Bài thực hành số 11

ÔN TẬP

1. Một hệ thống dữ liệu lưu trữ thông tin của các vụ án được bảo mật bằng cách thiết lập một chính sách OLS. Các vụ án được phân loại theo các cấp độ bảo mật khác nhau: NATIONAL_SECURITY (liên quan đến an ninh quốc gia), SENSITIVE (đang trong quá trình xử lý), PUBLIC (đã xử lý và được công khai). Ngoài ra, tùy loại hình phạm tội mà các vụ án được phân chia thành 2 dạng: CIVIL (dân sự), CRIMINAL (hình sự). Liên quan đến những thông tin vụ án này, có người thuộc 3 nhóm DEFENSE (biện hộ), PROSECUTION (công tố), COURT(tòa án). Ba nhóm trên đều nằm dưới sự quản lý chung của nhóm ADMINISTRATION (giám sát).
   a. Tạo một chính sách bảo mật OLS có tên là "Judicial_OLS" với tên cột chữa nhãn dữ liệu là "Judicial_label".
   b. Cấp role và các quyền cần thiết để user sec_manager có thể toàn quyền quản lý chính sách "Judicial_OLS".
   c. Tạo các thành phần nhãn tương ứng với nghiệp vụ đã mô tả ở trên.
   d. Tạo các nhãn dữ liệu cho những loại dữ liệu sau:
      - Dữ liệu về các vụ án dân sự đã xử lý và được công bố rộng rãi. Mọi người đều có thể xem được.
      - Dữ liệu về các vụ án hình sự đang trong quá trình xử lý. Dữ liệu loại này được phân ra dữ liệu của bên phía khởi tố và của bên phía biện hộ.
      - Dữ liệu về các vụ án hình sự nghiêm trọng ảnh hưởng đến an ninh quốc gia. Dữ liệu loại này được phân thành dữ liệu của 3 bên riêng biệt: công tố, biện hộ và tòa án.
   e. Tạo tập xác thực quyền cho các nhóm nhân viên sau theo 2 cách (bằng cách tạo nhãn và bằng cách tạo các thành phần):
      - Nhân viên công tố chuyên phụ trách các vụ án dân sự thông thường (không ảnh hưởng an ninh quốc gia). Loại nhân viên này toàn quyền đọc và viết trên các dữ liệu liên quan. Tuy nhiên đối với các vụ án đã xử xong, nhân viên này không được quyền chính sửa.
      - Nhân viên công tố chuyên phụ trách các vụ án hình sự đặc biệt nghiêm trọng tầm

quốc gia. Nhân viên này toàn quyền đọc và viết trên các dữ liệu liên quan.

- Luật sư thuộc nhóm biện hộ cho các vụ án hình sự thông thường. Nhân viên này toàn quyền đọc nhưng không được viết trên các dữ liệu liên quan.
- Nhân viên thuộc nhóm giám sát phụ trách giám sát các vụ án dân sự và hình sự thông thường. Nhân viên loại này có quyền đọc nhưng không được phép chỉnh sửa các thông tin liên quan. Đối với những dữ liệu không liên quan đến các vụ án, nhân viên này có thể viết những thông tin có mức độ SENSITIVE hoặc PUBLIC.
- Nhân viên thuộc nhóm giám sát phụ trách giám sát các vụ hình sự nghiêm trọng cấp quốc gia. Nhân viên loại này có quyền đọc nhưng không được phép chỉnh sửa các thông tin liên quan. Đối với những dữ liệu không liên quan đến các vụ án, nhân viên này chỉ có thể viết những thông tin có mức độ NATIONAL_SECURITY.

2. Cho bảng có cấu trúc như sau thuộc schema của sec_manager:

   Employee (empno, ename, email, salary, deptno)

   Chi tiết:

   - empno (number) : mã số nhân viên
   - ename (varchar2) : tên nhân viên
   - email (varchar2) : email của nhân viên
   - salary (number): lương nhân viên
   - deptno (number) : mã số phòng ban của nhân viên

   Hãy dùng kỹ thuật ***Row-level Security*** bảo vệ cho bảng **employee** theo chính sách được mô tả dưới đây:

   - Nhân viên thuộc phòng ban này không được phép xem hay chỉnh sửa bất kỳ thông tin nào của những nhân viên thuộc phòng ban khác.
   - Các nhân viên được phép xem (select) các thông tin của những người trong cùng phòng ban.
   - Nhân viên không được phép insert/delete trên bảng.
   - Nhân viên chỉ có thể update thông tin email của bản thân mình. Những thông tin cá nhân còn lại không được phép chỉnh sửa.

   Lưu ý:

   - Tên của nhân viên (ename) chính là username mà nhân viên đó dùng để log in vào hệ

thống. (Sinh viên có thể dùng hàm USER trả về username của người dùng hiện tại)

- Sinh viên phải viết cả policy function và các lệnh gán policy function cho table **employee**.
- Sinh viên có thể viết 1 hay nhiều policy function để hiện thực chính sách trên.
- Các *policy function* tạo ra thuộc schema của user sec_manager và user sec_manager là người gán các policy function cho *employee*.

3. Cho bảng có cấu trúc như sau thuộc schema của sec_manager:

   Employee (empno, ename, email , salary, deptno, manager)

   Chi tiết:

   - empno (number) : mã số nhân viên
   - ename (varchar2) : tên nhân viên
   - email (varchar2) : email của nhân viên
   - salary (number): lương nhân viên
   - deptno (number) : mã số phòng ban của nhân viên
   - manager(number): mã số người quản lý của phòng ban mà nhân viên thuộc về

   Hãy dùng kỹ thuật ***Row-level Security*** bảo vệ cho bảng **employee** theo chính sách được mô tả dưới đây:

   - Nhân viên hay quản lý thuộc phòng ban này không được phép xem hay chỉnh sửa bất kỳ thông tin nào của những nhân viên thuộc phòng ban khác.
   - Nhân viên thuộc phòng ban nào chỉ được xem (*select*) thông tin của các nhân viên thuộc cùng phòng ban với mình ngoại trừ lương (*salary*). Mỗi nhân viên chỉ có thể xem lương của bản thân họ.
   - Nhân viên không có quyền chỉnh sửa (*insert, update, delete*) bất cứ thông tin gì, kể cả thông tin của chính nhân viên đó.
   - Chỉ có người quản lý từng phòng ban được phép *select, insert, update, delete* tất cả các thông tin của các nhân viên thuộc phòng ban mình quản lý.

   Lưu ý:

   - Tên của nhân viên (ename) chính là username mà nhân viên đó dùng để log in vào hệ thống. (Sinh viên có thể dùng hàm USER trả về username của người dùng hiện tại)
   - Sinh viên phải viết cả policy function và các lệnh gán policy function cho table

employee.

- Sinh viên có thể viết 1 hay nhiều policy function để hiện thực chính sách trên.
- Các *policy function* tạo ra thuộc schema của user sec_manager và user sec_manager là người gán các policy function cho *employee*.