhật trên PHANCONG nhưng chỉ có thể tìm kiếm trên MANV, HONV, TENLOT và TENNV của bảng NHANVIEN và MADA, TENDA của bảng DEAN mà thôi.
iv. D có thể tìm kiếm trên tất cả các thuộc tính trên NHANVIEN hoặc THANNHAN và có thể cập nhật THANNHAN.
v. E có thể tìm kiếm tất cả các thuộc tính của NHANVIEN nhưng chỉ với những dòng có PHG = 3.

Hãy thực hiện vai trò của X trên HQT CSDL đang sử dụng.

Bài tập 7 Trên CSDL ở bài tập 6, có thể bổ sung một số trường cần thiết, hãy hiện thực các chính sách bảo mật sau:

1. Nhân viên có thể xem mọi dòng dữ liệu trong bảng NHANVIEN, nhưng chỉ có chính họ mới có thể xem thông tin cột LUONG của họ.
2. Nhân viên chỉ được xem dữ liệu liên quan đến chính nhân viên đó, dba được truy cập tất cả.
3. Trưởng phòng được xem thông tin nhân viên thuộc phòng ban mà họ phụ trách.
4. Hãy tạo chính sách bảo mật quy định không một người dùng nào có thể xem nhân viên thuộc phòng ban có mã là 10 trừ DBA.
5. Các người dùng chỉ được insert và update trên các dòng dữ liệu của phòng ban có mã phòng ban < 5.

6. Hãy tạo ra chính sách bảo mật không cho truy xuất đến dòng nào của một bảng dữ liệu dùng VPD.
7. Hãy tạo ra chính sách bảo mật biến 1 bảng dữ liệu thành bảng chỉ đọc (Read-Only).
8. Trên hai bảng NHANVIEN và PHONGBAN, hãy hiện thực chính sách bảo mật nói rằng:

– Mỗi nhân viên chỉ được xem và chỉnh sửa thông tin do chính nhân viên đó tạo ra.
– Trưởng phòng ban được sửa thông tin của chính họ và chỉ được xem thông tin các nhân viên thuộc phòng ban họ quản lý.
– Giả sử có thêm một bảng dữ liệu GIOIHAN ghi nhận lại ứng với từng giá trị mã nhân viên thì giá trị lương cao nhất mà nhân viên đó được phép đọc là bao nhiêu. Chính sách bảo mật là mỗi nhân viên chỉ được phép xem thông tin của những nhân viên có giá trị lương nhỏ hơn hoặc bằng giá trị được lưu trong bảng GIOIHAN.
– Một người dùng chỉ có thể xóa hoặc cập nhật dòng dữ liệu của chính họ.

Bài tập 8

Hãy cho một ví dụ cụ thể và vận dụng cơ chế MAC để kiểm chứng nguyên lý bảo vệ dữ liệu của cơ chế này? Hãy rút ra các nguyên tắc cơ bản giúp bạn hiểu và vận dụng được cơ chế MAC? Việc gán quyền và hủy bỏ quyền của một chủ thể trong cơ chế MAC được thực hiện như thế nào?

Bài tập 9

Xem bài giảng **Chương 2 – Các cơ chế điều khiển truy cập** phần **Cơ chế OLS (Oracle Label Security)**

Đối với từng trường hợp sau:

- Khi nhãn có 1 thành phần (Level).
- Khi nhãn có 2 thành phần (Level, Compartment).
- Khi nhãn có 3 thành phần (Level, Compartment, Group).

Hãy thực hiện các yêu cầu sau:

- Thống kê tất cả những nhãn dữ liệu và nhãn người dùng.
- Đối với từng nhãn người dùng, áp dụng thuật toán Đọc, cho biết họ có thể đọc được những dòng dữ liệu nào.
- Vận dụng cơ chế OLS (chưa cần cài đặt thực tế), trong từng trường hợp (3 trường hợp kể trên) hãy hiện thực chính sách bảo mật thể hiện thông qua hệ thống nhãn.