**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

Nhóm thực hiện: Nhóm 18

|  |  |
| --- | --- |
| 18120564 | Lâm Hồng Thành |
| 20120269 | Võ Văn Minh Đoàn |
| 20120542 | Trịnh Thị Tuyết Nhung |
| 20120590 | Nguyễn Trọng Thuận |

GV phụ trách: Thầy Lương Vĩ Minh, cô Phạm Thị Bạch Huệ, cô Tiết Gia Hồng

  AN TOÀN & BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

HỌC KỲ II – NĂM HỌC 2022 - 2023

**Báo cáo đồ án môn học**

**AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH,**

Logo

Description automatically generated**ĐẠI HỌC QUỐC GIA TP HCM**

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mã nhóm:** | **Nhóm 18** | | | |
| **Số lượng:** | **4** | | | |
| **MSSV** | **Họ tên** | **Email** | **Điện thoại** | **Nhóm trưởng** |
| 18120564 | Lâm Hồng Thành | 18120564@student.hcmus.edu.vn |  | x |
| 20120269 | Võ Văn Minh Đoàn | 20120269@student.hcmus.edu.vn |  |  |
| 20120542 | Trịnh Thị Tuyết Nhung | 20120542@student.hcmus.edu.vn |  |  |
| 20120590 | Nguyễn Trọng Thuận | 20120590@student.hcmus.edu.vn |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bảng phân công & đánh giá hoàn thành công việc** | | | |
| **PHÂN HỆ 1** | | | |
| **Công việc thực hiện** | **Người thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| * Viết procedure xem danh sách người dùng, Thông tin về quyền của User/Role, Tạo User mới. * Tạo form chức năng: Xem danh sách người dùng trong hệ thống, Xem thông tin về quyền của User/Role, Login, Main. * Làm báo cáo. | 18120564 – Lâm Hồng Thành | 100% | 10/10 |
| * Viết procedure tạo User mới, xóa User/Role, Hiệu chỉnh User, Tạo Role mới. * Tạo form chức năng: Tạo mới, xóa, hiệu chỉnh user; Tạo, xoá role, Kết nối Oracle Database to C#. * Quay video đề mô. | 20120590 – Nguyễn Trọng Thuận | 100% | 10/10 |
| * Viết procedure cấp quyền cho User/Role trên hệ thống và đối tượng, Cấp Role cho User, Kiểm tra quyền của User/Role. * Tạo form chức năng: Cấp quyền của User/ Role trên hệ thống và đối tượng, Gán Role cho User/Role, Kiểm tra quyền của User/Role. | 20120269 – Võ Văn Minh Đoàn | 100% | 10/10 |
| * Viết procedure thu hồi quyền của User/Role trên hệ thống và đối tượng, Chỉnh sửa quyền của User/Role. * Tạo form chức năng: Thu hồi quyền từ User/ Role trên hệ thống và đối tượng, Chỉnh sửa quyền của User/Role. * Làm báo cáo. | 20120542 – Trịnh Thị Tuyết Nhung | 100% | 10/10 |
| **PHÂN HỆ 2** | | | |
| * Thực hiện CS#1 * Làm giao diện CS#1 * Cài đặt chính sách audit | 18120564 – Lâm Hồng Thành | 100% | 10/10 |
| * Thực hiện CS#2, CS#5 * Làm giao diện CS#2, CS#5 * Cài đặt chính sách OLS | 20120590 –  Nguyễn Trọng Thuận | 100% | 10/10 |
| * Thực hiện CS#3 * Làm giao diện CS#3 * Cài đặt chính sách Encryption * Backend, kết nối database | 20120269 – Võ  Văn Minh Đoàn | 100% | 10/10 |
| * Thực hiện CS#4, CS#6 * Làm giao diện CS#4, CS#6 * Cài đặt chính sách OLS * Làm báo cáo | 20120542 – Trịnh  Thị Tuyết Nhung | 100% | 10/10 |

Mục Lục

[PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU 5](#_Toc139101517)

[I. Lý thuyết 6](#_Toc139101518)

[1. Người dùng (User) 6](#_Toc139101519)

[2. Vai trò (Role) 6](#_Toc139101520)

[3. Khung nhìn (View) 7](#_Toc139101521)

[4. Quyền người dùng (Privilege) 9](#_Toc139101522)

[II. Triển khai cài đặt danh sách chức năng 10](#_Toc139101523)

[1. Xem danh sách User trong hệ thống: 10](#_Toc139101524)

[5. Thông tin về quyền của User/Role: 11](#_Toc139101525)

[6. Tạo User mới: 12](#_Toc139101526)

[7. Xoá User / Role: 14](#_Toc139101527)

[8. Hiệu chỉnh User: 16](#_Toc139101528)

[9. Tạo Role mới: 18](#_Toc139101529)

[10. Cấp quyền cho User/Role: 19](#_Toc139101530)

[a. Cấp quyền hệ thống 19](#_Toc139101531)

[b. Cấp quyền đối tượng 19](#_Toc139101532)

[11. Cấp Role cho User: 20](#_Toc139101533)

[12. Thu hồi quyền từ User / Role 22](#_Toc139101534)

[a. Thu hồi quyền hệ thống 22](#_Toc139101535)

[b. Thu hồi quyền đối tượng 22](#_Toc139101536)

[13. Kiểm tra quyền của User / Role 24](#_Toc139101537)

[14. Chỉnh sửa quyền của User / Role 25](#_Toc139101538)

[PHÂN HỆ 2: XÂY DỰNG HỆ THỐNG ĐỂ QUẢN LÝ THÔNG TIN NHÂN VIÊN VÀ VIỆC THAM GIA ĐỀ ÁN CỦA NHÂN VIÊN. 28](#_Toc139101539)

[I. Mô hình cơ sở dữ liệu 28](#_Toc139101540)

[II. Ràng buộc toàn vẹn 28](#_Toc139101541)

[III. Xác định và phân quyền các loại người dùng 28](#_Toc139101542)

[IV. Các chính sách bảo mật 30](#_Toc139101543)

[1. Chính sách DAC 30](#_Toc139101544)

[2. Chính sách RBAC 30](#_Toc139101545)

[3. Chính sách VPD 31](#_Toc139101546)

[4. Chính sách OLS 39](#_Toc139101547)

[5. Chính sách Encryption 43](#_Toc139101548)

[6. Chính sách Audit 47](#_Toc139101549)

[a. Kích hoạt audit toàn hệ thống 48](#_Toc139101550)

[b. Tắt audit 49](#_Toc139101551)

[c. Standard audit 50](#_Toc139101552)

[d. Fine-grained audit 50](#_Toc139101553)

[V. Tài liệu tham khảo 53](#_Toc139101554)

**YÊU CẦU ĐỒ ÁN**

|  |  |
| --- | --- |
| **Loại bài tập** | **Lý thuyết 🗹 Thực hành 🗹 Đồ án Bài tập** |
| **Ngày bắt đầu** | **29/03/2023** |
| **Ngày kết thúc** | **09/03/2023** |

# PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU

Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc sau:

- Xem danh sách người dùng trong hệ thống.

- Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.

- Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.

- Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role,

cấp role cho user. Quá trình cấp quyền có tùy chọn là có cho phép người được

cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không). Quyền, select, update thì cho phép phân quyền

tinh đến mức cột; quyền insert, delete thì không.

- Cho phép thu hồi quyền từ người dùng/ role.

- Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.

- Cho phép chỉnh sửa quyền của user/ role.

# Lý thuyết

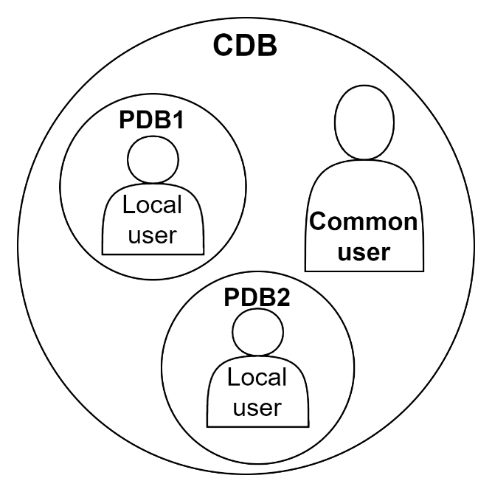
## *Người dùng (User)*

Trong Oracle, user là một tài khoản được tạo để cho phép người dùng truy cập vào cơ sở dữ liệu. Mỗi user có một tên đăng nhập và một mật khẩu riêng để đăng nhập vào hệ thống. Các quyền truy cập và quyền hạn của user được xác định bởi quản trị viên hệ thống hoặc người quản lý cơ sở dữ liệu.

Một user có thể được phép truy cập vào một số bảng hoặc chế độ xem cụ thể, cũng như có thể được phép thực hiện các hoạt động như tạo bảng, thêm dữ liệu hoặc thực hiện các thủ tục lưu trữ. Các user cũng có thể được gán các vai trò và quyền hạn để kiểm soát việc truy cập cơ sở dữ liệu và các tài nguyên.

Oracle lưu trữ cơ sở dữ liệu trong một **CDB** (Container database hay Root) lớn để quản lý tất cả dữ liệu, trong CDB có chứa các **PDB** (Pluggable database), PDB chứa các lược đồ, dữ liệu của riêng nó.

Trong Oracle, có 2 loại user là Common user và Local user:



(Mô tả common user và local user trong Oracle)

* **Common user**: Có thể sử dụng tài nguyên trên toàn bộ CDB (toàn bộ CSDL), tên người dùng phải bắt đầu bằng kí tự “C##” và không được trùng nhau.
* **Local user**: Chỉ có thể sử dụng tài nguyên ở 1 PDB nó thuộc về, tên user có thể khác nhau nếu không cùng PDB.

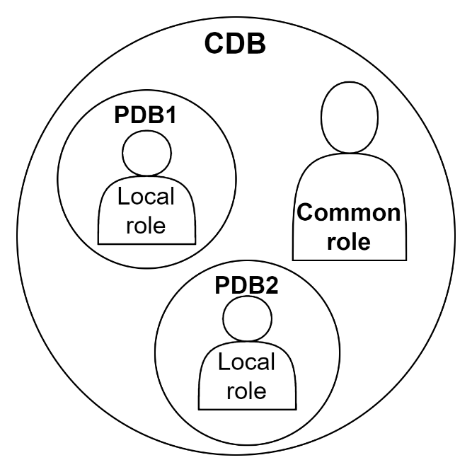
Trong Oracle, **1 user tương ứng 1 schema**, chứa tất cả những đối tượng (table, view, procedure) của riêng schema đó, những đối tượng khác schema có thể khác tên.

Ví dụ ta có 1 user C##NHOM1 thì tuong ứng ta sẽ có 1 schema C##NHOM1, ta có thể tạo các đối tượng trên shema (sử dụng toán tử ‘.’ để truy cập vào các đối tượng), chẳng hạn C##NHOM1.BANG\_1, C##NHOM1.KHUNG\_NHIN\_1.

## *Vai trò (Role)*

Trong Oracle, role là một tập hợp các quyền hoặc đặc quyền được gán cho một tài khoản người dùng hoặc một tập hợp các tài khoản người dùng. Role cung cấp một cách tiện lợi để quản lý quyền và phân quyền trong cơ sở dữ liệu Oracle.

Một role có thể được tạo để đại diện cho một nhóm đối tượng hoặc để cung cấp truy cập cho một tập hợp các đối tượng cụ thể trong cơ sở dữ liệu. Khi một role được gán cho một tài khoản người dùng, tài khoản đó được cấp quyền hoặc đặc quyền tương ứng với role đó.

Tương tự như user, role cũng có 2 loại là **Common role** (có thể truy cập trên CDB, tên phải bắt đầu là “C##”) và **Local role** (chỉ được truy cập PDB của mình).

(Mô tả common role và local role trong Oracle)

## *Khung nhìn (View)*

Trong Oracle, khung nhìn (view) là một đối tượng cơ sở dữ liệu ảo, nó là kết quả của một truy vấn trên các bảng hoặc khung nhìn khác trong cơ sở dữ liệu. Khung nhìn được lưu trữ trong cơ sở dữ liệu nhưng không chứa bất kỳ dữ liệu nào, mà chỉ chứa các câu lệnh truy vấn để lấy dữ liệu từ các bảng hoặc khung nhìn khác.

Khung nhìn cung cấp một cách tiện lợi để truy vấn dữ liệu từ nhiều bảng mà không cần phải thao tác trên các bảng trực tiếp. Chúng ta có thể sử dụng khung nhìn để giới hạn quyền truy cập vào dữ liệu hoặc để ẩn thông tin nhạy cảm trong cơ sở dữ liệu. Khung nhìn có thể được sử dụng như một bảng trong các truy vấn SELECT, INSERT, UPDATE và DELETE.

Ví dụ:Tạo view để xem thông tin giáo viên thuộc bộ môn HTTT

CREATE VIEW GIAOVIEN\_HTTT AS

SELECT \* FROM GIAOVIEN

WHERE MABM = ‘HTTT’;

Thực chất, View trong Oracle chỉ là những câu truy vấn đã được xác thực được lưu lại trong data dictionary.

*Ảnh có chứa văn bản

Mô tả được tạo tự động*

(Cách Oracle lưu view)

Bên cạnh việc tăng hiệu năng truy vấn. Thì mục đích chính của việc dùng View là để thực hiện các chính sách bảo mật trong CSDL.

* **Bảo vệ dữ liệu mức dòng:** ta dùng điều kiện WHERE để loại những dòng dữ liệu cần bảo vệ khỏi View. Chẳng hạn, ta tạo View để truy vấn thông tin nhân viên kế toán (KT), những nhân viên khác sẽ không được xem

CREATE VIEW NHAN\_VIEN\_NHANSU AS

SELECT \* FROM NHANVIEN

**WHERE LOAINV = ‘NHÂN SỰ’;**

* **Bảo vệ dữ liệu mức cột**: ta có thể chọn ra những cột dữ liệu cần thiết cho View và ẩn những cột còn lại đi. Chẳng hạn, ta tạo View để truy vấn thông mã nhân viên và họ tên nhân viên, các trường còn lại (ngày sinh, số CMND, lương, …) sẽ bị ẩn đi khỏi View.

CREATE VIEW THONGTINNHANVIEN AS

**SELECT MANV, HOTEN**

FROM NHANVIEN;

## *Quyền người dùng (Privilege)*

Trong Oracle, quyền người dùng(privilege) là một khái niệm quan trọng liên quan đến việc quản lý cơ sở dữ liệu và đảm bảo tính bảo mật của hệ thống. Quyền người dùng là những đặc quyền được cấp cho người dùng để thực hiện các thao tác trên các đối tượng trong cơ sở dữ liệu như bảng, khung nhìn, thủ tục, package và chức năng.

Có 2 loại quyền trong Oracle:

* **Quyền hệ thống (System privilege):** Cho phép người dùng thực hiện hành động trên đối tượng (table, view, index, …) của **bất kì schema nào**. Loại quyền này chỉ nên cấp cho những user có độ tin cậy và quyền hành cao.

Ảnh có chứa văn bản

Mô tả được tạo tự động

*(Ví dụ 1 số quyền hệ thống. Nguồn:* [*Privileges (oracle.com)*](https://docs.oracle.com/database/121/TTSQL/privileges.htm#TTSQL339)*)*

* **Quyền đối tượng (Object privilege):** Cho phép 1 user có thể thực hiện hành động hoặc truy cập vào các **đối tượng của 1 user khác** (schema khác). **User sẽ có toàn bộ quyền đối tượng trên schema của mình**

Ảnh có chứa văn bản

Mô tả được tạo tự động

*(Ví dụ 1 số quyền đối tượng. Nguồn:* [*Privileges (oracle.com)*](https://docs.oracle.com/database/121/TTSQL/privileges.htm#TTSQL339)*)*

Cú pháp câu lệnh cấp quyền**:**

**GRANT <PRIVILLEGE> ON <OBJECT> TO <USER>**

(với những câu lệnh có mức cột thì privilege cần có thêm thông tin cột)

Ví dụ:

**GRANT UPDATE (COLUMN\_1, COLUMN\_2) ON ANOTHER.TABLE\_TEST TO USER\_TEST**: cấp quyền UPDATE trên các cột COLUMN\_1, COLUMN\_2 của bảng TABLE\_TEST thuộc schema ANOTHER cho user USER\_TEST.

Cú pháp câu lệnh thu hồi quyền đã cấp:

**REVOKE <PRIVILLEGE> ON <OBJECT> FROM <USER>**

(khi thu hồi chỉ thu hồi toàn bộ quyền, không thu hồi trên chi tiết từng cột)

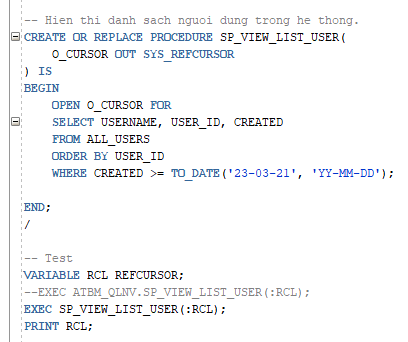
Ví dụ:

**REVOKE UPDATE ON ANOTHER.TABLE\_TEST FROM USER\_TEST**: Đây là câu lệnh đúng, tiến hành thu hồi quyền UPDATE trên bảng TABLE\_TEST thuộc shema ANOTHER của user USER\_TEST.

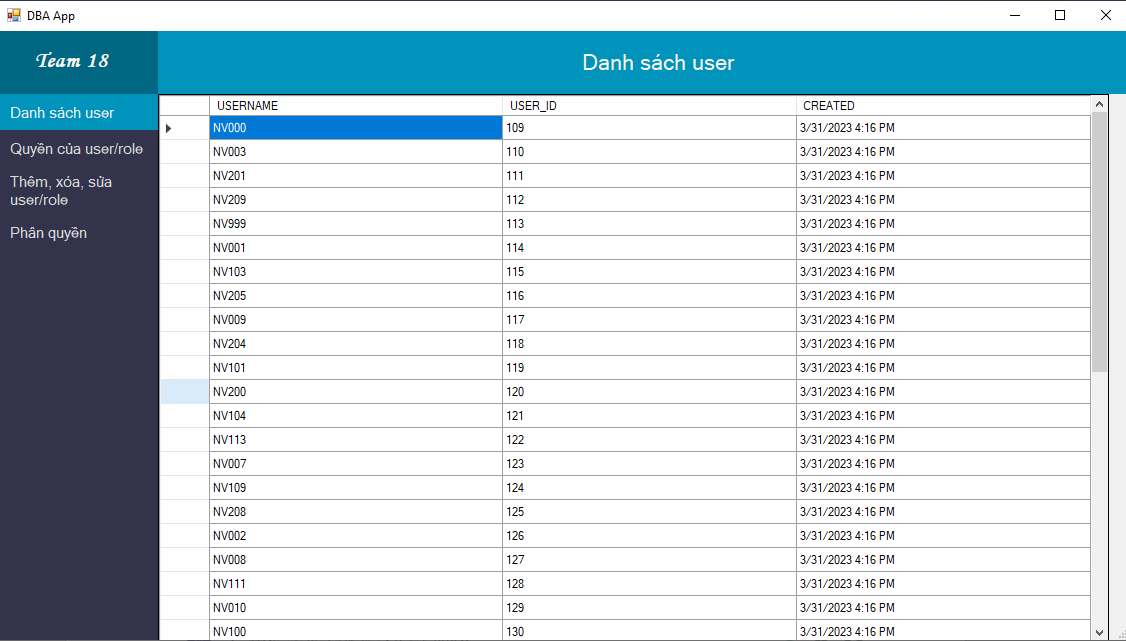
# Triển khai cài đặt danh sách chức năng

## Xem danh sách User trong hệ thống:

Cài đặt procedure hiển thị danh sách người dùng trong hệ thống: chức năng này cho phép quản trị viên xem tất cả các User tồn tại trong hệ thống với thông tin là các User được tạo từ sau ngày 21/03/2023.



Kết quả của chương trình sau khi cài đặt procedure:

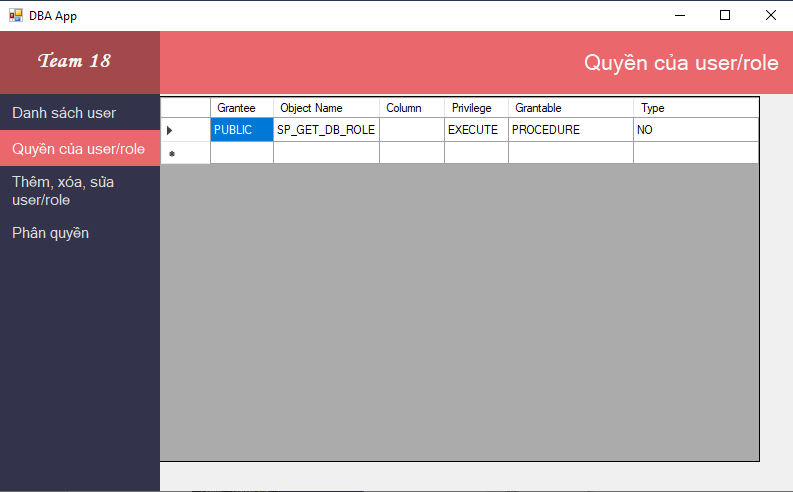


## Thông tin về quyền của User/Role:

Cài đặt procedure hiển thị thông tin về quyền của User/Role: chức năng cho phép hiển thị tất cả những quyền mà người quản trị hệ thống tạo ra.

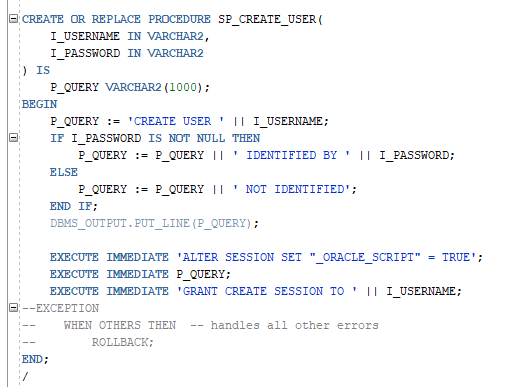


Kết quả hiển thị của chương trình sau khi cài đặt procedure:

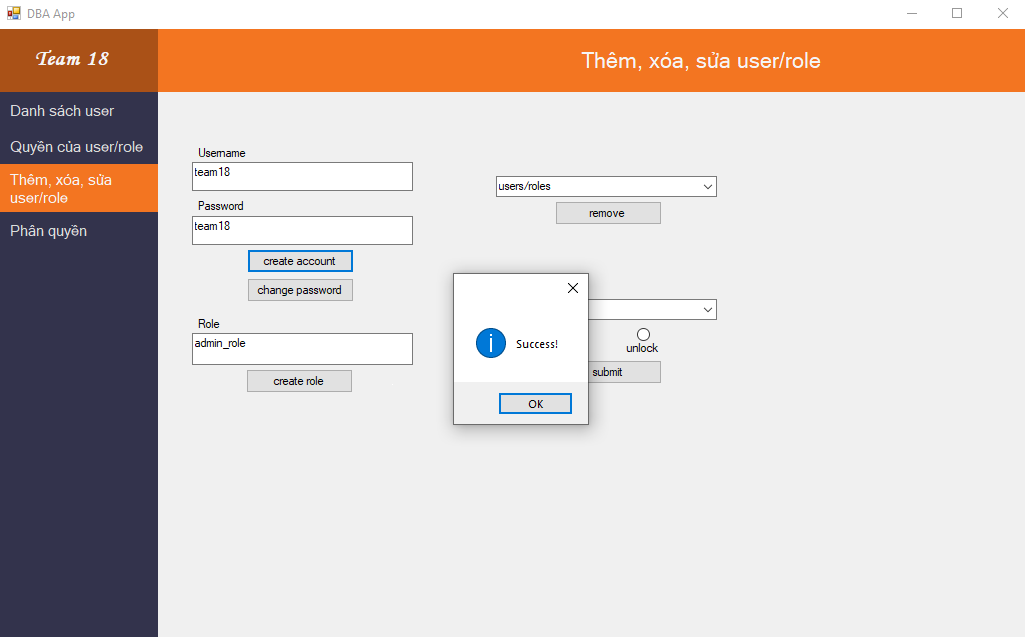


## Tạo User mới:

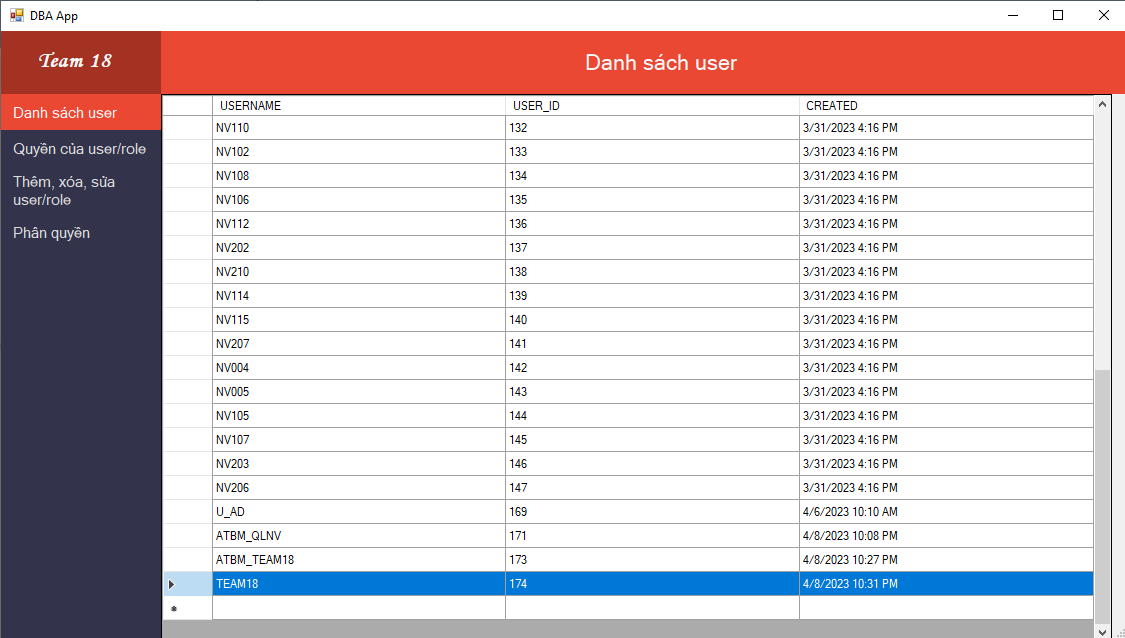
Cài đặt procedure tạo User mới: chức năng này cho phép người quản trị viên tạo ra một User mới trong hệ thống để cấp cho người dùng.



Kết quả hiển thị của chương trình sau khi cài đặt procedure:

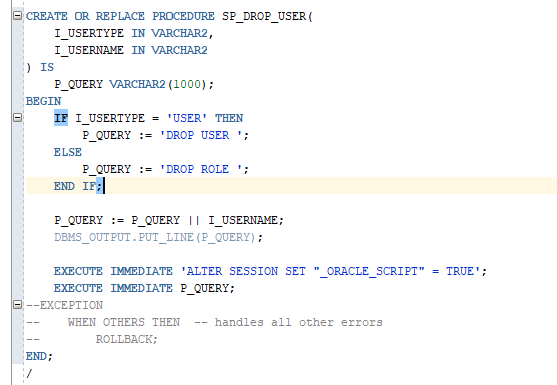


Tra cứu Danh sách User ta thấy User “team18” đã được thêm vào cơ sở dữ liệu:

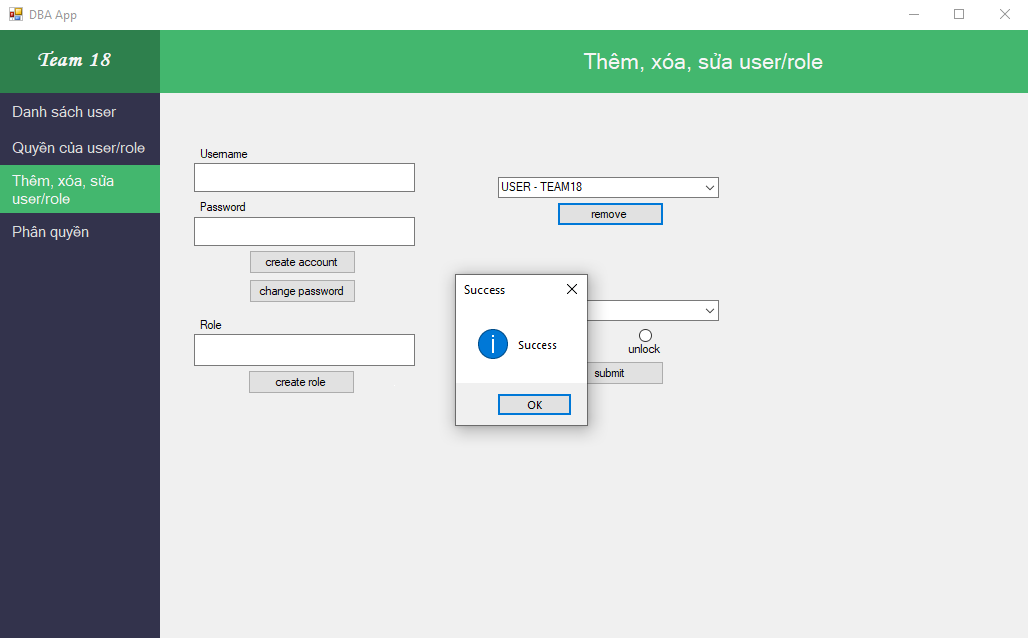


## Xoá User / Role:

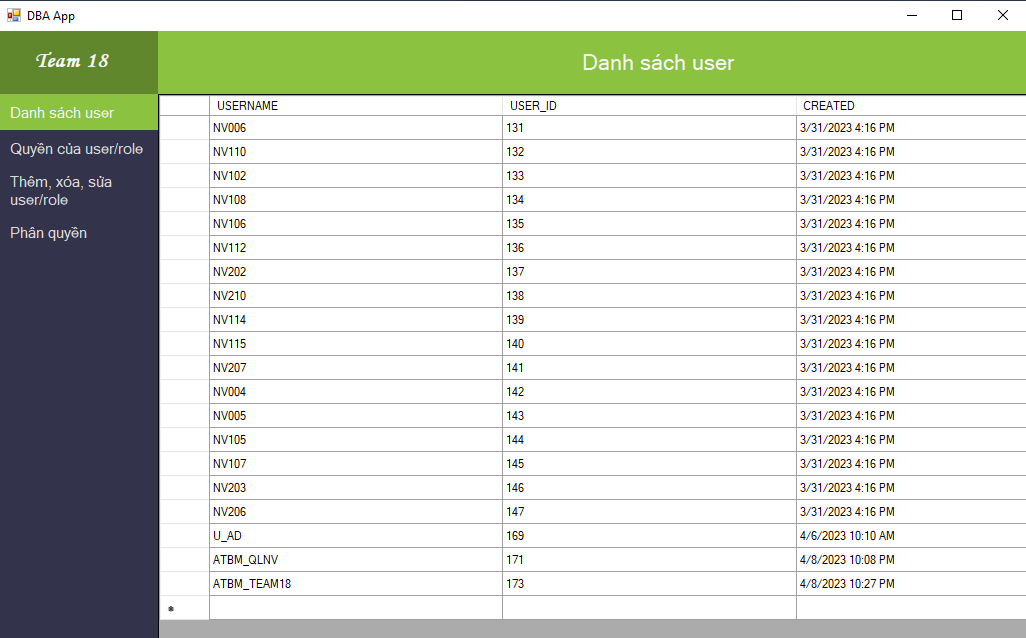
Cài đặt procedure xóa User / Role: chức năng này cho phép người quản trị xóa đi User/Role đã tồn tại trong hệ thống.



Kết quả hiển thị của chương trình sau khi cài đặt procedure:



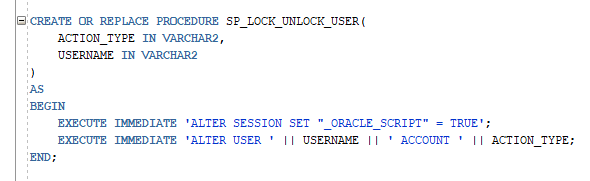
Tra cứu Danh sách User ta thấy User “team18” đã được xóa khỏi cơ sở dữ liệu:



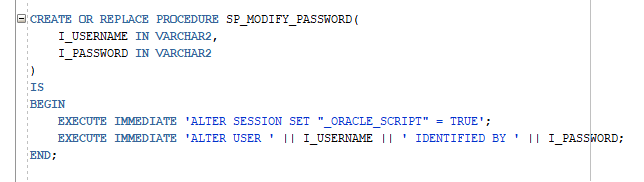
## Hiệu chỉnh User:

Cài đặt procedure hiệu chỉnh User: chức năng này cho phép người quản trị viên thay đổi mật khẩu của User hoặc có thể Lock/Unlock một tài khoản

* Lock / Unlock User:

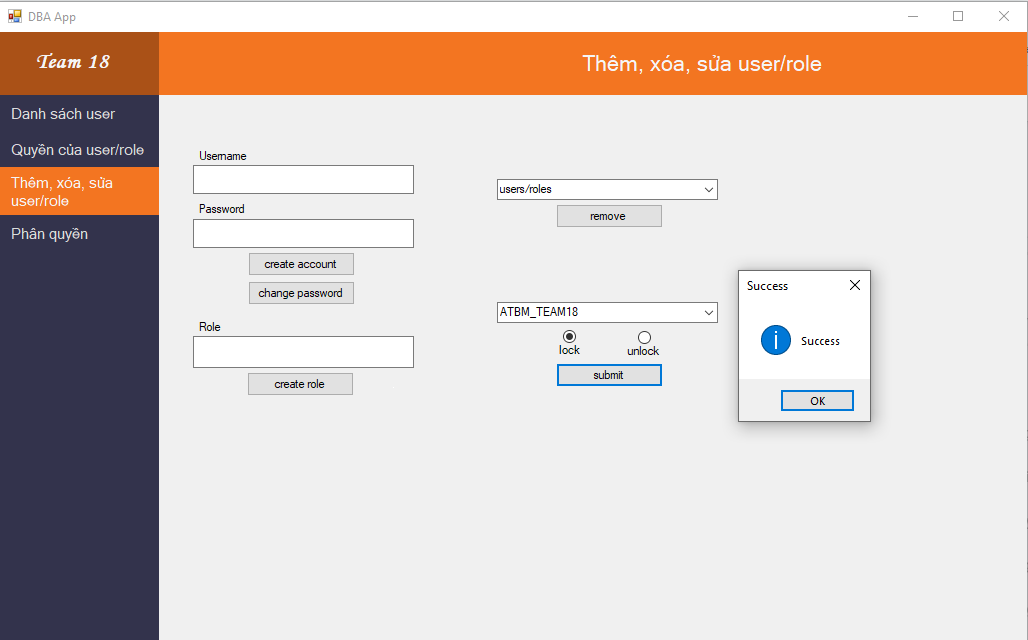


* Change password:

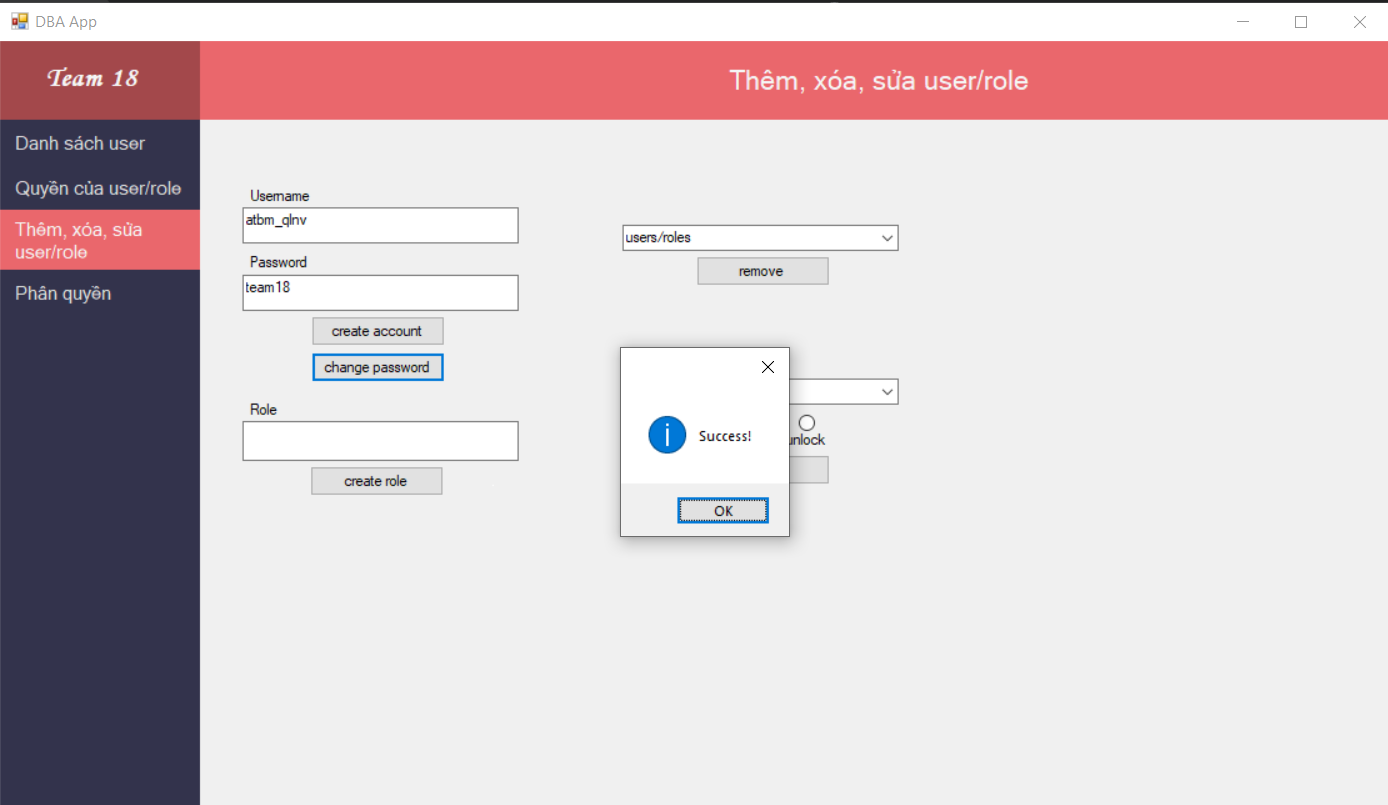


Kết quả hiển thị của chương trình sau khi cài đặt procedure:

* Lock / Unlock User:

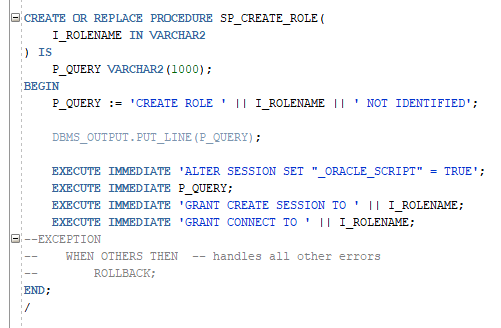


* Change password User:

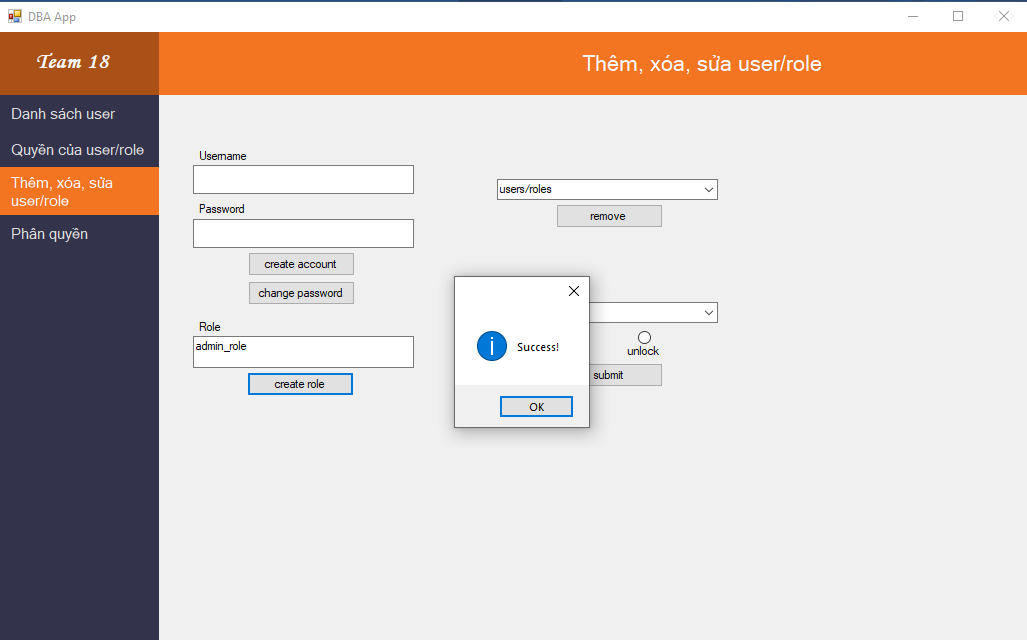


## Tạo Role mới:

Cài đặt procedure tạo Role mới: chức năng này cho phép quản trị viên tạo một Role mới cho hệ thống



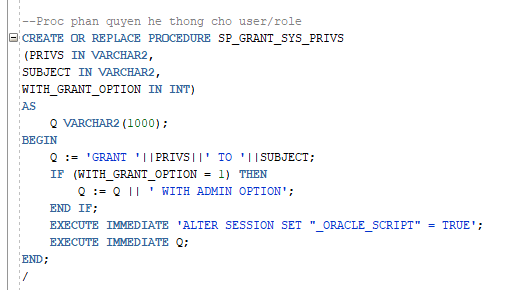
Kết quả hiển thị của chương trình sau khi cài đặt procedure:



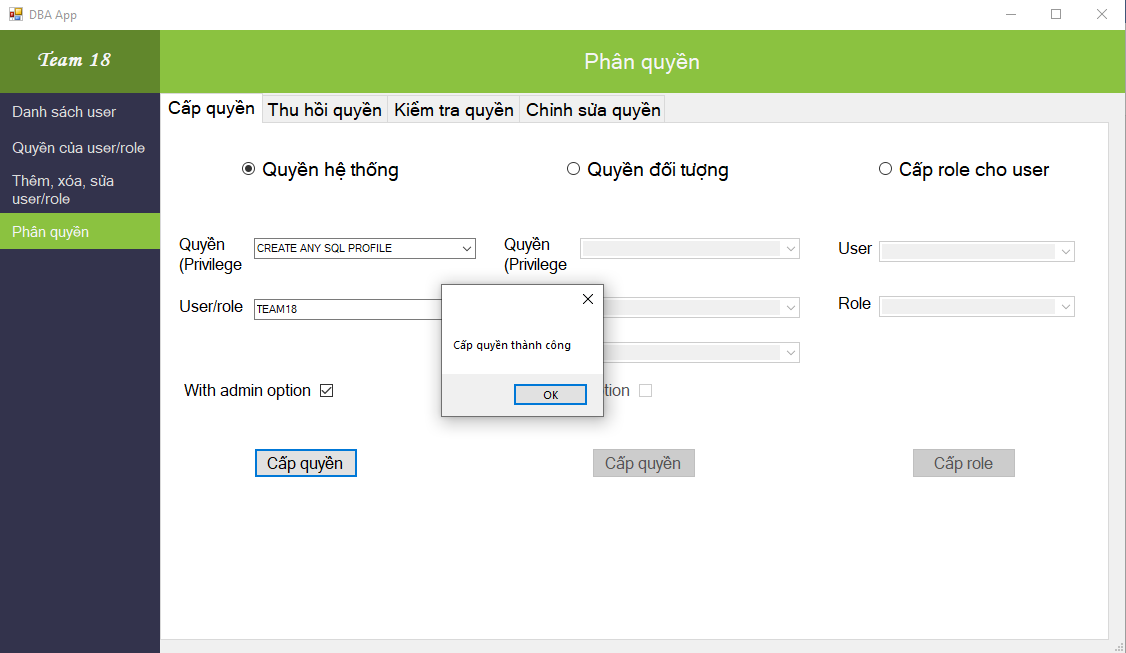
## Cấp quyền cho User/Role:

### Cấp quyền hệ thống

Cài đặt procedure cấp quyền hệ thống cho User / Role:

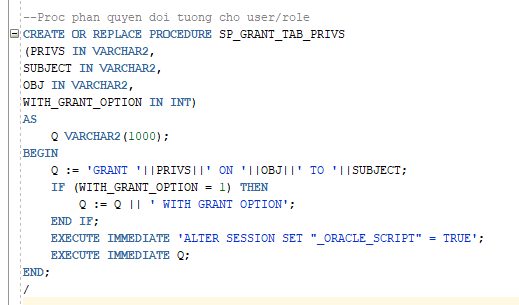


Kết quả hiển thị của chương trình sau khi cài đặt procedure:

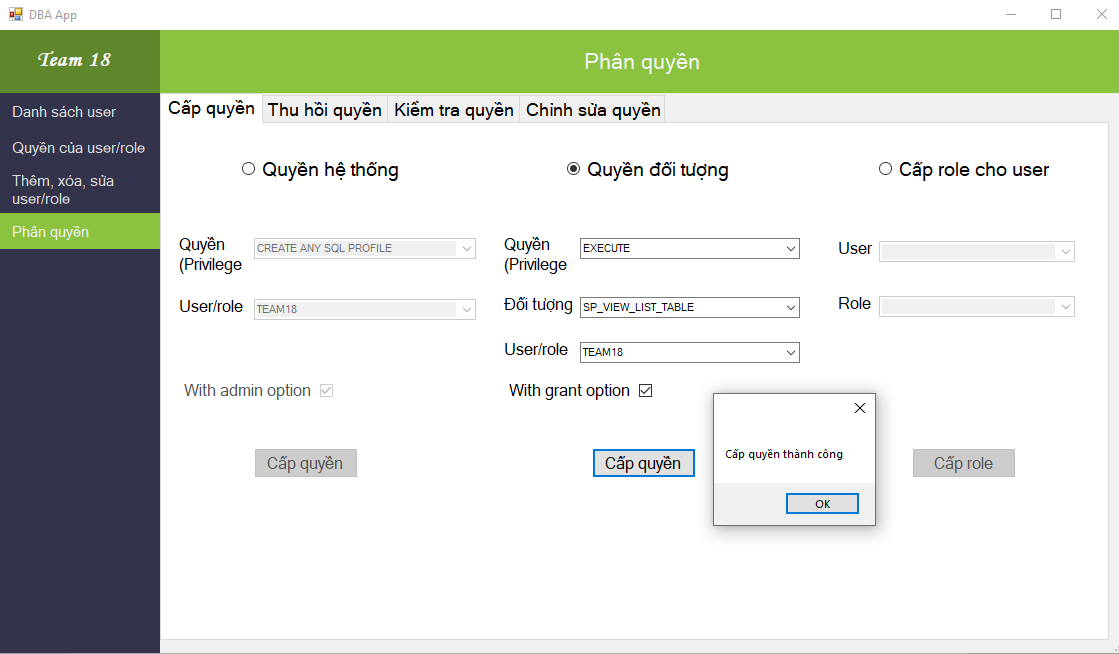


### Cấp quyền đối tượng

Cài đặt procedure cấp quyền đối tượng cho User / Role:

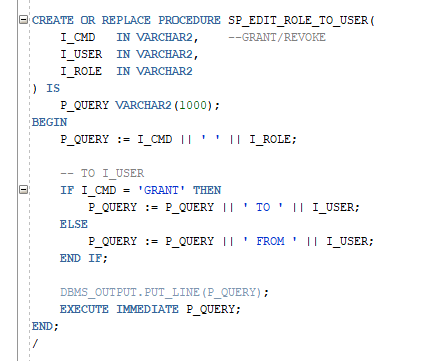


Kết quả hiển thị của chương trình sau khi cài đặt procedure:

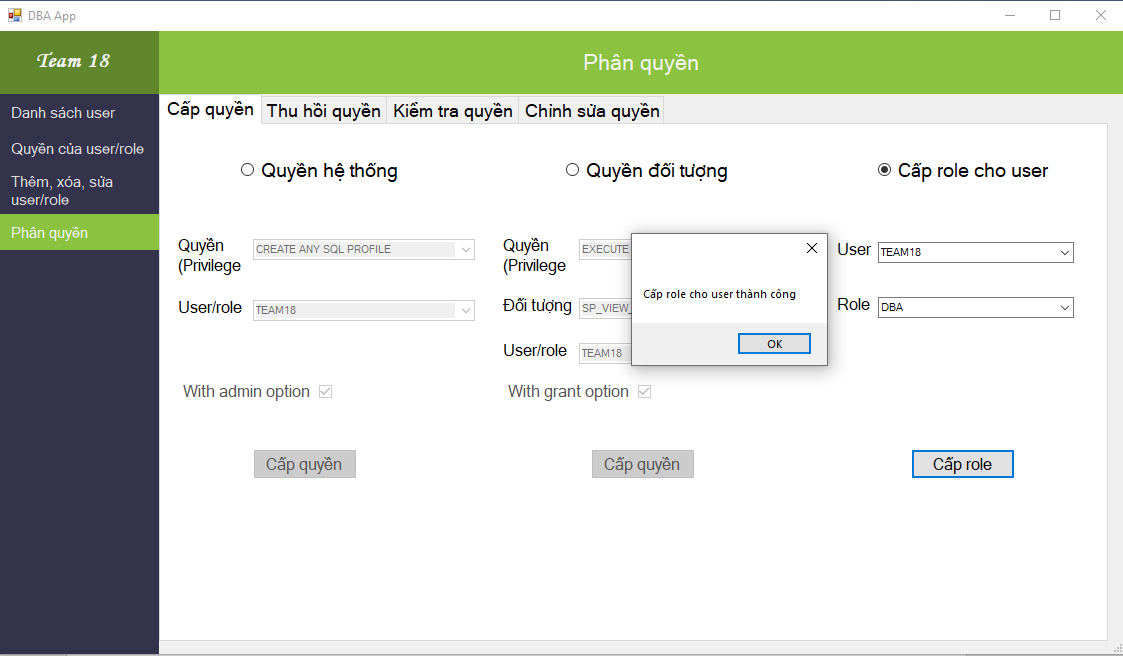


## Cấp Role cho User:

Cài đặt procedure cấp Role cho User:



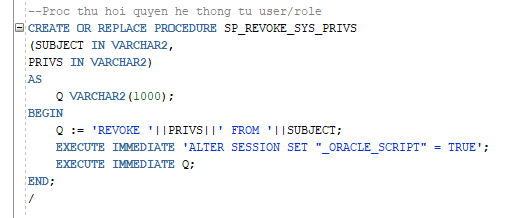
Kết quả hiển thị của chương trình sau khi cài đặt procedure:

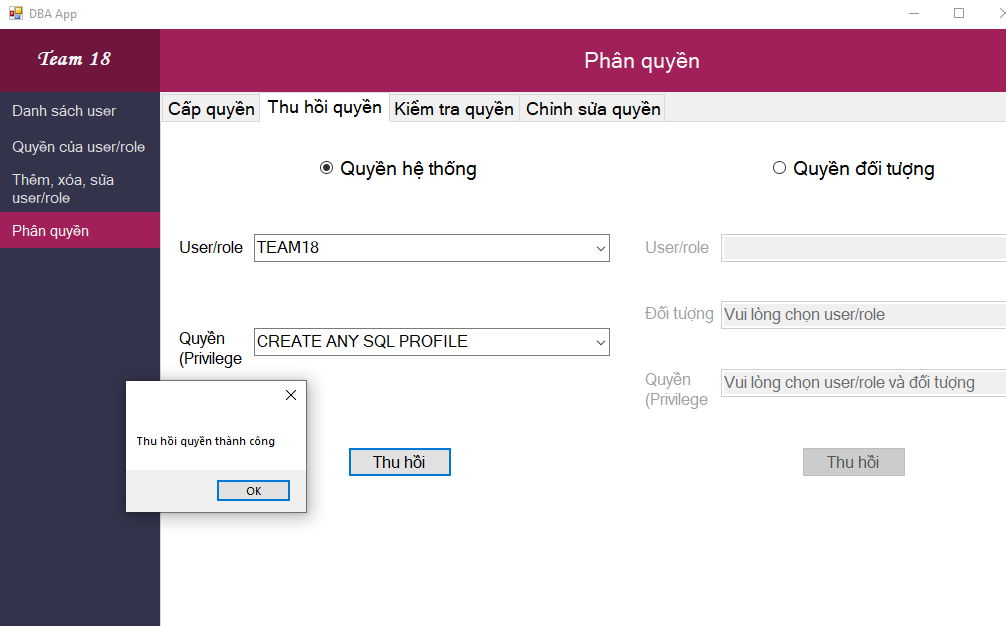


## Thu hồi quyền từ User / Role

### Thu hồi quyền hệ thống

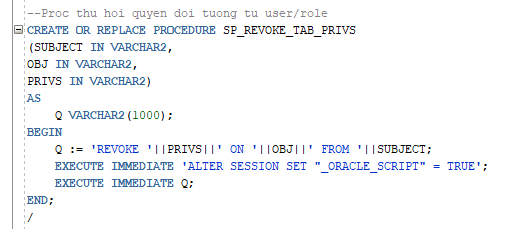
Cài đặt procedure thu hồi quyền hệ thống của User / Role:



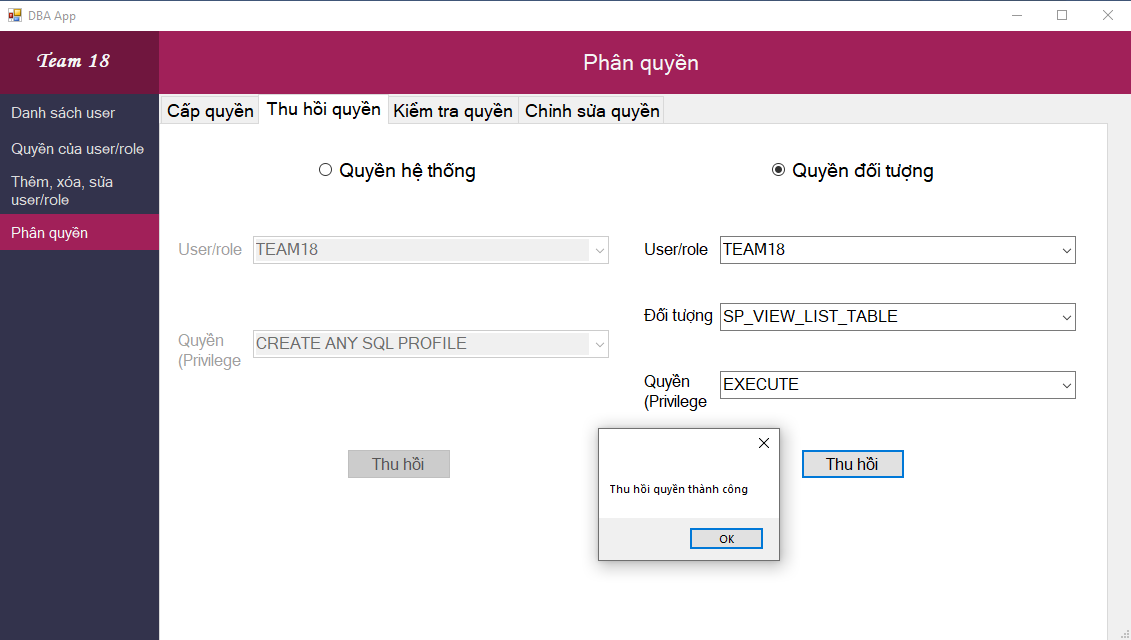


### Thu hồi quyền đối tượng

Cài đặt procedure thu hồi quyền đối tượng của User / Role:



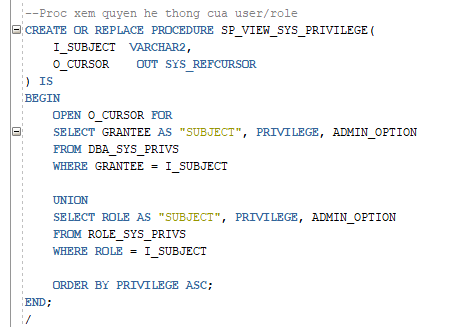
Kết quả hiển thị của chương trình sau khi cài đặt procedure:



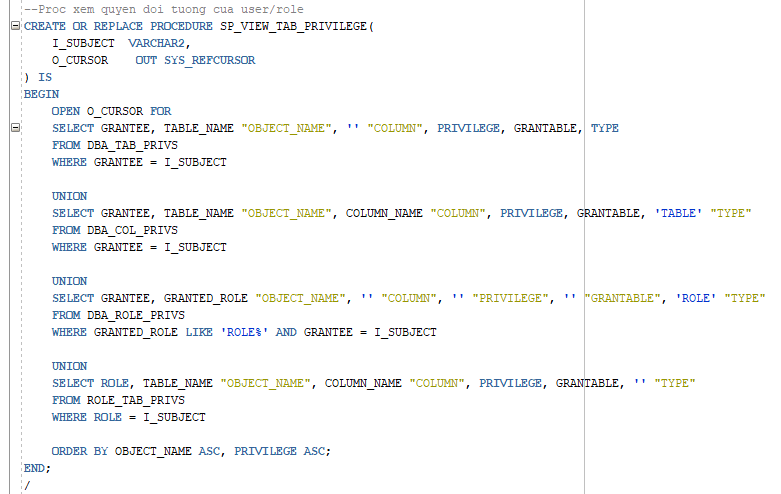
## Kiểm tra quyền của User / Role

Cài đặt procedure kiểm tra quyền của User / Role:

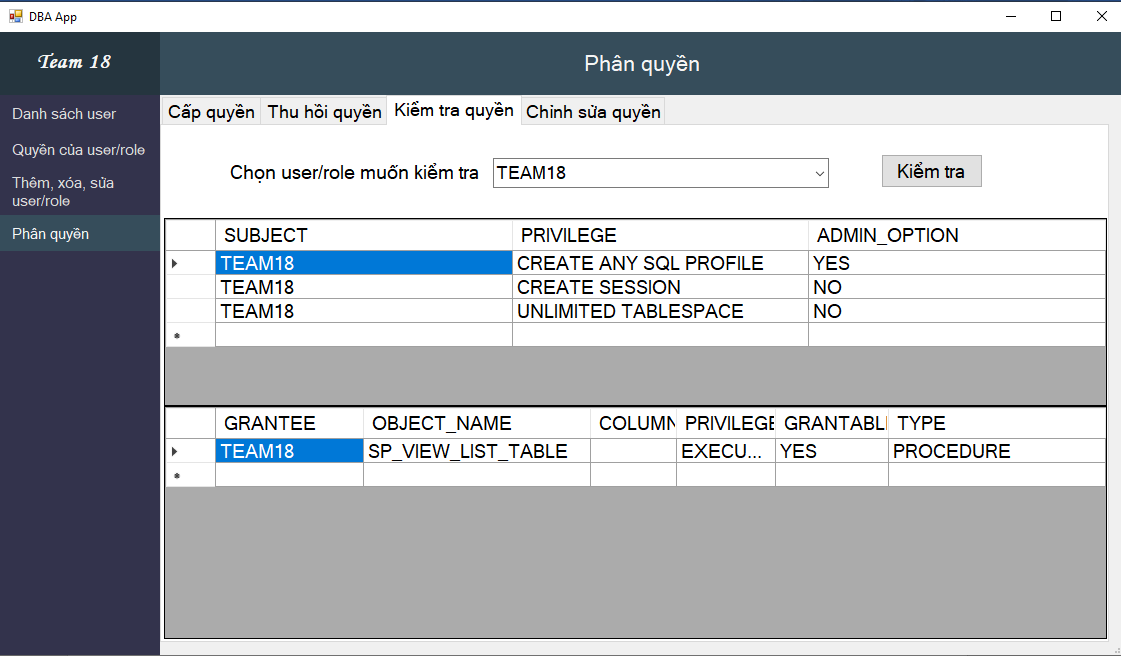
* Procedure xem quyền hệ thống của User / Role:



* Procedure xem quyền đối tượng của User / Role:

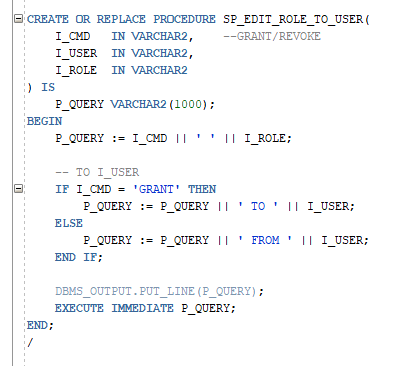


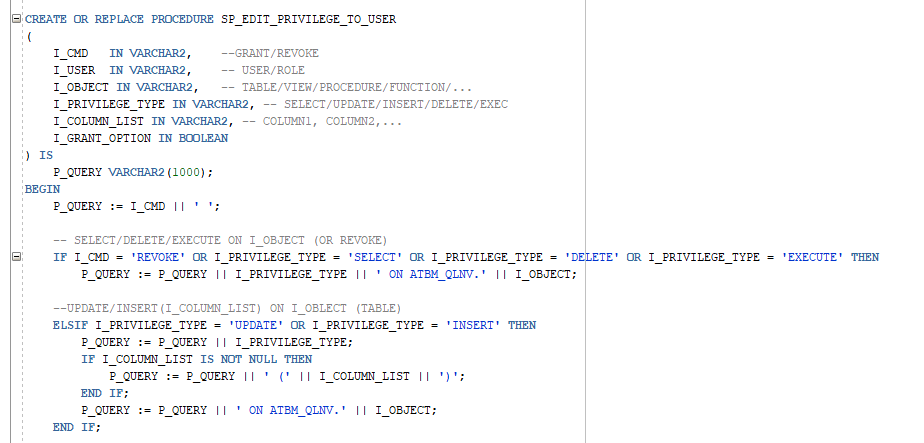
Kết quả hiển thị của chương trình sau khi cài đặt procedure:

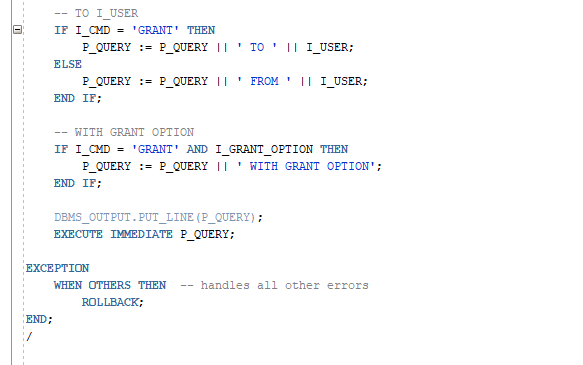


## Chỉnh sửa quyền của User / Role

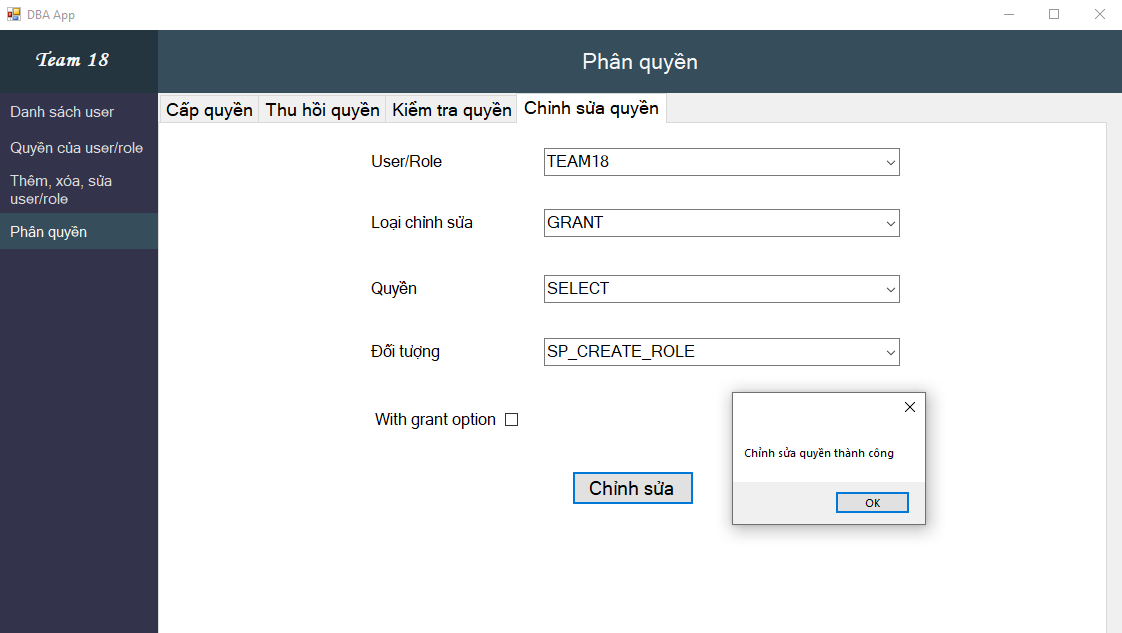
Cài đặt procedure chỉnh sửa quyền của User / Role:





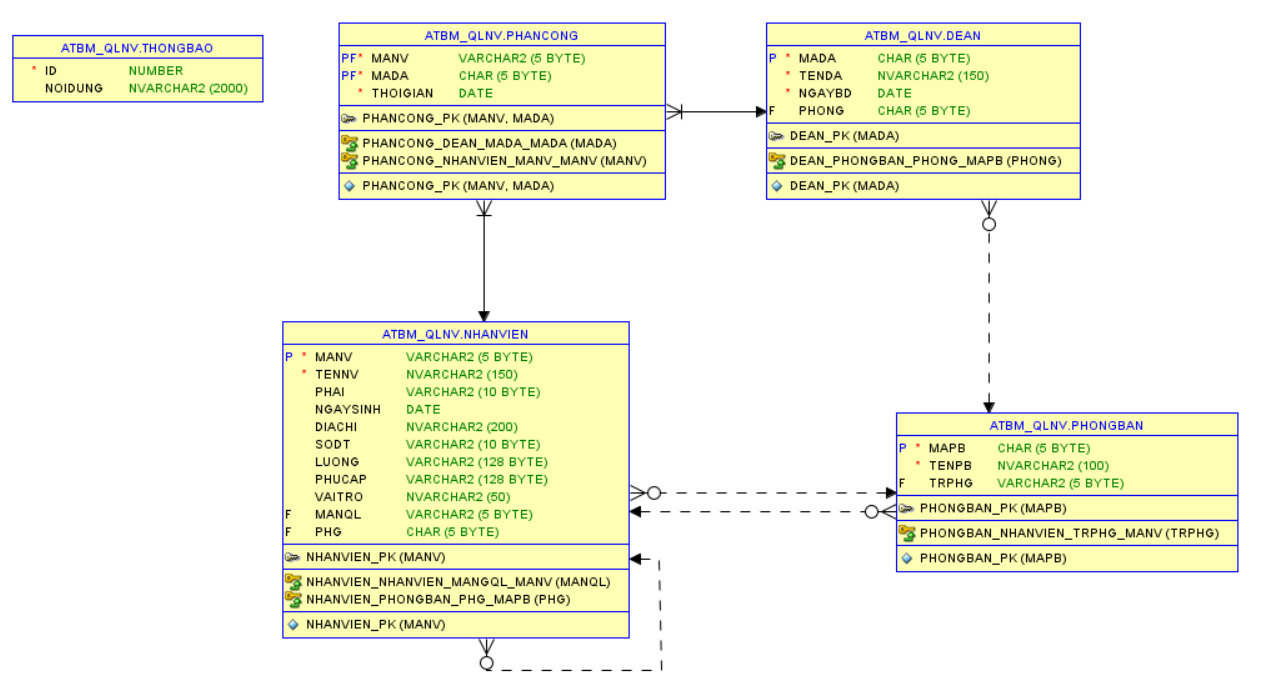


Kết quả hiển thị của chương trình sau khi cài đặt procedure:



# PHÂN HỆ 2: XÂY DỰNG HỆ THỐNG ĐỂ QUẢN LÝ THÔNG TIN NHÂN VIÊN VÀ VIỆC THAM GIA ĐỀ ÁN CỦA NHÂN VIÊN.

# Mô hình cơ sở dữ liệu



# Ràng buộc toàn vẹn

Các thuộc tính của bảng NHANVIEN không nhận giá trị NULL.

Thuộc tính PHAI của bảng NHANVIEN chỉ nhận các giá trị: private, male, female.

Thuộc tính LUONG, PHUCAP của bảng NHANVIEN chỉ nhận giá trị >= 0.

Thuộc tính VAITRO của bảng NHANVIEN chỉ nhận các giá trị: Nhân viên, QL trực tiếp, Trưởng phòng, Tài chính, Nhân sự, Trưởng đề án, Ban giám đốc.

Các thuộc tính của bảng PHONGBAN không nhận giá trị NULL.

Các thuộc tính của bảng DEAN không nhận giá trị NULL.

Các thuộc tính của bảng PHANCONG không nhận giá trị NULL.

# Xác định và phân quyền các loại người dùng

|  |  |
| --- | --- |
| **O** | **Owner** – Người dùng chỉ được thao thác trên dữ liệu của người dùng. |
| **G** | **Group** - Người dùng được quyền thao thác trên dữ liệu của nhân viên, phòng ban do người dùng quản lý. |
| **A** | **All –** Người dùng được quyền thao tác trên tất cả dữ liệu |
| **V** | **View –** Người dùng được quyền xem tất cả |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Nhân viên** | **QL trực tiếp** | **Trưởng phòng** | **Tài chính** | **Nhân sự** | **Trưởng đề án** | **Ban giám đốc** | **ATBM\_QLNV (DBA)** |
| **NHANVIEN** | **I** |  |  |  |  | A (LUONG, PHUCAP null) |  |  | A |
| **S** | O | O; G (trừ LUONG, PHUCAP) | O; G (trừ LUONG, PHUCAP) | V | O | O | A | A |
| **U** | O (NGAY SINH, DIACHI, SODT) | O (NGAY SINH, DIACHI, SODT) | O (NGAY SINH, DIACHI, SODT) | O (NGAY SINH, DIACHI, SODT);  A (LUONG, PHUCAP) | O (NGAY SINH, DIACHI, SODT); | O (NGAY SINH, DIACHI, SODT) |  | A |
| **D** |  |  |  |  |  |  |  | A |
| **PHONGBAN** | **I** |  |  |  |  | A |  |  | A |
| **S** | V | V | V | V | V |  | A | A |
| **U** |  |  |  |  | A |  |  | A |
| **D** |  |  |  |  |  |  |  | A |
| **DEAN** | **I** |  |  |  |  | A |  |  | A |
| **S** | V | V | V | V | A |  | A | A |
| **U** |  |  |  |  | A |  |  | A |
| **D** |  |  |  |  | A |  |  | A |
| **PHANCONG** | **I** |  |  |  | G |  |  |  | A |
| **S** | O | O, G | O | O, G | O |  | A | A |
| **U** |  |  |  | G |  |  |  | A |
| **D** |  |  |  | G |  |  |  | A |

# Các chính sách bảo mật

## Chính sách DAC

DAC (Direct Access Control) được sử dụng để phân quyền trên đối tượng dữ liệu cho từng người dùng khác nhau trong hệ thống thông qua các câu lệnh GRANT và REVOKE. Các quyền ở đây có thể Select, Insert, Update, Delete, Execute.

Ở phân hệ này, mỗi người dùng sẽ được cấp một USERNAME riêng và đăng nhập vào CSDL bằng USER với USERNAME đã cấp. Nhưng do số lượng người dùng lớn nên nhóm chủ yếu sử dụng RBAC thay vì DAC.

## Chính sách RBAC

RBAC (Role-based access control) là một cơ chế phân quyền cho một nhóm người dùng có quyền tương tự nhau thông qua các role và cấp các role cho người dùng.

RBAC được cài đặt như sau:

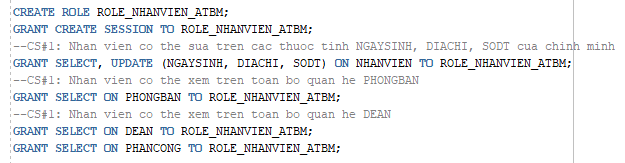
* Cấu hình toàn bộ người dùng thông qua 6 Role:
  + ROLE\_NHANVIEN\_ATBM: quản lý người dùng có vai trò là Nhân viên.
  + ROLE\_QLTRUCTIEP\_ATBM quản lý người dùng có vai trò là Quản lý trực tiếp.
  + ROLE\_TRUONGPHONG\_ATBM: quản lý người dùng có vai trò là Trưởng phòng.
  + ROLE\_TAICHINH\_ATBM: quản lý người dùng có vai trò là Tài chính.
  + ROLE\_NHANSU\_ATBM: quản lý người dùng có vai trò là Nhân sự.
  + ROLE\_TRUONGDEAN\_ATBM: quản lý người dùng có vai trò là Trưởng đề án.
* **CS#1:**

*Nhân viên có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến chính nhân viên đó.*

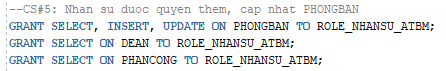
*Nhân viên có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.*

*Nhân viên có thể xem dữ liệu của toàn bộ quan hệ PHONGBAN và DEAN.*

Để role Nhân viên có thể thực hiện trên chính dữ liệu của mình, đầu tiên ta phải cấp quyền trên những bảng hoặc dữ liệu mà Nhân viên có thể thao tác.



* **CS#5:** Nhân sự có quyền thêm và cập nhật trên quan hệ PHONGBAN.



* **CS#6:** Trưởng đề án được quyền thêm, xóa, cập nhật trên quan hệ DEAN.

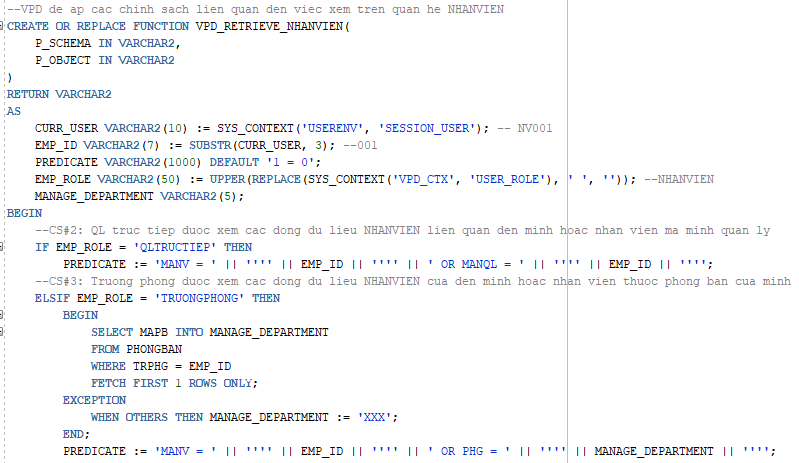


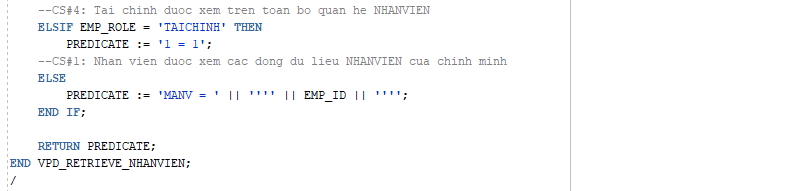
## Chính sách VPD

Sau khi người dùng được cấp quyền trên cơ sở dữ liệu, hệ quản trị sẽ xét đến các chính sách VPD (Virtual Private Database) dùng để kiểm soát các dòng cụ thể trong một bảng bằng cách thêm mệnh đề where vào câu truy vấn của người dùng, từ đó có thể giới hạn những dòng dữ liệu mà người dùng được phép xem.

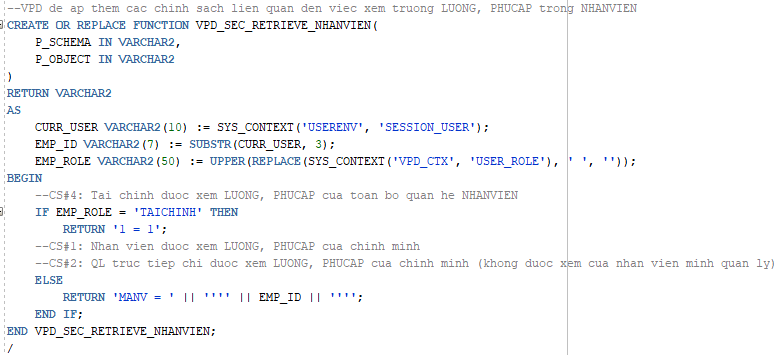
Nhóm chúng em tiến hành xét chính sách VPD liên quan đến các thuộc tính và quan hệ như sau:

***Xem trên quan hệ NHANVIEN:***





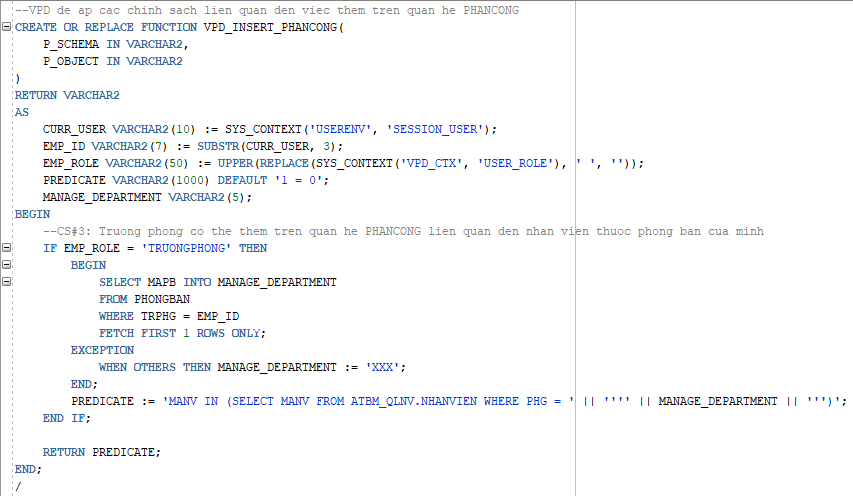
***Xem các thuộc tính LUONG, PHUCAP trên quan hệ NHANVIEN:***

******

***Xem trên quan hệ PHANCONG:***

******

***Thêm trên quan hệ PHANCONG:***

******

***Sửa trên quan hệ PHANCONG:***

******

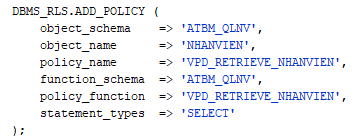
***Xóa trên quan hệ phân công:***

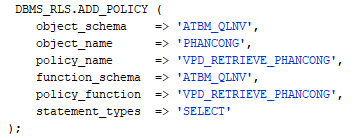
******

Sau đó ta tiến hành **add\_policy()** trên gói **DBMS\_RLS** cho các chính sách sau:

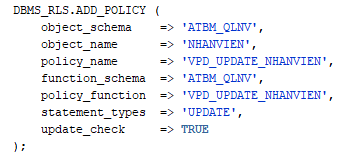
* **CS#1**:

*Nhân viên có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến chính nhân viên đó.*





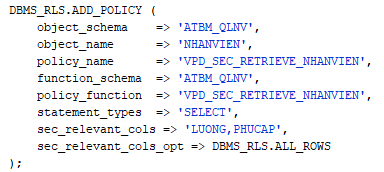
*Nhân viên có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.*



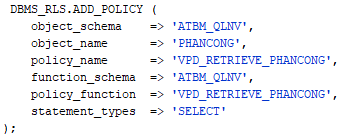
* **CS#2:**

*Nhân viên có vai trò là “QL trực tiếp”:*

*Với các dòng dữ liệu trong quan hệ NHANVIEN liên quan đến các nhân viên mà người dùng là quản lý trực tiếp thì QL trực tiếp được xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.*

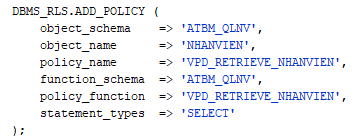


*Có thể xem các dòng trong quan hệ PHANCONG liên quan đến chính người dùng QL trực tiếp và các nhân viên được quản lý trực tiếp bởi người dùng.*

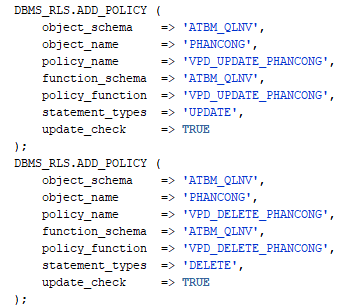


* **CS#3:**

*Với các dòng trong quan hệ NHANVIEN liên quan đến các nhân viên thuộc phòng ban mà Trưởng phòng quản lý thì Trưởng phòng có quyền xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.*

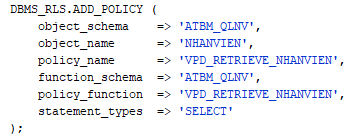


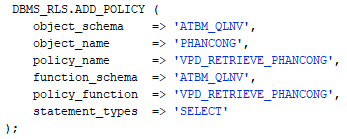
*Có thể thêm, xóa, cập nhật trên quan hệ PHANCONG liên quan đến các nhân viên thuộc  
phòng ban mà Trưởng phòng quản lý.*

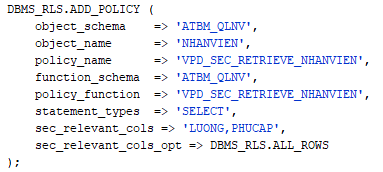
**

* **CS#4:**

*Người dùng có vai trò là “Tài chính” có thể xem trên toàn bộ quan hệ NHANVIEN và PHANCONG, có thể sửa trên thuộc tính LUONG và PHUCAP.*





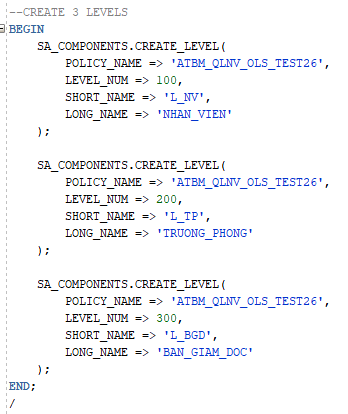


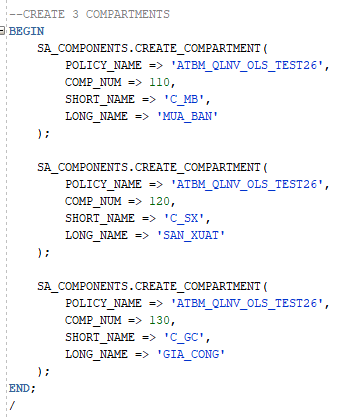
s

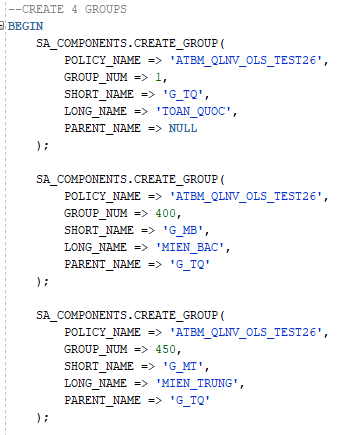
## Chính sách OLS

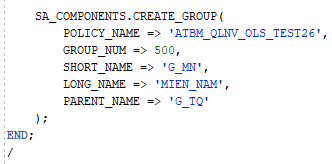
*Cài đặt OLS:* OLS (Oracle label security) là một trong chính sách điều khiển quyền truy cập các dòng trong một bảng bằng cách dán nhãn lên các dòng dữ liệu và lên từng người dùng. Khi người dùng gọi đến bảng dữ liệu được cài đặt chính sách OLS thì chỉ xem được những dòng dữ liệu thỏa mãn nhãn của mình. Các nhãn được chia thành 3 mức độ là Level, Compartment và Group. Chính sách được cài đặt cụ thể như sau:

* *Level:* 
  + L\_NV: Nhân viên (level\_num = 100).
  + L\_TP: Trưởng phòng (level\_num = 200).
  + L\_BGD: Ban giám đốc (level\_num = 300).
* *Compartment:*
  + C\_MB: mua bán.
  + C\_SX: sản xuất.
  + C\_GC: gia công.
* *Group:*
  + G\_TQ: toàn quốc.
  + G\_MB: miền Bắc.
  + G\_MT: miền Trung.
  + G\_MN: miền Nam.

******

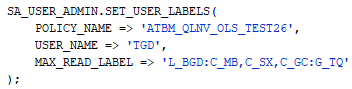
******

******

******

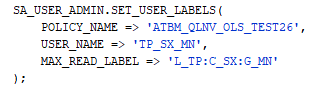
* *Diễn giải lý do cài đặt các thuộc tính của nhãn như trên:*
* Về *Level*: Level của nhãn thể thiện mức độ nhạy cảm của dữ liệu do đó để thỏa mãn YC3, ta sẽ tạo ra 3 levels tương ứng với 3 cấp bậc người dùng (Nhân viên, Trưởng phòng, Ban giám đốc). Trong đó level *L\_BGD* tương ứng với “Ban giám đốc” sẽ là level cao nhất và level *L\_NV* tương ứng với “Nhân viên” sẽ là level thấp nhất.
* Về *Compartment*: ta thấy theo YC3 thì hệ thống hoạt động được chia thành 3 lĩnh vực khác nhau đo đó ta tạo 3 compartments khác nhau tương ứng với 3 lĩnh vực: mua bán, gia công, sản xuất.
* Về *Group*: ta thấy theo YC3 thì ta thấy công ty sẽ có các chi nhánh đặt tại 3 nơi khác nhau đo đó ta tạo 3 groups khác nhau tương ứng là: miền Bắc, miền Trung, miền Nam. Hơn nữa, ta tiến hành thêm thuộc tính parent\_group của 3 nơi là toàn quốc.
* *Thiết lập hệ thống nhãn tương ứng với 3 loại người dùng khác nhau thỏa YC3:*
* Giám đốc có thể đọc được toàn bộ dữ liệu

Nhãn tương ứng với người dùng: L\_BGD:C\_MB, C\_SX, C\_GC:G\_TQ

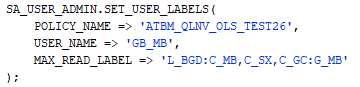
****

* Trưởng phòng phụ trách lĩnh vực sản xuất miền Nam

Nhãn tương ứng với người dùng: *L\_TP:C\_SX:G\_MN*

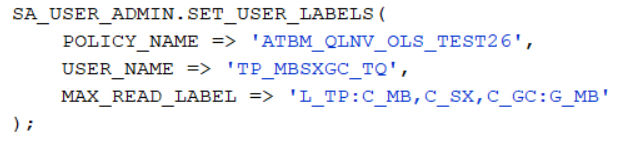
* ****
* Giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc

Nhãn tương ứng với người dùng: *L\_BGD:C\_SX, C\_GC, C\_MB:G\_MB*

**

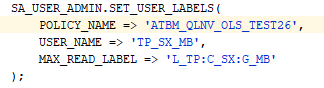
* Trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.

Nhãn tương ứng với người dùng: *L\_TP:C\_SX, C\_GC, C\_MB:G\_TQ*

**

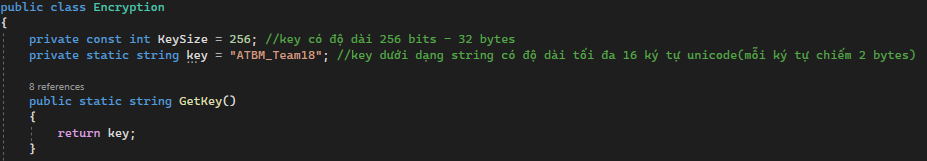
* Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.

Nhãn tương ứng với người dùng: *L\_TP:C\_SX:G\_MB*

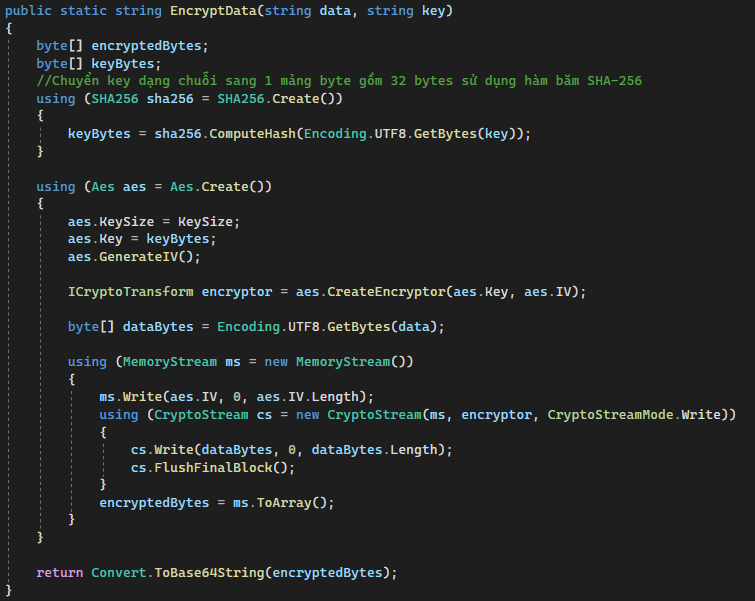
**

## Chính sách Encryption

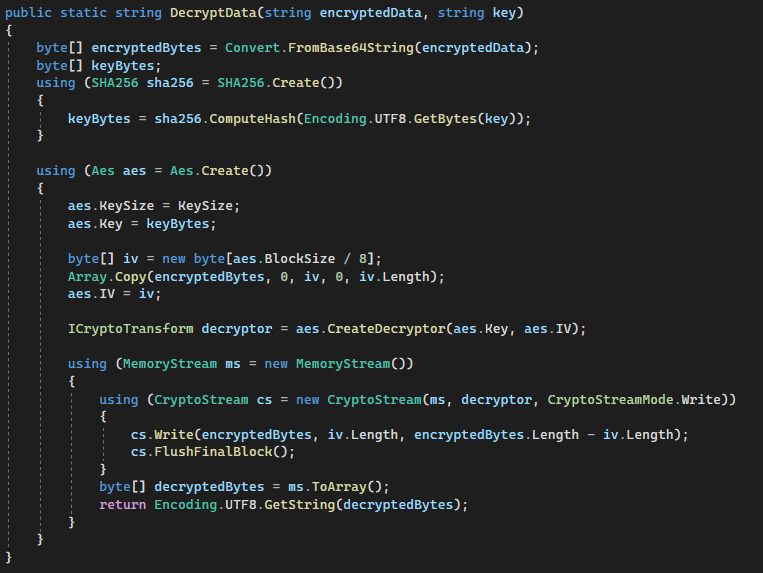
* Người dùng có vai trò “Tài chính” thực hiện mã hóa trường LUONG, PHUCAP khi cập nhật trên các trường này và dữ liệu được giải mã khi thực hiện đọc dữ liệu LUONG, PHUCAP.
* Mã hóa dữ liệu mức ứng dụng vì trong C# có thư viện hỗ trợ việc mã hóa đơn giản hơn và việc mã hóa trong ứng dụng rồi lưu trữ chuỗi ký tự mã hóa vào cơ sở dữ liệu dễ dàng hơn, tránh việc xung đột với các chính sách bảo mật của hệ thống.
* Phương pháp mã hóa là mã hóa đối xứng sử dụng thuật toán AES (Advanced Encryption Standard) trong thư viện “System.Security.Cryptography”. Dữ liệu đầu vào được chuyển thành một dãy byte và sau đó được mã hóa bằng cách sử dụng khóa và vector khởi tạo (IV).
* Thay đổi kiểu dữ liệu trường LUONG, PHUCAP trong bảng NHANVIEN sang VARCHAR2 để lưu chuỗi ký tự mã hóa.
* Cơ chế quản lý khóa:
  + Thiết lập khóa: sử dụng khóa cứng có độ dài 256 bits – 32 bytes (16 ký tự UNICODE). Khóa ban đầu là “ATBM\_Team18”;
  + Lưu trữ khóa: khóa được lưu trữ dưới dạng thuộc tính trong class Encryption trong ứng dụng.
  + Phân phối khóa: khóa bí mật được lưu trong mã nguồn ứng dụng và không được chia sẻ.
  + Phục hồi khóa: do khóa không được chia sẻ nên không có việc phục hồi khóa.
  + Thay khóa: Sau một thời gian, việc thay khóa được thực hiện thủ công.
* Lưu trữ key trong class Encryption.cs của ứng dụng:



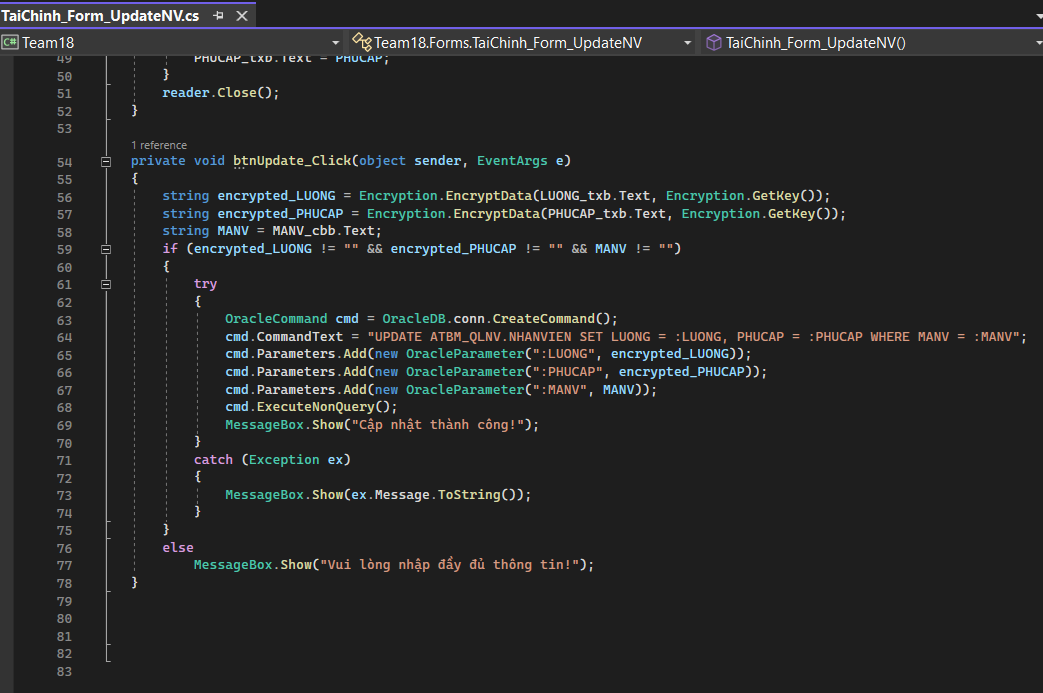
* Hàm mã hóa trong C# (class Encryption.cs):



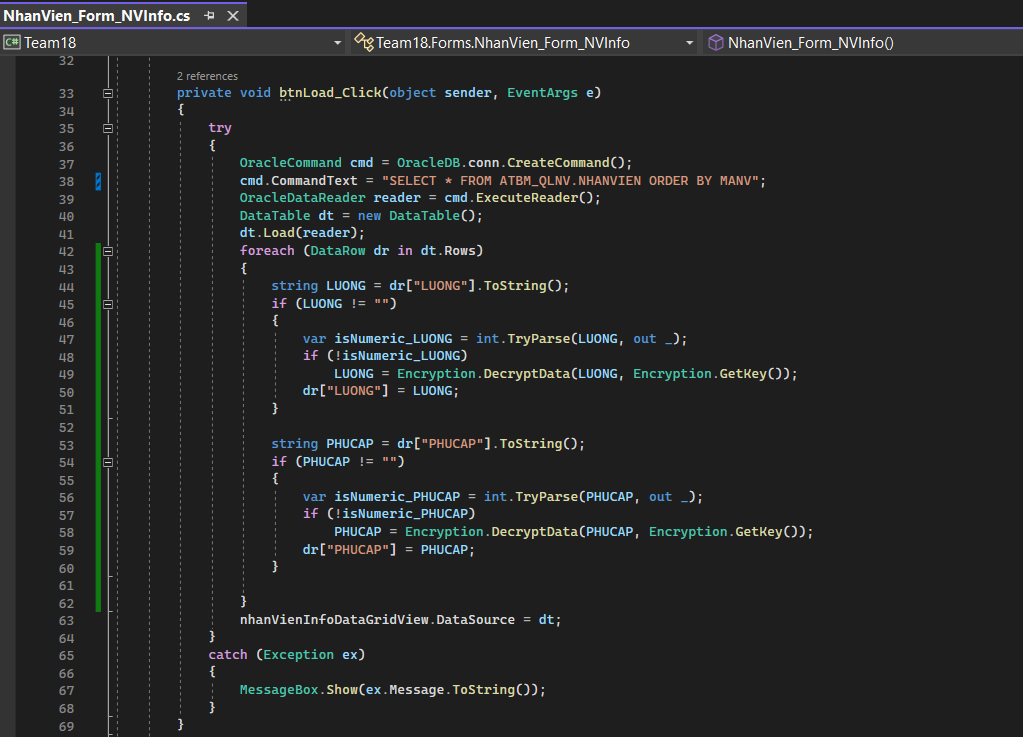
* Hàm giải mã trong C# (class Encryption.cs):



* Khi user có role “Tài chính” cập nhật trên trường LUONG, PHUCAP của NHANVIEN thì dữ liệu được mã hóa trước khi truyền vào tham số của câu lệnh OracleCommand và gửi đến cơ sở dữ liệu:



* Khi user bất kỳ có quyền xem trường LUONG, PHUCAP thì dữ liệu được giải mã sau khi được gửi từ cơ sở dữ liệu đến ứng dụng (ví dụ user có role “Nhân viên” có thể xem LUONG, PHUCAP của chính mình):



## Chính sách Audit

Audit là hành động theo dõi, nó đóng vai trò như một chiếc camera ghi lại những thao tác, hành động tác động trực tiếp lên dữ liệu. Đây không phải là cơ chế phân quyền người dùng, điều khiển truy cập... nó chỉ tương tự như việc ghi lại log, giúp người quản trị cơ sở dữ liệu theo dõi, kiểm soát những đối tượng có hành vi xấu đối với database...nhằm phục vụ cho cơ chế dò tìm để phát hiện tấn công

Mục đích của việc auditing:

* Auditing cho phép ta bắt các user phải có trách nhiệm về hành động mà họ thực hiện, bằng cách theo dõi hành vi của họ.
* Dữ liệu audit giúp phát hiện lỗ hổng trong chính sách bảo mật.
* Liên quan đến trách nhiệm giải trình của user. Cần phải đảm bảo rằng user chỉ được thực hiện những gì họ được phép. Ghi nhận sự lạm quyền hoặc dùng sai quyền.
* Auditing để ghi nhận lại những gì đã xảy ra và có hồi đáp thích hợp.
* Không thực hiện auditing ta sẽ không thể biết khía cạnh bảo mật của hệ thống có đảm bảo hay không hay có ai đã đọc hoặc cập nhật dữ liệu một cách bất hợp pháp hay không.

### Kích hoạt audit toàn hệ thống

Chức năng Audit mặc định không được kích hoạt, nhưng có thể kích hoạt bằng lệnh sau: alter system set audit\_trail = DB,EXTENDED scope = spfile;

Các giá trị của audit trail: audit\_trail = {none | os | db | DB,EXTENDED | xml | xml, extended} trong đó:

* + none: tắt chế độ audit.
  + os: bật chế độ audit và các audit record sẽ được lưu trong file OS.
  + DB,EXTENDED: bật chế độ audit và các audit record sẽ được lưu trong database audit trail (SYS.AUD$), ngoài ra, điền các cột SQLBIND và SQLTEXT CLOB của bảng (SYS.AUD$).
  + xml: bật chế độ audit và các audit record sẽ được lưu file OS có định dạng XML.

Sau đó chúng ta thực hiện reset Oracle Database bằng lệnh:

* + shutdown immediate;
  + startup;

Kích hoạt STANDARD AUDIT: lệnh AUDIT thiết lập lựa chọn giám sát câu lệnh và quyền thường đi sau mệnh đề "BY" để giới hạn tầm vực của câu lệnh và lựa chọn giám sát quyền:

* + BY ACCESS: Ghi một record cho mỗi câu lệnh và hoạt động được audit
  + BY SESSION: Ghi một record cho tất cả các câu lệnh SQL cùng loại và tất cả các hoạt động cùng loại được thực hiện trên cùng một đối tượng schema trong cùng một session
  + WHENEVER SUCCESSFUL: thực hiện ghi dữ liệu audit đối với những câu lệnh được thực hiện thành công. ví dụ: AUDIT SELECT ON USERS BY ACCESS WHENEVER SUCCESSFUL; -- Thực hiện audit đối với việc thực thi thành công câu lệnh SELECT trên bảng USERS. audit update on USERS by access WHENEVER successful;-- -- Thực hiện audit đối với việc thực thi thành công câu lệnh UPDATE trên bảng USERS.
  + WHENEVER NOT SUCCESSFUL: thực hiện ghi dữ liệu audit đối với những câu lệnh được thực hiện không thành công. ví dụ: audit update on USERS by access WHENEVER not successful; -- Thực hiện audit đối với việc thực thi lỗi câu lệnh UPDATE trên bảng USERS.
  + Có thể cài đặt thực hiện audit(tạo/xóa/chỉnh sửa cấu trúc bảng) trên bất kì bảng nào trên database: AUDIT DROP ANY TABLE; AUDIT CREATE ANY TABLE; AUDIT DELETE ANY TABLE;

### Tắt audit

Ở mức tổng quát, ta có thể dùng trực tiếp câu lệnh NOAUDIT với các schema\_object:

* + VD1: tắt audit trên quyền: NOAUDIT ALL PRIVILEGES;.
  + VD2: tắt audit trên role( ví dụ việc create/ drop... role): NOAUDIT ROLE;
  + VD3: tắt giám sát trên câu lệnh: NOAUDIT ALL;

Sử dụng câu lệnh NOAUDIT để tắt các lựa chọn giám sát:

Diagram

Description automatically generated

Diagram

Description automatically generated

Diagram, text

Description automatically generated

* + VD1: tắt chế độ audit khi lấy list users thành công: NOAUDIT SELECT ON USERS WHENEVER SUCCESSFUL;
  + VD2: tắt chế độ audit khi lấy list users không thành công:NOAUDIT SELECT ON USERS WHENEVER NOT SUCCESSFUL;
  + VD3: tắt chế độ audit khi lấy list users chỉ đối với user có tên là user\_name: NOAUDIT SELECT USERS BY user\_name;
  + VD4: tắt chế độ audit khi lấy list users: NOAUDIT SELECT ON USERS;

### Standard audit

Hành vi 1: Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG



Hành vi 2: Những người đã đọc trên trường LUONG và PHUCAP của người khác.

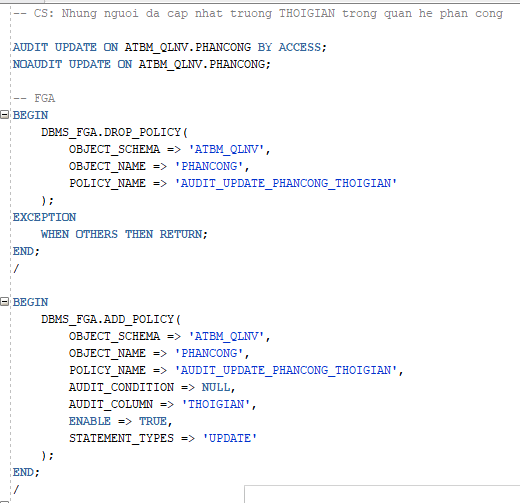


Hành vi 3: Một người không thuộc vai trò “Tài chính” những đã cập nhật thành công trên trường LUONG và PHUCAP.



### Fine-grained audit

Hành vi 1: Theo nguyên tắc phải ghi dấu lại thời gian đề án được phân công cho nhân viên nên Fine – grained audit được cài đặt lên cột THOIGIAN trong bảng PHANCONG để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.



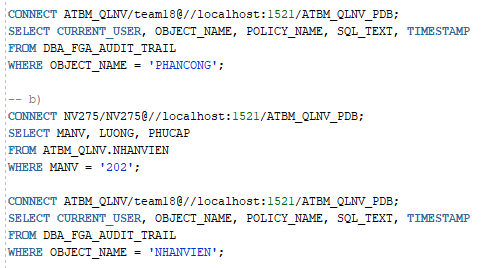
Hành vi 2: Theo nguyên tắc thông tin về LUONG và PHUCAP của từng người dùng phải được bảo vệ và giữ bí mật thì Fine – grained audit được cài đặt lên cột LUONG và PHUCAP trong bảng NHANVIEN để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.



Hành vi 3: Ghi vết lại một người **không** thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP. Thì Fine – grained audit được cài đặt lên cột LUONG và PHUCAP trong bảng NHANVIEN để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.



Hành vi 4: Kiểm tra nhật ký hệ thống.



# Tài liệu tham khảo

<https://docs.oracle.com/cd/E11882_01/network.112/e10745/getstrtd.htm?fbclid=IwAR1x-EwFnOgXpZz3TXbfwFyJeUG-hIGXQfVfVv9QLvndlQwtwsGMtRDIjd0>

<https://www.oracle.com/webfolder/technetwork/tutorials/obe/db/10g/r2/prod/security/vpd/vpd_otn.htm?fbclid=IwAR2M-PiifNrmVj_aZZ_vvX4BHqC37gT8ggsFAVAmh5wavt1IfBEvIEMd7H4>

<https://docs.oracle.com/cd/B14117_01/server.101/b10759/statements_4007.htm?fbclid=IwAR09_pKrHxY9D6p1FL5QnDi-k2S3QqDizxNALWN4TRpqKuue3DO9JhX2x-k>