BỘ CÔNG THƯƠNG

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG THÀNH PHỐ HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

---------------------------

A white circle with blue and red text and a book with a graduation cap

AI-generated content may be incorrect.

**Đề tài**

**QUẢN LÝ PHÒNG GYM**

**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**BẢO MẬT CƠ SỞ DỮ LIỆU**

**SINH VIÊN THỰC HIỆN:**

1. 2001230510 Đỗ Lê Thanh Mẫn

2. 2001230550 Nguyễn Ngà

3. 2001230467 Bùi Hữu Lộc

**GVHD: Nguyễn Phương Hạc**

TP. HỒ CHÍ MINH, 07 tháng 01 năm 2025

**PHÂN CÔNG NHIỆM VỤ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BẢNG PHÂN CÔNG** | | | | |
| **Tuần** | **Bùi Hữu Lộc** | **Nguyễn Ngà** | **Đỗ Lê Thanh Mẫn** | **Tiến độ** |
| **5** | Tạo tài khoản nhân viên (áp dụng mã hóa bất đối xứng) | Đăng xuất tài khoản nhân viên | Đăng nhập tài khoản nhân viên (áp dụng mã hóa bất đối xứng) | 100% |
| **6** | Đăng nhập khách hàng | Đăng ký tài khoản khách hàng (áp dụng mã hóa đổi xứng ) | Hiển thị danh sách sản phẩm, đăng xuất khách hàng | 100% |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  | Khôi phục mật khẩu (áp dụng des cho Otp) | Cập nhật mã hóa mật khẩu tài khoản ở mức csdl (áp dụng des) | 100% |
| **10** | Xuất và xem danh sách hóa đơn (áp dụng mã hóa lai DES+RSA) |  |  | 100% |
| **11** |  | Ký số hóa đơn gửi mail cho khách hàng (áp dụng RSA) | Kiểm tra file ký số | 100% |
| **12** | Thiếp lập form phân quyền | Áp dụng Profile |  | 100% |
| **13** | Kiểm toán | Áp dụng VPD, backup | Giám sát người dùng | 100% |

**MỤC LỤC**

[**DANH MỤC HÌNH** 5](#_Toc217853865)

[**CHƯƠNG 1: XÂY DỰNG CƠ SỞ DỮ LIỆU** 7](#_Toc217853866)

[**1.1 Khảo sát, phân tích nghiệp vụ:** 7](#_Toc217853867)

[**1.1.1 Nghiệp vụ quản trị và bảo mật** 7](#_Toc217853868)

[**1.1.2 Nghiệp vụ bán hàng và kho** 7](#_Toc217853869)

[**1.1.3 Nghiệp vụ dịch vụ và hội viên** 7](#_Toc217853870)

[**1.1.4 Nghiệp vụ đào tạo và huấn luyện** 7](#_Toc217853871)

[**1.1.5 Nghiệp vụ nhân sự** 8](#_Toc217853872)

[**1.2 Thiết kế cơ sở dữ liệu trên Oracle** 8](#_Toc217853873)

[**1.3 Xây dựng ứng dụng kết nối đến cơ sở dữ liệu:** 14](#_Toc217853874)

[**1.3.1 Cấu hình kết nối (Constring):** 14](#_Toc217853875)

[**1.3.2 Bảo mật kết nối:** 15](#_Toc217853876)

[**CHƯƠNG 2: MÃ HÓA** 15](#_Toc217853877)

[**2.1 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa đối xứng ở mức ứng dụng, cơ sở dữ liệu** 15](#_Toc217853878)

[**2.1.1 Áp dụng mã hóa nhân** 15](#_Toc217853879)

[**2.1.2 Áp dụng mã hóa DES** 17](#_Toc217853880)

[**2.2 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa bất đối xứng ở mức ứng dụng, cơ sở dữ liệu** 20](#_Toc217853881)

[**2.3 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa lai ở mức ứng dụng, cơ sở dữ liệu** 22](#_Toc217853882)

[**CHƯƠNG 3: ĐIỀU KHIỂN TRUY CẬP** 28](#_Toc217853883)

[**3.1 Cài đặt nhóm quyền, profile, session, tablespace** 28](#_Toc217853884)

[**3.1.1. Cài đặc nhóm quyền** 28](#_Toc217853885)

[**3.1.2. Thiết lập Profile quản lý chính sách người dùng.** 29](#_Toc217853886)

[**3.1.3. Xây dựng các thủ tục (Stored Procedures) quản lý Session** 30](#_Toc217853887)

[**3.1.4. Cấu hình Tablespace** 33](#_Toc217853888)

[**3.2 Cài đặt ứng dụng phân quyền, nhóm quyền để điều khiển truy cập** 34](#_Toc217853889)

[**3.2.1. Chức năng Bổ nhiệm và Quản lý Nhóm quyền (Role Management)** 38](#_Toc217853890)

[**3.3 Dùng công cụ FGA cài đặt VPD, cài đặt OLS** 41](#_Toc217853891)

[**3.3.1. Cài đặt VPD** 41](#_Toc217853892)

[**3.3.2. Cài đặt FGA** 42](#_Toc217853893)

[**CHƯƠNG 4: KIỂM TOÁN** 46](#_Toc217853894)

[**4.1 Cài đặt ứng dụng có tính năng giám sát người dùng** 46](#_Toc217853895)

[**4.1.1 Cơ chế hoạt động (Technical Mechanism):** 46](#_Toc217853896)

[**4.1.2 Giao diện** 48](#_Toc217853897)

[**KẾT LUẬN** 49](#_Toc217853898)

[**DANH MỤC TÀI LIỆU THAM KHẢO** 50](#_Toc217853899)

# **DANH MỤC HÌNH**

[Hình 1 Bảng CHECKIN 8](#_Toc218710855)

[Hình 2 Bảng CHITIETGIOHANG 8](#_Toc218710856)

[Hình 3 Bảng CHITIETHOADON 9](#_Toc218710857)

[Hình 4 Bảng CHUCVU 9](#_Toc218710858)

[Hình 5 Bảng CHUYENMON 9](#_Toc218710859)

[Hình 6 Bảng DANGKYGOITAP 9](#_Toc218710860)

[Hình 7 Bảng DANGKYLOP 10](#_Toc218710861)

[Hình 8 Bảng DANGKYPT 10](#_Toc218710862)

[Hình 9 Bảng DIACHI 10](#_Toc218710863)

[Hình 10 Bảng GOITAP 11](#_Toc218710864)

[Hình 11 Bảng HINHANH 11](#_Toc218710865)

[Hình 12 Bảng HOADON 11](#_Toc218710866)

[Hình 13 Bảng KHACHHANG 12](#_Toc218710867)

[Hình 14 Bảng LICHLOP 12](#_Toc218710868)

[Hình 15 Bảng LICHTAPPT 12](#_Toc218710869)

[Hình 16 Bảng LOAIKHACHHANG 13](#_Toc218710870)

[Hình 17 Bảng LOAISANPHAM 13](#_Toc218710871)

[Hình 18 Bảng LOPHOC 13](#_Toc218710872)

[Hình 19 Bảng NHANVIEN 13](#_Toc218710873)

[Hình 20 Bảng NHANVIENCHUYENMON 14](#_Toc218710874)

[Hình 21 Bảng SANPHAM 14](#_Toc218710875)

[Hình 22 Cấu hình kết nối 14](#_Toc218710876)

[Hình 23 mã hóa nhân 16](#_Toc218710877)

[Hình 24 CurReigister 16](#_Toc218710878)

[Hình 25 CusLogin 17](#_Toc218710879)

[Hình 26 DES 18](#_Toc218710880)

[Hình 27 ForgotPassword Action 18](#_Toc218710881)

[Hình 28 Mã hóa mật khẩu nhân viên 19](#_Toc218710882)

[Hình 29 Mã hóa mật khẩu nhân viên 19](#_Toc218710883)

[Hình 30 RSA 20](#_Toc218710884)

[Hình 31 Hash 20](#_Toc218710885)

[Hình 32 Sing 21](#_Toc218710886)

[Hình 33 DataExport 22](#_Toc218710887)

[Hình 34 CSV 23](#_Toc218710888)

[Hình 35 Mã hóa lai 23](#_Toc218710889)

[Hình 36 Key 24](#_Toc218710890)

[Hình 37 EncryptFile 24](#_Toc218710891)

[Hình 38 DecryltFile 25](#_Toc218710892)

[Hình 39 managerole 27](#_Toc218710893)

[Hình 40 grant 27](#_Toc218710894)

[Hình 41 procedure tạo tài khoản và phân quyền 28](#_Toc218710895)

[Hình 42 khởi tạo profile 28](#_Toc218710896)

[Hình 43 Thủ tục lấy danh sách phiên làm việc 29](#_Toc218710897)

[Hình 44 Thủ tục ngắt kết nối (Kill Session) 30](#_Toc218710898)

[Hình 45 kiểm tra cảnh báo bảo mật 31](#_Toc218710899)

[Hình 46 kiểm tra trạng thái chi tiết 31](#_Toc218710900)

[Hình 47 cấp quyền 32](#_Toc218710901)

[Hình 48 khởi tạo lệnh DATA\_GYM 32](#_Toc218710902)

[Hình 49 grant 33](#_Toc218710903)

[Hình 50 thu hồi quyền 33](#_Toc218710904)

[Hình 51 hàm cập nhật quyền 34](#_Toc218710905)

[Hình 52 giao diện phân quyền 35](#_Toc218710906)

[Hình 53 giao diện quản lý sản phẩm 35](#_Toc218710907)

[Hình 54 quản trị phân quyền 35](#_Toc218710908)

[Hình 55 cập nhật sản phẩm 36](#_Toc218710909)

[Hình 56 thủ tục bổ nhiệm 36](#_Toc218710910)

[Hình 57 thủ tục bãi nhiệm 37](#_Toc218710911)

[Hình 58 hàm bổ nhiệm 37](#_Toc218710912)

[Hình 59 hàm bãi nhiệm 38](#_Toc218710913)

[Hình 60 giao diện bổ nhiệm 38](#_Toc218710914)

[Hình 61 giao diện bãi nhiệm 39](#_Toc218710915)

[Hình 62 hàm chính sách 40](#_Toc218710916)

[Hình 63 gán chính sách vào bảng 40](#_Toc218710917)

[Hình 64 góc nhìn StaffPt 41](#_Toc218710918)

[Hình 65 góc nhìn admin 41](#_Toc218710919)

[Hình 66 kill session 45](#_Toc218710920)

[Hình 67 get auditlog 46](#_Toc218710921)

[Hình 68 audittrail 47](#_Toc218710922)

[Hình 69 giao diện giám sát 47](#_Toc218710923)

# **CHƯƠNG 1: XÂY DỰNG CƠ SỞ DỮ LIỆU**

## **1.1 Khảo sát, phân tích nghiệp vụ:**

Gồm 5 nhóm nghiệp vụ chính:

### **1.1.1 Nghiệp vụ quản trị và bảo mật**

**Mục tiêu:** Đảm bảo hệ thống vận hành an toàn, đúng người đúng việc.

* **Quản lý phiên làm việc:**

Hệ thống cần có cơ chế giám sát xem ai đang đăng nhập và làm việc vào thời điểm nào. Cần ghi lại lịch sử đăng nhập để tra cứu khi có sự cố hoặc mất mát dữ liệu.

* **Phân quyền người dùng:**

Hệ thống phải cho phép quản trị viên cấp quyền hạn cụ thể cho từng nhân viên.

### **1.1.2 Nghiệp vụ bán hàng và kho**

**Mục tiêu:** Quản lý việc bán các sản phẩm phụ trợ (nước uống, thực phẩm chức năng, găng tay...) tại quầy lễ tân.

* **Quản lý sản phẩm:**

Hệ thống cho phép nhập liệu thông tin các mặt hàng đang bán, cập nhật giá cả và phân loại hàng hóa để dễ tìm kiếm.

* **Quy trình bán hàng:**

Khi khách mua hàng, hệ thống cần hỗ trợ nhân viên tạo giỏ hàng (chọn nhiều món), tính tổng tiền tự động và xuất phiếu thanh toán (hóa đơn) cho khách.

### **1.1.3 Nghiệp vụ dịch vụ và hội viên**

**Mục tiêu:** Quản lý vòng đời của một hội viên từ lúc đăng ký đến lúc tập luyện.

* **Quản lý khách hàng:**

Cần lưu trữ đầy đủ thông tin cá nhân, hình ảnh để nhận diện, và phân loại khách (Khách mới, VIP, Thân thiết) để có chính sách chăm sóc phù hợp.

* **Quản lý gói tập:**

Hệ thống phải hỗ trợ thiết lập đa dạng các loại gói tập (theo tháng, theo năm, hoặc vé lượt). Khi khách đăng ký, hệ thống sẽ ghi nhận ngày kích hoạt và ngày hết hạn.

* **Kiểm soát ra vào:**

Đây là chức năng quan trọng nhất. Khi khách đến tập, hệ thống phải kiểm tra ngay lập tức: Gói tập còn hạn không? Còn số buổi không? Nếu hợp lệ mới cho phép vào.

### **1.1.4 Nghiệp vụ đào tạo và huấn luyện**

**Mục tiêu:** Quản lý lịch trình tập luyện chuyên sâu.

* **Lớp học nhóm:**

Hệ thống cần có chức năng lên lịch các lớp học cố định trong tuần. Cho phép hội viên đăng ký giữ chỗ trước để tránh quá tải phòng tập.

* **Huấn luyện viên cá nhân:**

Hệ thống cần quản lý lịch làm việc của từng PT. Ghi nhận việc hội viên thuê riêng PT, theo dõi số buổi đã tập và số buổi còn lại với HLV đó.

### **1.1.5 Nghiệp vụ nhân sự**

**Mục tiêu:** Tối ưu hóa việc sử dụng nhân sự dựa trên kỹ năng.

* **Quản lý hồ sơ nhân viên:**

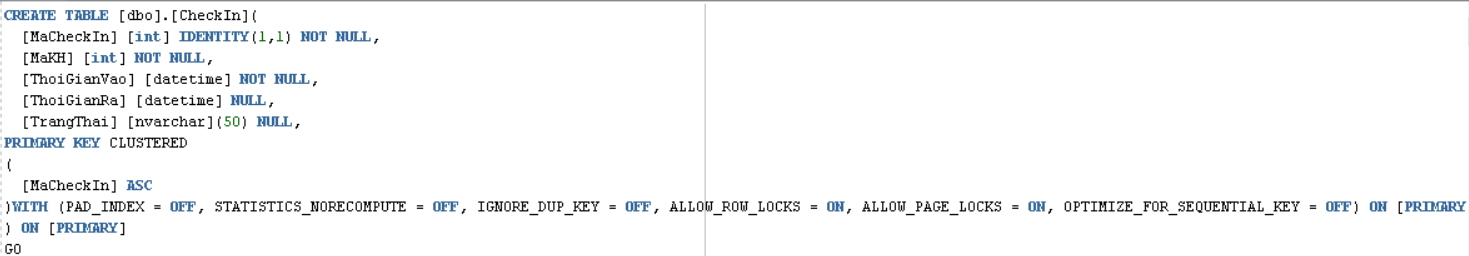
Quản lý danh sách nhân viên, thông tin liên lạc và chức vụ hiện tại.

* **Quản lý chuyên môn:**

Hệ thống cần ghi nhận mỗi Huấn luyện viên có thế mạnh gì để bộ phận xếp lớp hoặc lễ tân có thể tư vấn, sắp xếp lịch dạy phù hợp cho khách hàng.

## **1.2 Thiết kế cơ sở dữ liệu trên Oracle**

* **Bảng CHECKIN**

****

Hình 1 Bảng CHECKIN

* **Bảng CHITIETGIOHANG**

****

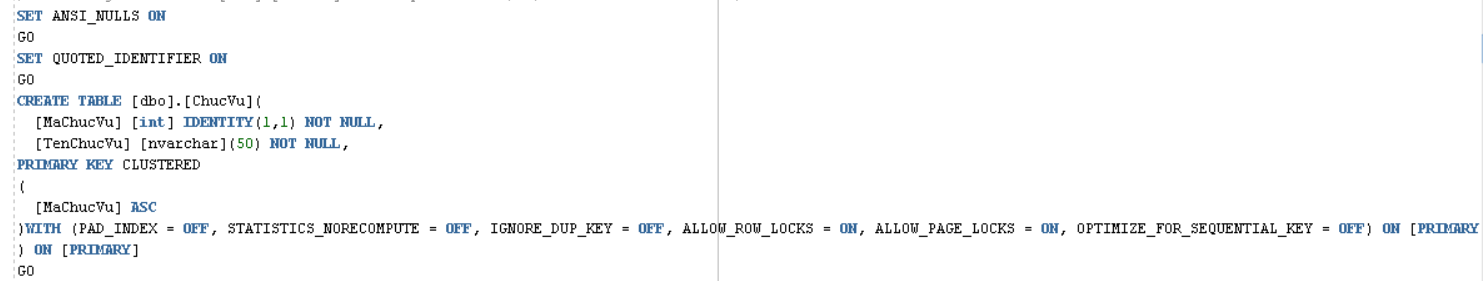
Hình 2 Bảng CHITIETGIOHANG

* **Bảng CHITIETHOADON**

****

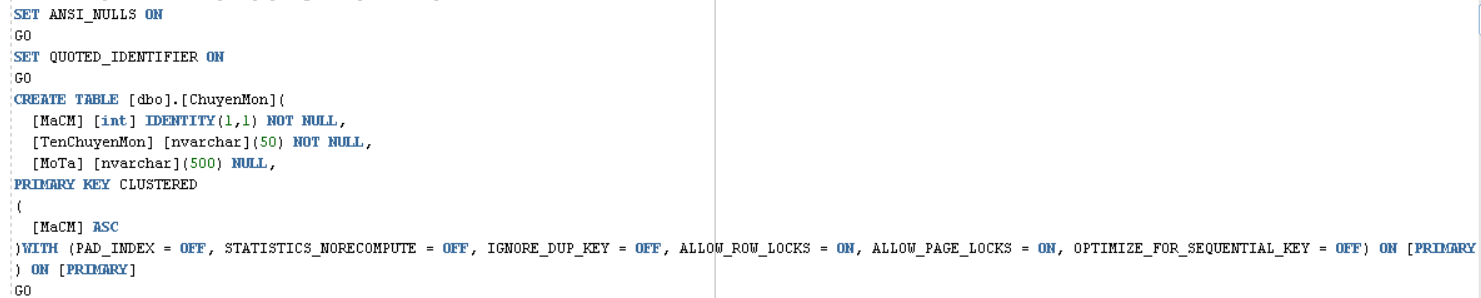
Hình 3 Bảng CHITIETHOADON

* **Bảng CHUCVU**

****

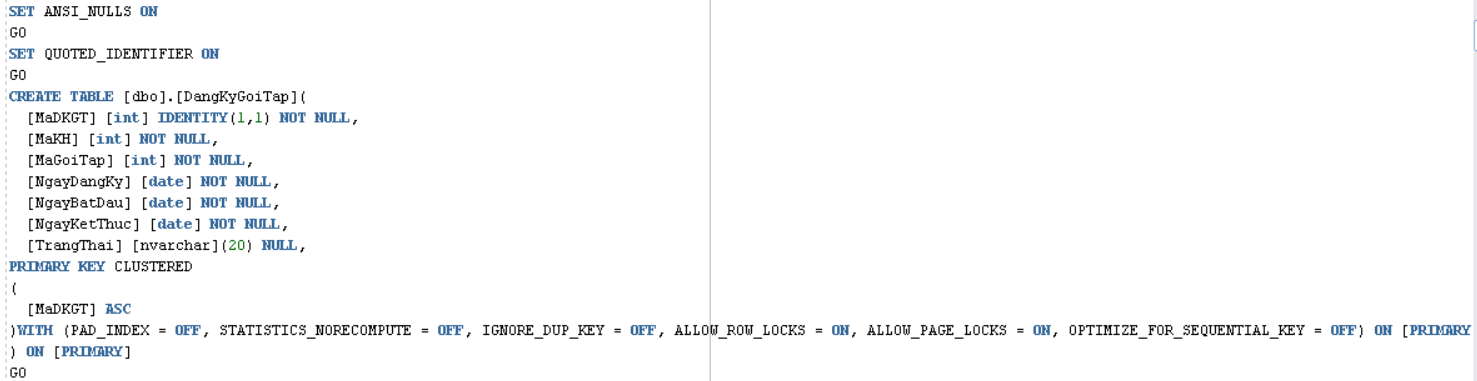
Hình 4 Bảng CHUCVU

* **Bảng CHUYENMON**

****

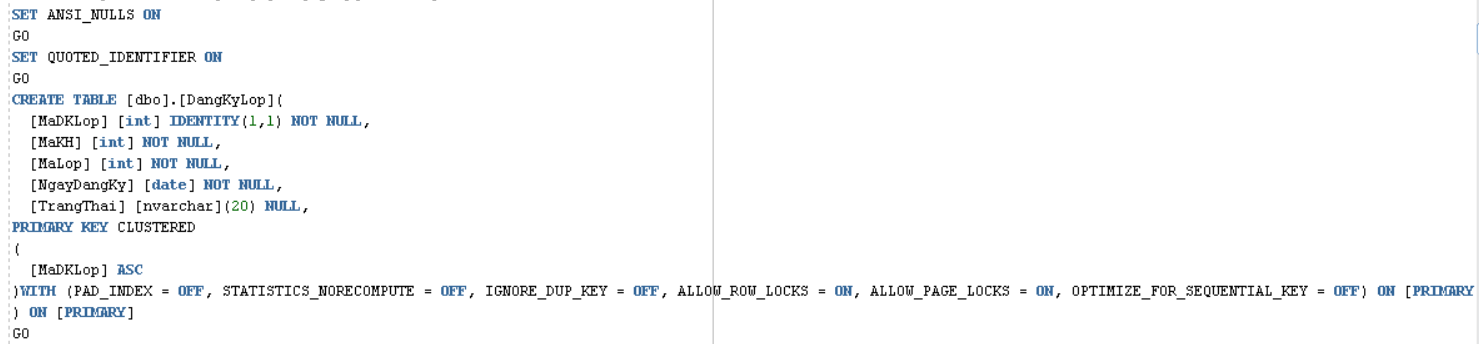
Hình 5 Bảng CHUYENMON

* **Bảng DANGKYGOITAP**

****

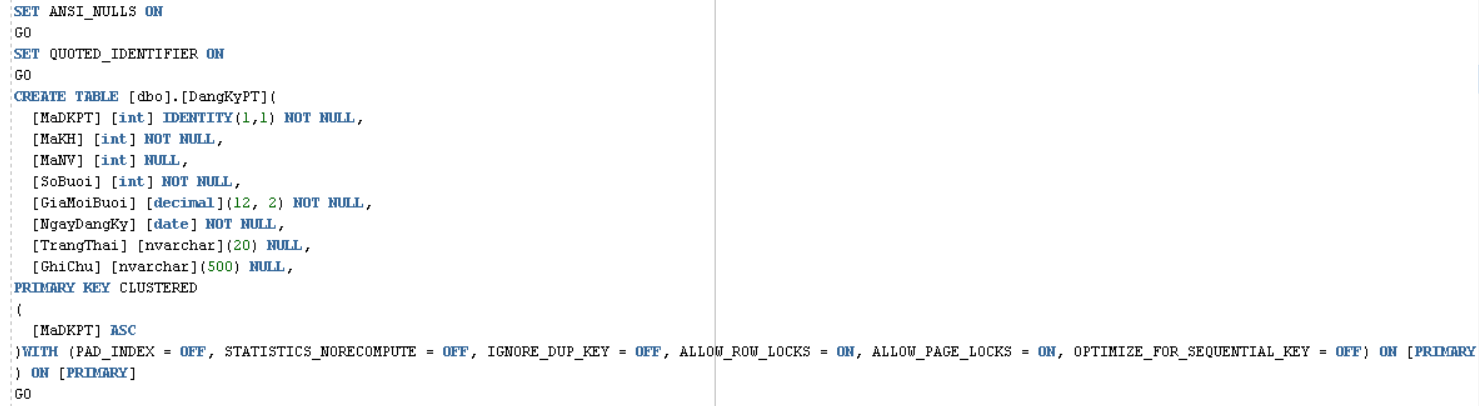
Hình 6 Bảng DANGKYGOITAP

* **Bảng DANGKYLOP**

****

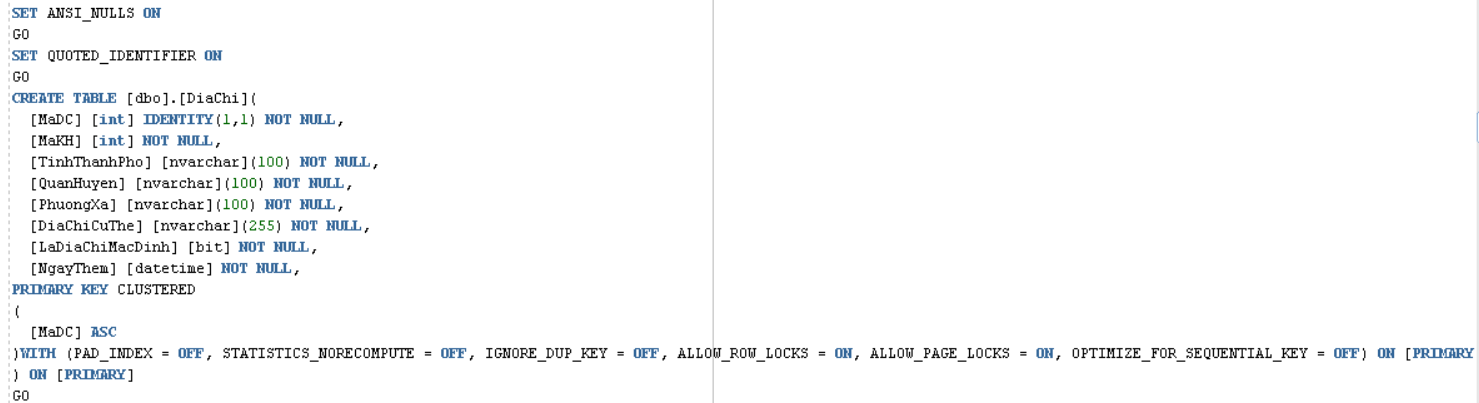
Hình 7 Bảng DANGKYLOP

* **Bảng DANGKYPT**

****

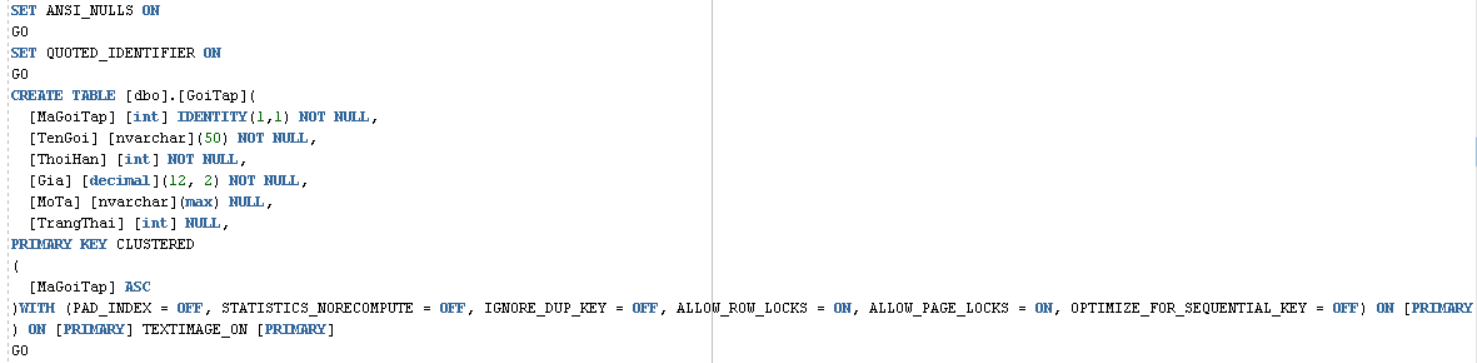
Hình 8 Bảng DANGKYPT

* **Bảng DIACHI**

****

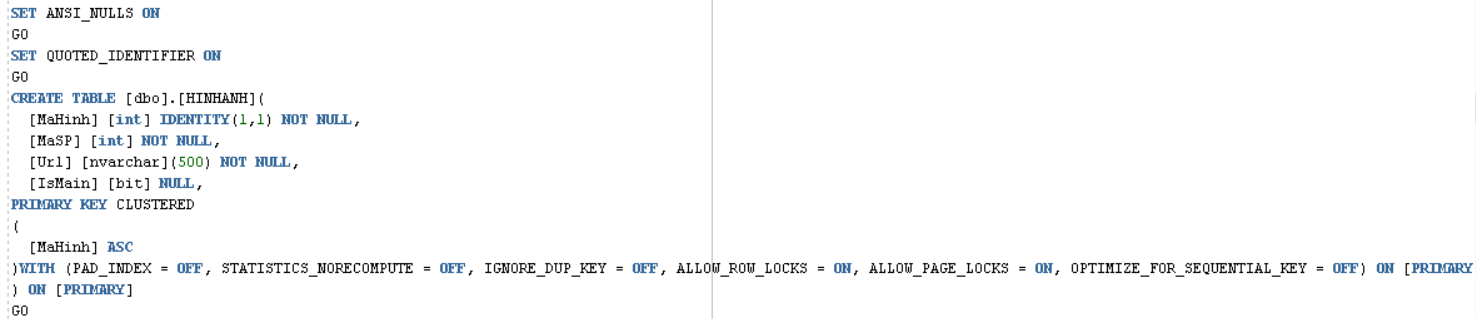
Hình 9 Bảng DIACHI

* **Bảng GOITAP**

****

Hình 10 Bảng GOITAP

* **Bảng HINHANH**

****

Hình 11 Bảng HINHANH

* **Bảng HOADON**

****

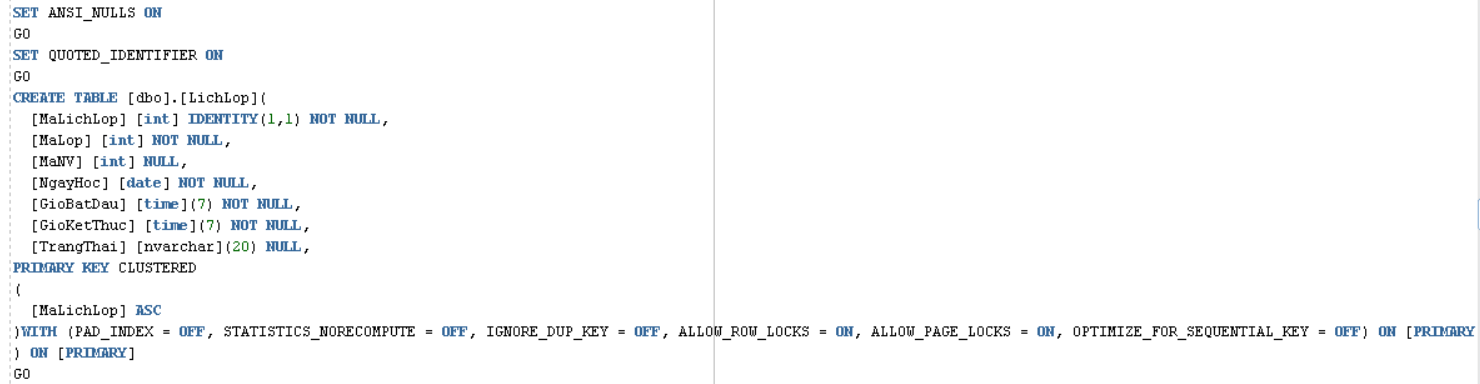
Hình 12 Bảng HOADON

* **Bảng KHACHHANG**

****

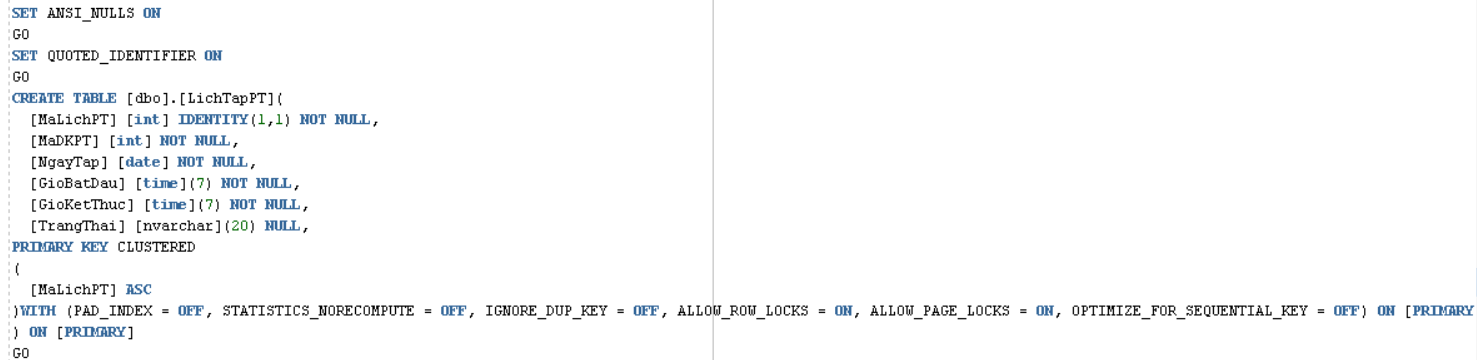
Hình 13 Bảng KHACHHANG

* **Bảng LICHLOP**

****

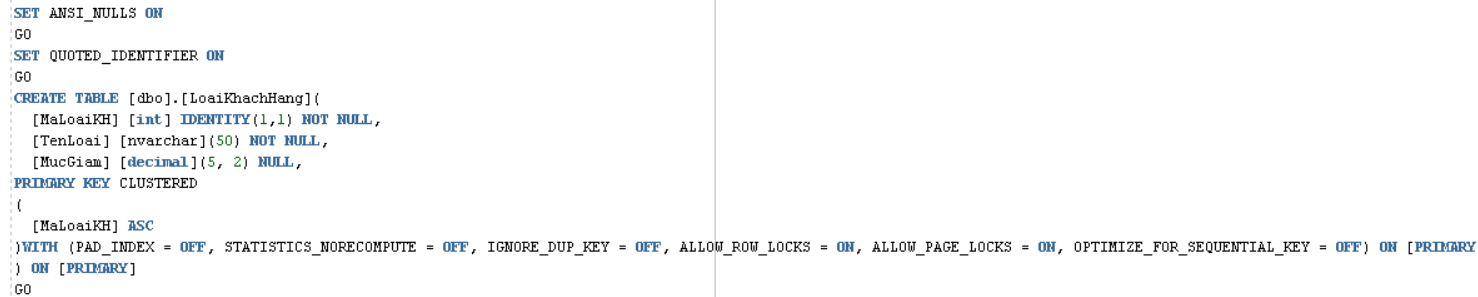
Hình 14 Bảng LICHLOP

* **Bảng LICHTAPPT**

****

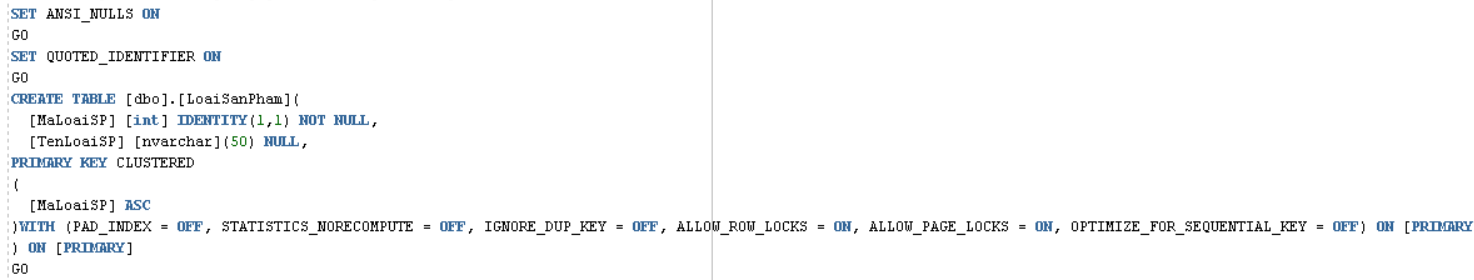
Hình 15 Bảng LICHTAPPT

* **Bảng LOAIKHACHHANG**

****

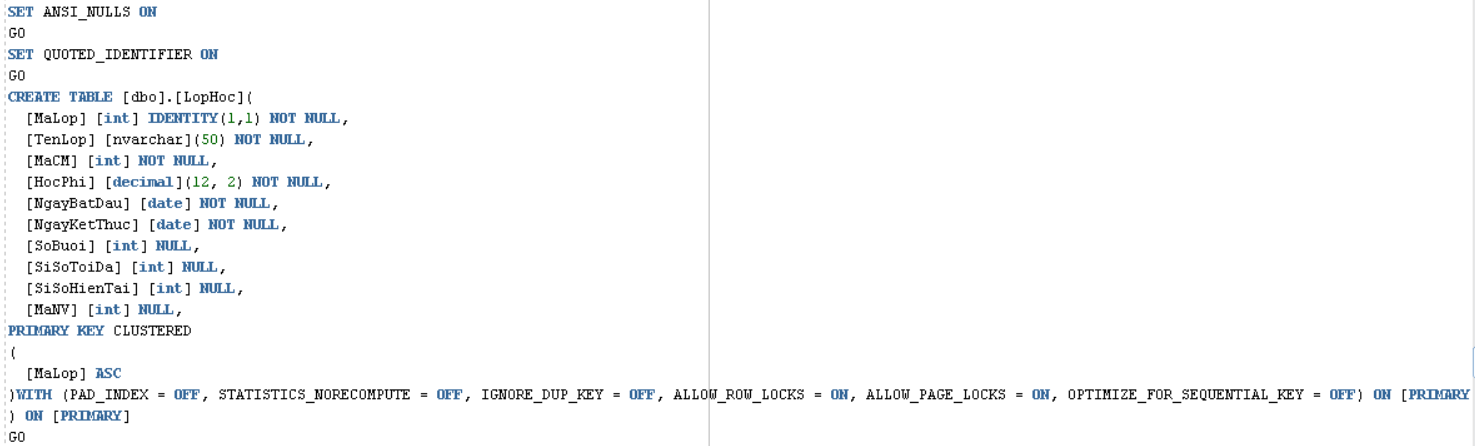
Hình 16 Bảng LOAIKHACHHANG

* **Bảng LOAISANPHAM**

****

Hình 17 Bảng LOAISANPHAM

* **Bảng LOPHOC**

****

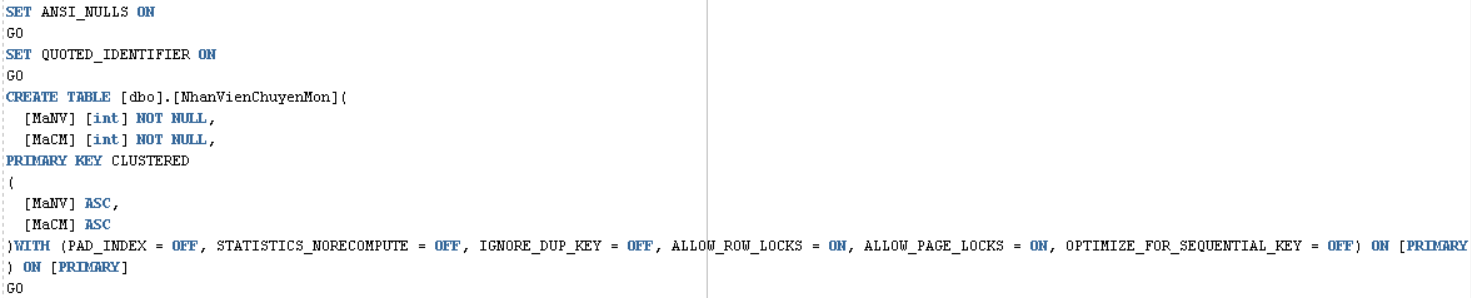
Hình 18 Bảng LOPHOC

* **Bảng NHANVIEN**

****

Hình 19 Bảng NHANVIEN

* **Bảng NHANVIENCHUYENMON**

****

Hình 20 Bảng NHANVIENCHUYENMON

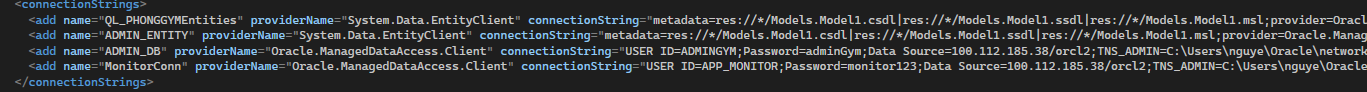
* **Bảng SANPHAM**

****

Hình 21 Bảng SANPHAM

## **1.3 Xây dựng ứng dụng kết nối đến cơ sở dữ liệu:**

### **1.3.1 Cấu hình kết nối (Constring):**

****

Hình 22 Cấu hình kết nối

**Server:** 100.112.185.38 (Remote Server) - Ứng dụng kết nối tới Server thật chứ không chỉ chạy Localhost.

**Cơ chế kết nối**: Sử dụng song song 2 cơ chế:

* **Entity Framework 6 (ORM):** Dùng cho các thao tác nghiệp vụ chính (CRUD) giúp code gọn gàng, bảo mật.
* **ADO.NET (Raw SQL):** Dùng cho các tác vụ quản trị hoặc báo cáo cần hiệu năng cao.

### **1.3.2 Bảo mật kết nối:**

Để đảm bảo an toàn dữ liệu theo nguyên tắc **Least Privilege (Quyền tối thiểu)**, ứng dụng không dùng một tài khoản 'sa' hay 'sys' cho mọi việc, mà chia tách thành các luồng kết nối riêng biệt

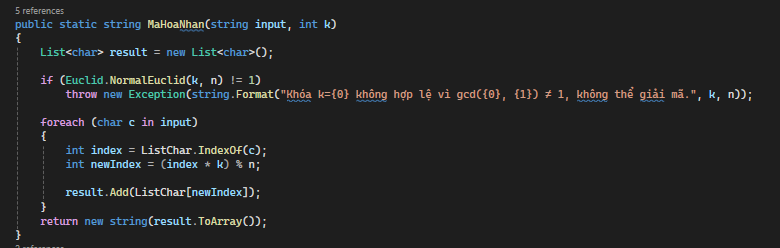
* Kết nối Người dùng (User Connection):
* Tên chuỗi: QL\_PHONGGYMEntities
* User DB: APPUSER
* Mục đích: Dành cho các chức năng của hội viên và nhân viên thông thường. Tài khoản này chỉ có quyền thao tác trên các bảng nghiệp vụ, không được can thiệp cấu trúc bảng.
* Kết nối Quản trị (Admin Connection):
* Tên chuỗi: ADMIN\_ENTITY / ADMIN\_DB
* User DB: ADMINGYM
* Mục đích: Dành riêng cho module Admin. Tài khoản này có quyền cao hơn để quản lý hệ thống, cấp quyền hoặc sửa đổi dữ liệu nhạy cảm.
* Kết nối Giám sát (Monitor Connection):
* Tên chuỗi: MonitorConn
* User DB: APP\_MONITOR
* Mục đích: Dành cho các service chạy ngầm hoặc dashboard theo dõi trạng thái hệ thống.

# **CHƯƠNG 2: MÃ HÓA**

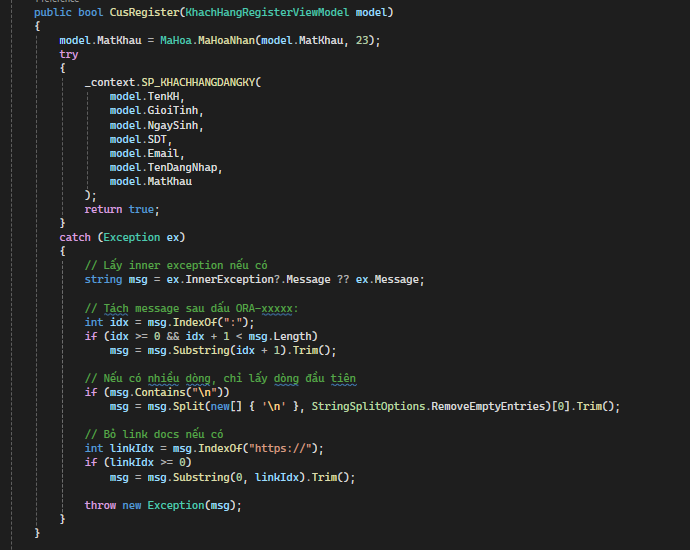
## **2.1 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa đối xứng ở mức ứng dụng, cơ sở dữ liệu**

### **2.1.1 Áp dụng mã hóa nhân**

* Dùng mã hóa nhân (k = 23) để mã hóa mật khẩu người dùng tại Repository trước khi gọi Stored Procedure lưu xuống Oracle Database



Hình 23 mã hóa nhân



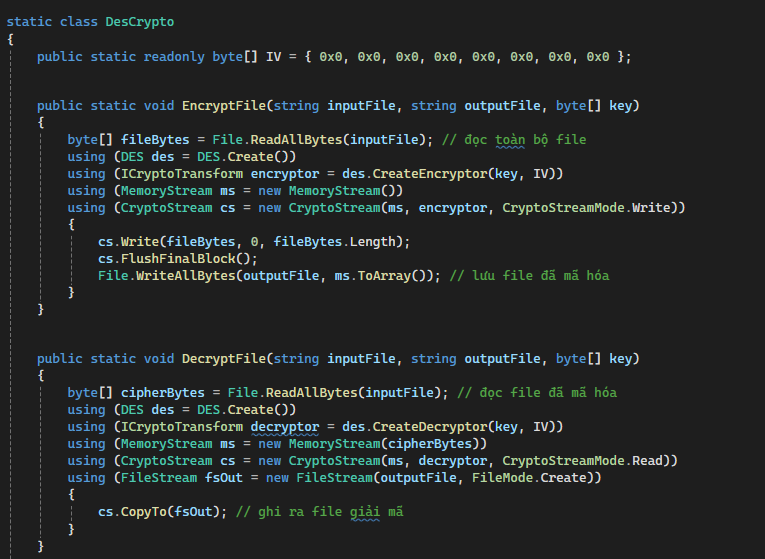
Hình 24 CurReigister



Hình 25 CusLogin

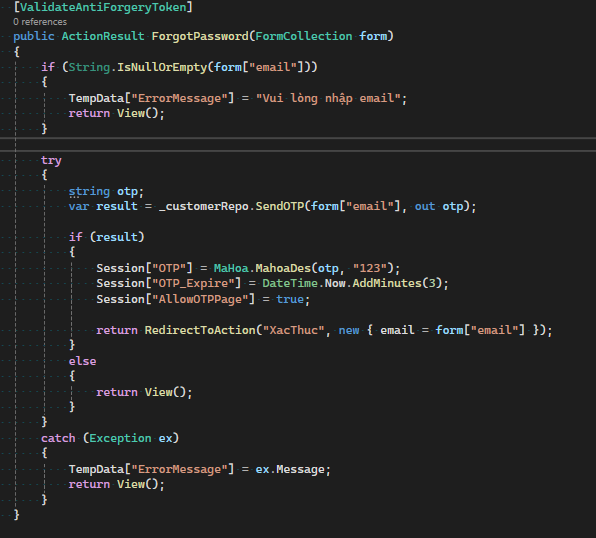
### **2.1.2 Áp dụng mã hóa DES**

* Khi người dùng sử dụng chức năng Quên mật khẩu, một mã xác thực (OTP) ngẫu nhiên được sinh ra. Trước khi lưu vào bộ nhớ phiên làm việc (Session) để phục vụ quá trình xác thực sau này, hệ thống sẽ sử dụng thuật toán DES với khóa bí mật là 8 bytes để mã hóa mã OTP này.
* Hàm mã hóa DES



Hình 26 DES

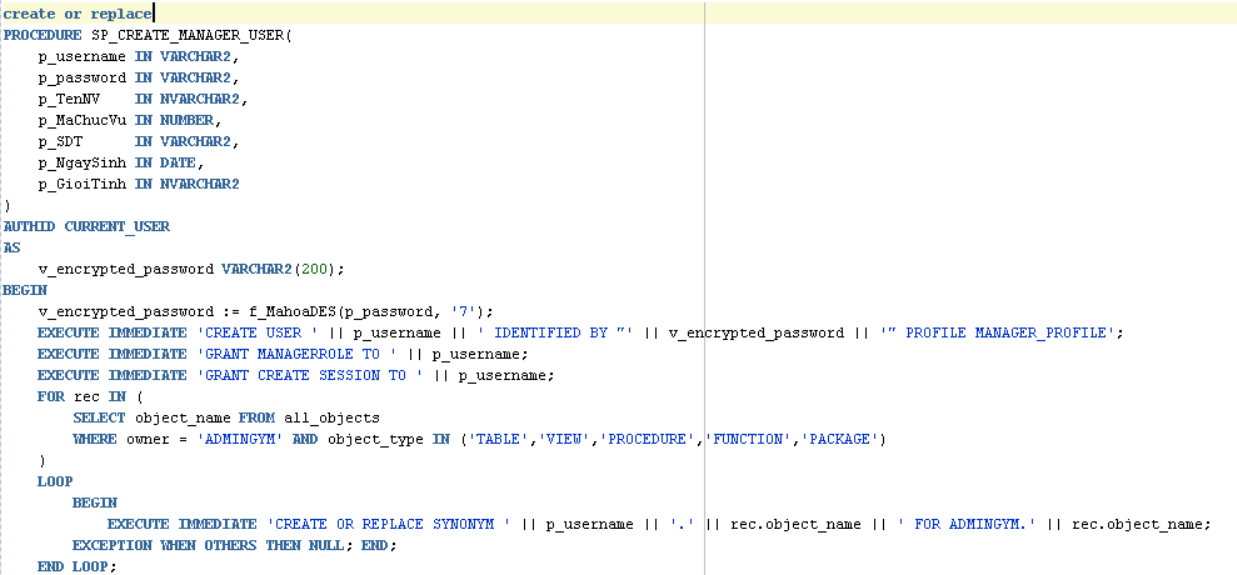
* Áp dụng vào Action Quên mật khẩu



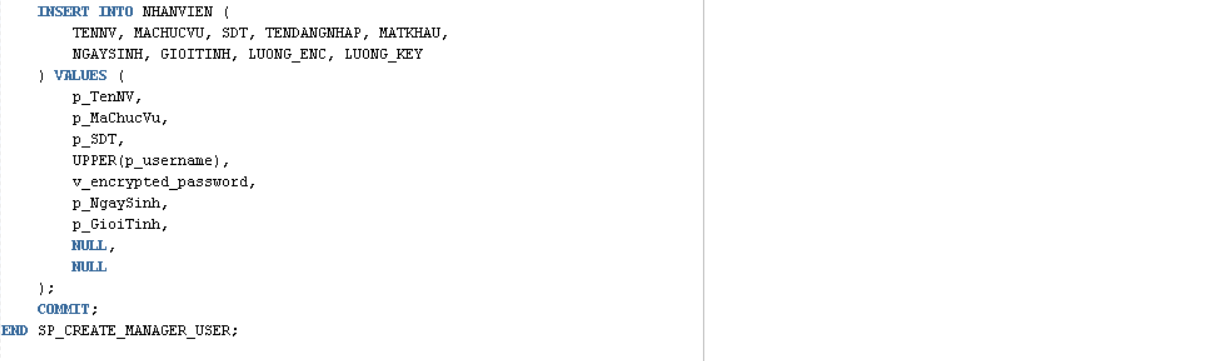
Hình 27 ForgotPassword Action

* Áp dụng mã hóa DES mật khẩu lúc tạo nhân viên:

Mục tiêu: Đảm bảo an toàn thông tin khi tạo mới nhân viên. Mật khẩu của nhân viên không được lưu trữ dưới dạng văn bản thuần mà phải được mã hóa qua thuật toán DES trước khi lưu vào cơ sở dữ liệu và khởi tạo User trên hệ thống Oracle.



Hình 28 Mã hóa mật khẩu nhân viên

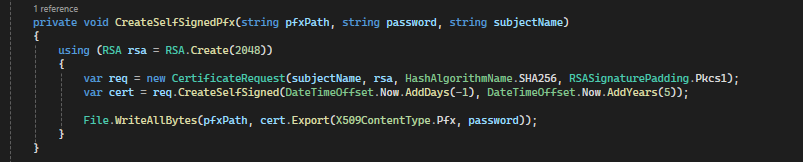


Hình 29 Mã hóa mật khẩu nhân viên

* Mã hóa dữ liệu: Sử dụng hàm con f\_MahoaDES để chuyển đổi mật khẩu người dùng nhập vào thành chuỗi mã hóa. Điều này giúp ngăn chặn việc lộ mật khẩu ngay cả khi quản trị viên truy cập trực tiếp vào bảng NHANVIEN.
* Cơ chế thực thi: Sử dụng EXECUTE IMMEDIATE để thực thi các câu lệnh DDL (Create User, Grant) một cách linh hoạt trong Stored Procedure.
* Phân quyền (Privileges): Sau khi tạo User, hệ thống tự động cấp Role MANAGERROLE để giới hạn quyền hạn của nhân viên đó đúng với chức trách.
* Tính toàn vẹn: Thông tin nhân viên và thông tin tài khoản hệ thống được đồng bộ hóa trong cùng một tiến trình giao dịch.

## **2.2 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa bất đối xứng ở mức ứng dụng, cơ sở dữ liệu**

* Hàm này để khởi tạo thuật toán RSA 2048 bit



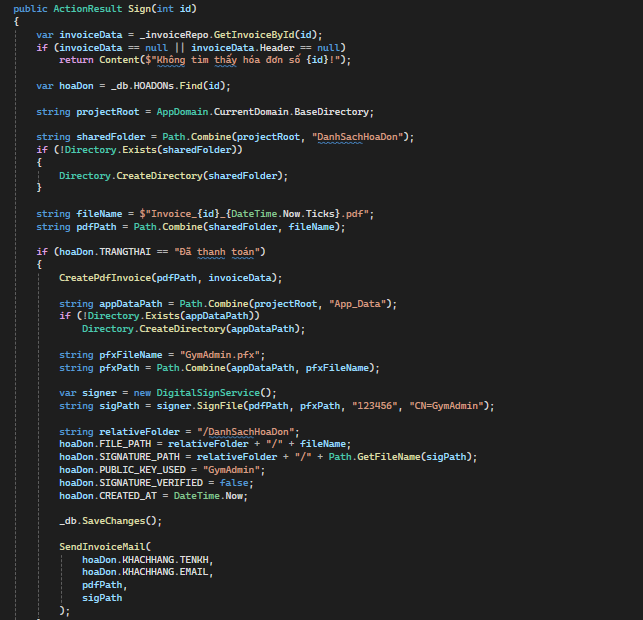
Hình 30 RSA

* Hàm này tự động băm (Hash) dữ liệu bằng SHA256, sau đó dùng Private Key RSA để mã hóa cái Hash đó => Tạo ra chữ ký.



Hình 31 Hash

* Tại Controller thanh toán, sau khi khách hàng thanh toán thành công, hệ thống gọi dịch vụ ký số để đóng dấu hóa đơn trước khi gửi email cho khách.



Hình 32 Sing

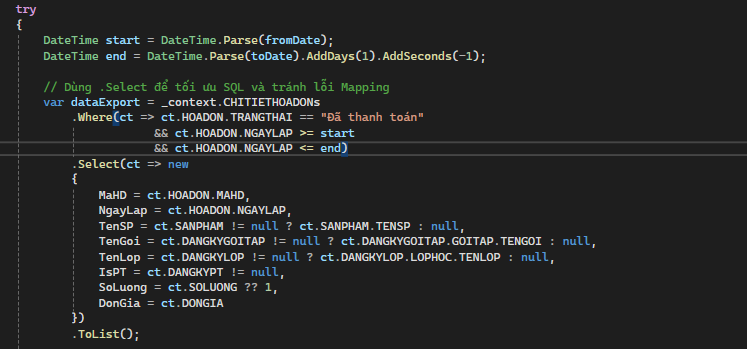
## **2.3 Cài đặt chức năng xử lý nghiệp vụ có tích hợp mã hóa lai ở mức ứng dụng, cơ sở dữ liệu**

Chức năng xuất báo cáo doanh thu được thiết kế để bảo mật dữ liệu nhạy cảm thông qua cơ chế mã hóa lai (Hybrid Encryption), kết hợp giữa **DES** (tốc độ cao) và **RSA** (bảo mật khóa).

#### 2.3.1 Triển khai tại lớp ứng dụng (Controller)

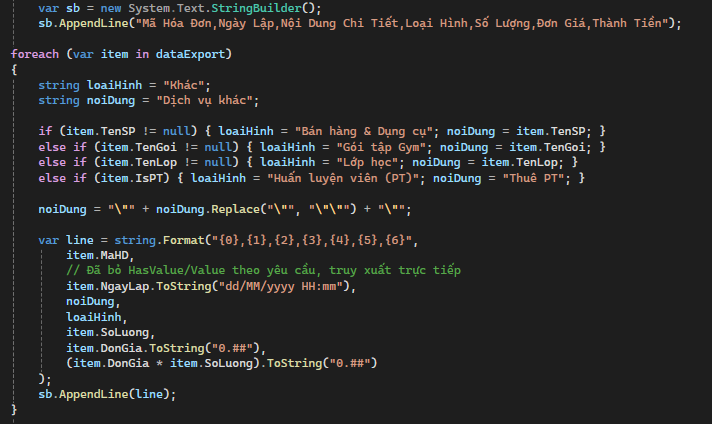
Quy trình thực thi tại Controller được chia thành 3 giai đoạn chính:

**Giai đoạn 1: Truy vấn và tối ưu hóa dữ liệu** Hệ thống sử dụng LINQ kết hợp phương thức .Select() để thực hiện kỹ thuật **Projection**. Điều này giúp chỉ lấy đúng các trường thông tin cần thiết từ cơ sở dữ liệu, tối ưu hóa băng thông và bộ nhớ RAM của Web Server.



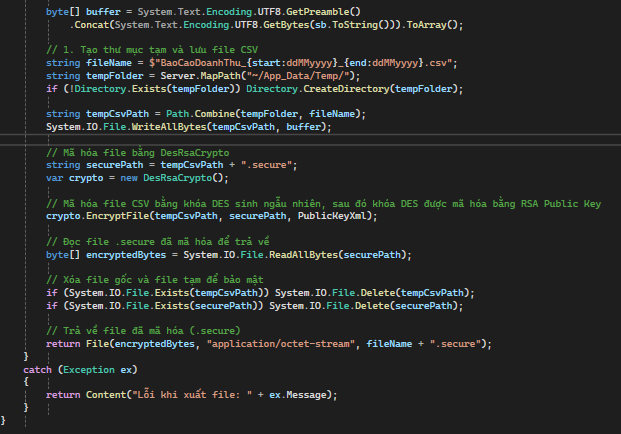
Hình 33 DataExport

**Giai đoạn 2: Định dạng nội dung báo cáo (CSV)** Dữ liệu sau khi truy vấn được duyệt qua vòng lặp để phân loại nghiệp vụ (Gói tập, Sản phẩm, Lớp học...). Toàn bộ nội dung được xây dựng bằng StringBuilder để đạt hiệu suất tối ưu và được xử lý định dạng chuẩn CSV (bao gồm việc xử lý dấu ngoặc kép và Encoding UTF-8 có BOM để hiển thị đúng tiếng Việt trong Excel).



Hình 34 CSV

**Giai đoạn 3: Thực thi mã hóa lai và quản lý tệp tạm** Sau khi file CSV thô được tạo thành công, hệ thống gọi lớp DesRsaCrypto để thực hiện mã hóa. Để đảm bảo an toàn, tệp tin gốc và tệp tin tạm đều được xóa khỏi Server ngay sau khi dữ liệu đã được chuyển đổi thành mảng byte mã hóa và gửi trả về trình duyệt người dùng.

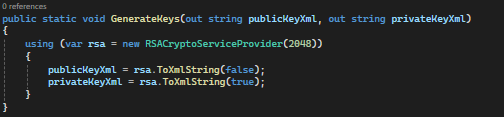


Hình 35 Mã hóa lai

#### **2.3.2 Cài đặt các hàm hỗ trợ trong lớp DesRsaCrypto**

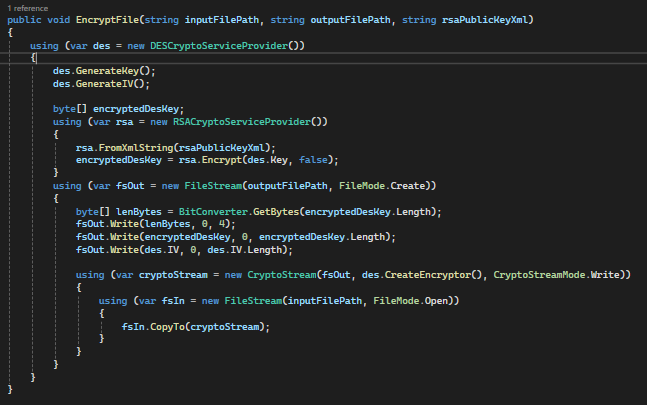
Lớp DesRsaCrypto đóng vai trò là thư viện xử lý các thuật toán mã hóa cấp thấp.

**Hàm GenerateKeys:** Khởi tạo cặp khóa RSA 2048-bit. Khóa công khai (Public Key) được dùng để mã hóa khóa phiên, trong khi khóa bí mật (Private Key) được giữ an toàn để giải mã.



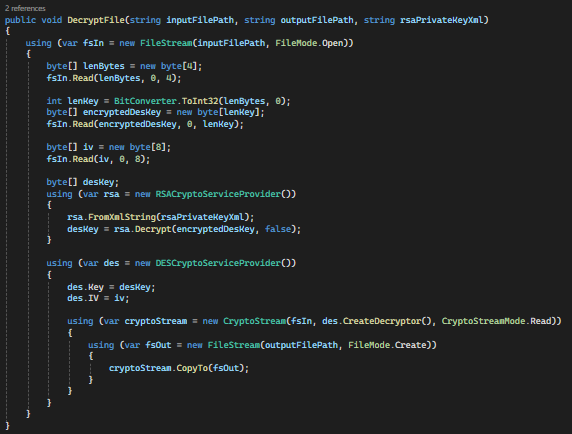
Hình 36 Key

**Hàm EncryptFile (Mã hóa):** 1. Sinh ngẫu nhiên một khóa **DES Key** và **IV** cho mỗi lần xuất báo cáo. 2. Dùng RSA Public Key để mã hóa khóa DES này. 3. Dùng khóa DES ban đầu mã hóa toàn bộ nội dung file qua CryptoStream.



Hình 37 EncryptFile

**Hàm DecryptFile (Giải mã):** Thực hiện bóc tách Header của file để lấy lại khóa DES (đã giải mã bằng RSA Private Key), từ đó khôi phục lại nội dung báo cáo gốc.

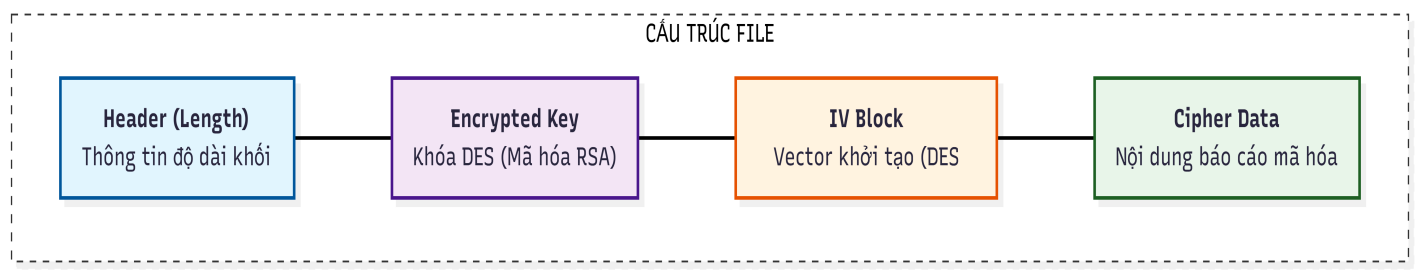


Hình 38 DecryltFile

#### **2.3.3 Cấu trúc đóng gói tệp tin bảo mật (.secure)**

Tệp tin đầu ra được thiết kế theo cấu trúc nhị phân đặc biệt để đảm bảo tính toàn vẹn và khả năng giải mã chính xác:

| **Thành phần** | **Độ dài** | **Mô tả** |
| --- | --- | --- |
| **Header (Length)** | 4 bytes | Lưu độ dài của khóa DES đã được mã hóa RSA. |
| **Encrypted Key** | Biến thiên | Khóa đối xứng DES đã được bảo vệ bởi RSA. |
| **IV Block** | 8 bytes | Vector khởi tạo phục vụ thuật toán DES. |
| **Cipher Data** | Biến thiên | Toàn bộ nội dung báo cáo đã được mã hóa hoàn toàn. |

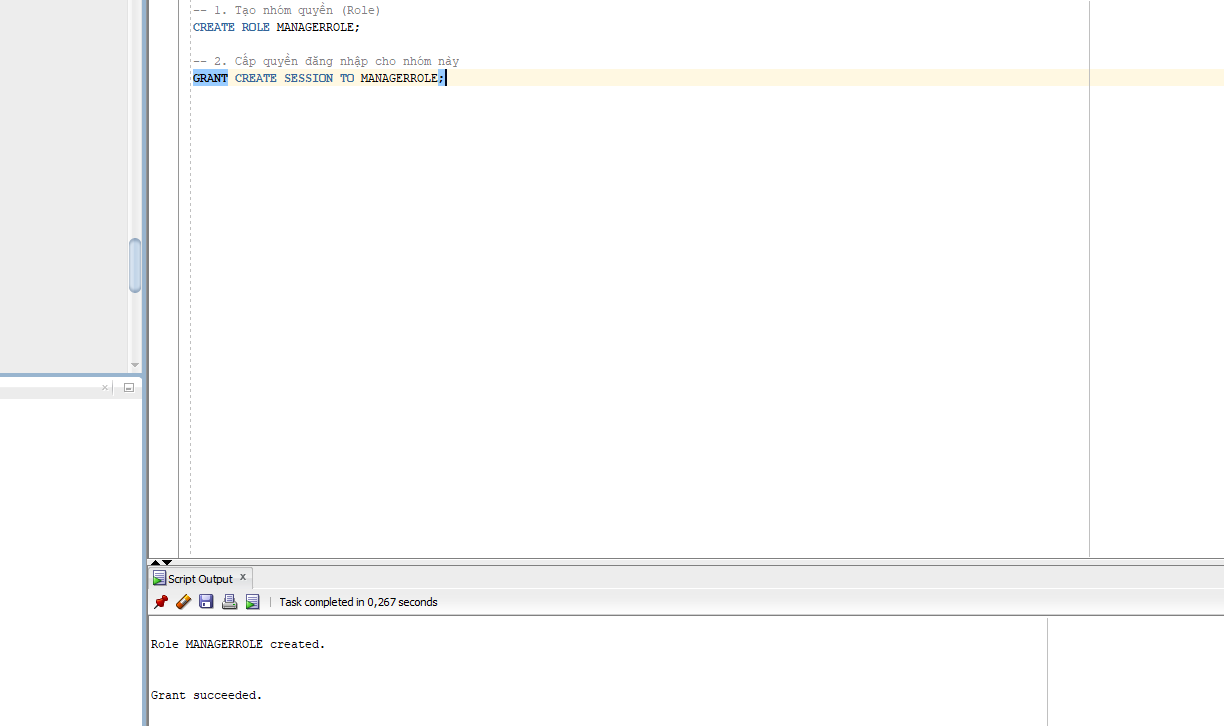
****

# **CHƯƠNG 3: ĐIỀU KHIỂN TRUY CẬP**

## **3.1 Cài đặt nhóm quyền, profile, session, tablespace**

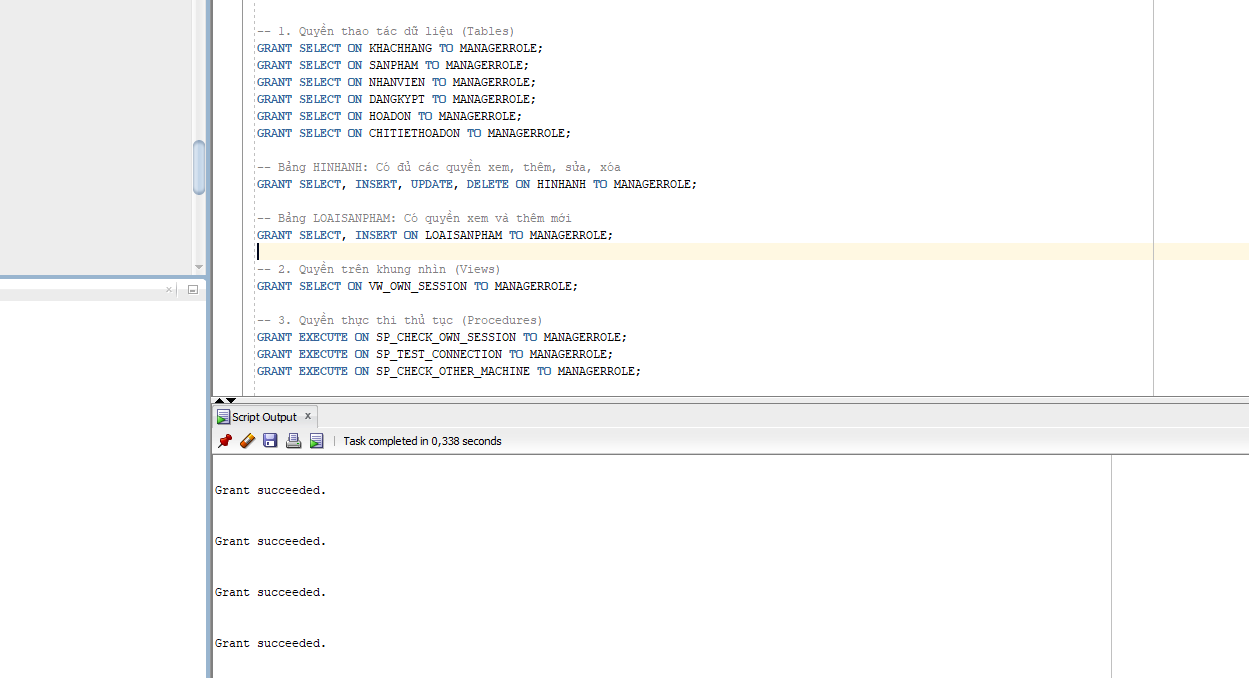
### **3.1.1. Cài đặc nhóm quyền**

Mã lệnh tạo nhóm quyền MANAGERROLE:



Hình 39 managerole

Các câu lệnh và kết quả gán quyền cho ManagerRole:



Hình 40 grant

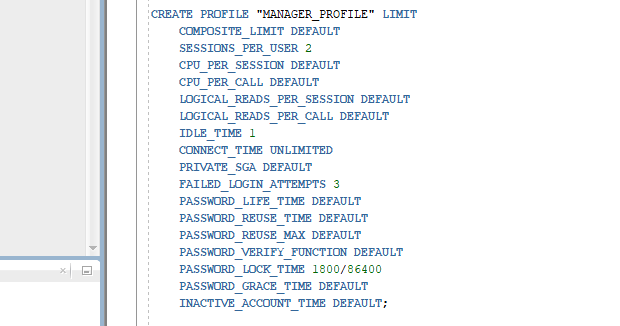
Stored Procedure tự động khởi tạo tài khoản và phân quyền cho nhân viên mới:



Hình 41 procedure tạo tài khoản và phân quyền

### **3.1.2. Thiết lập Profile quản lý chính sách người dùng.**

Mã lệnh khởi tạo MANAGER\_PROFILE:



Hình 42 khởi tạo profile

**c. Giải thích các tham số quan trọng:**

**SESSIONS\_PER\_USER 2:** Giới hạn mỗi tài khoản quản lý chỉ được mở tối đa **2 phiên làm việc** đồng thời. Điều này giúp ngăn chặn việc chia sẻ tài khoản cho nhiều người sử dụng trái phép.

**IDLE\_TIME 1:** Hệ thống sẽ tự động ngắt kết nối nếu người dùng không thực hiện thao tác nào trong vòng **1 phút**. Đây là biện pháp bảo mật tránh trường hợp người dùng quên đăng xuất khi rời khỏi máy tính.

**FAILED\_LOGIN\_ATTEMPTS 3:** Giới hạn số lần nhập sai mật khẩu là **3 lần**. Biện pháp này nhằm ngăn chặn các cuộc tấn công dò mật khẩu (Brute Force).

**PASSWORD\_LOCK\_TIME 1800/86400:** Thời gian khóa tài khoản sau khi nhập sai quá số lần quy định. Vì Oracle tính thời gian theo đơn vị Ngày (Day). Công thức 1800/86400 tương ứng với 1800 giây, tức là tài khoản sẽ bị khóa tạm thời trong **30 phút** trước khi được phép thử đăng nhập lại.

### **3.1.3. Xây dựng các thủ tục (Stored Procedures) quản lý Session**

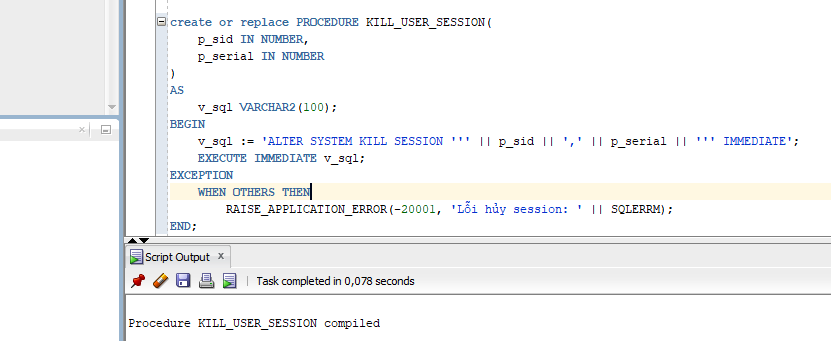
**a. Thủ tục lấy danh sách phiên làm việc**  
Thủ tục GET\_USER\_SESSIONS giúp người quản trị xem toàn bộ các kết nối đang hoạt động của một tài khoản cụ thể, bao gồm thông tin máy trạm (Machine) và trạng thái (Status).



Hình 43 Thủ tục lấy danh sách phiên làm việc

**b. Thủ tục ngắt kết nối (Kill Session)**

Thủ tục KILL\_USER\_SESSION thực hiện quyền ngắt kết nối cưỡng chế đối với các phiên làm việc bị treo hoặc vi phạm chính sách. *(Lưu ý: Sử dụng EXECUTE IMMEDIATE để chạy câu lệnh động)*.

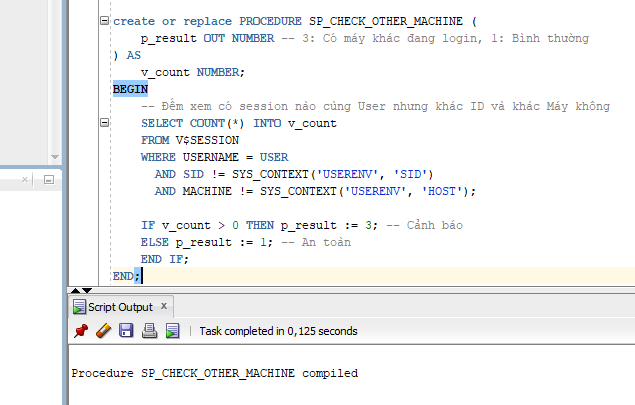


Hình 44 Thủ tục ngắt kết nối (Kill Session)

#### **c. Thủ tục kiểm tra và cảnh báo bảo mật**

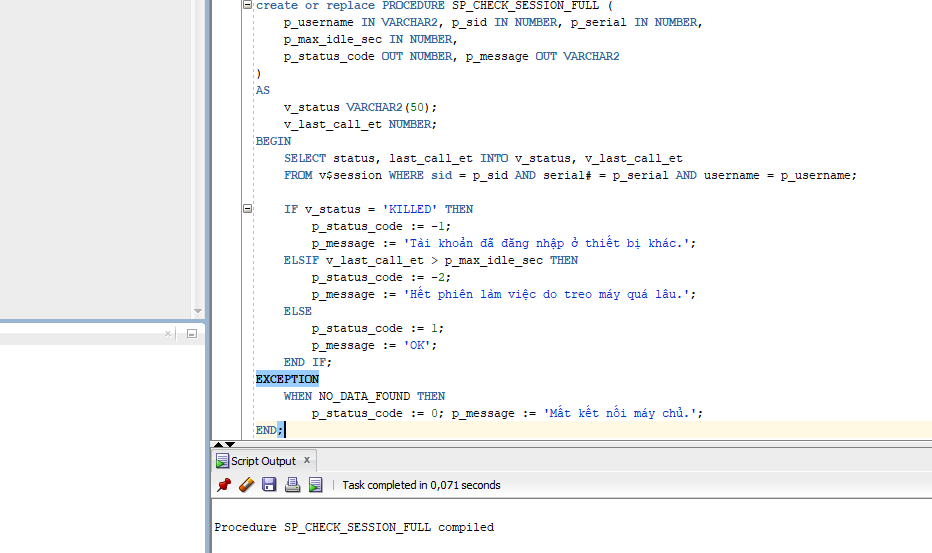
Đây là phần xử lý nghiệp vụ quan trọng nhằm phát hiện các hành vi đăng nhập bất thường (đăng nhập đè từ máy khác) hoặc hết thời gian chờ (Timeout).

Logic phát hiện đăng nhập từ máy khác (SP\_CHECK\_OTHER\_MACHINE):



Hình 45 kiểm tra cảnh báo bảo mật

Logic kiểm tra trạng thái chi tiết để phản hồi cho giao diện (SP\_CHECK\_SESSION\_FULL):



Hình 46 kiểm tra trạng thái chi tiết

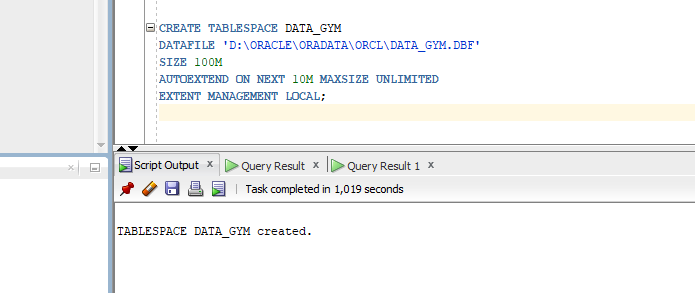
Stored Procedure tự động khởi tạo tài khoản và phân quyền cho nhân viên mới:



Hình 47 cấp quyền

### **3.1.4. Cấu hình Tablespace**

Mã Lệnh khởi tạo Tablespace DATA\_GYM



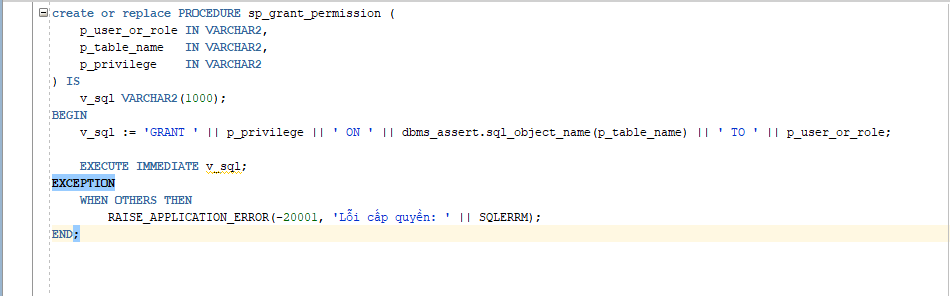
Hình 48 khởi tạo lệnh DATA\_GYM

## **3.2 Cài đặt ứng dụng phân quyền, nhóm quyền để điều khiển truy cập**

#### **3.2.1. Xây dựng Thủ tục cấp quyền động (Stored Procedures)**

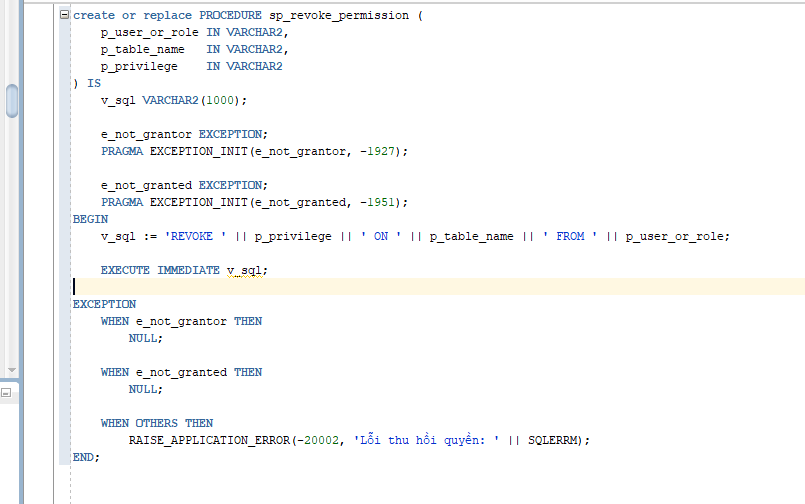
Sử dụng kỹ thuật **Dynamic SQL** (Câu lệnh động) trong Oracle để thực thi các lệnh DCL (Data Control Language) thông qua tham số truyền vào từ ứng dụng.

**Thủ tục cấp quyền (sp\_grant\_permission):**



Hình 49 grant

**Thủ tục thu hồi quyền (sp\_revoke\_permission):**

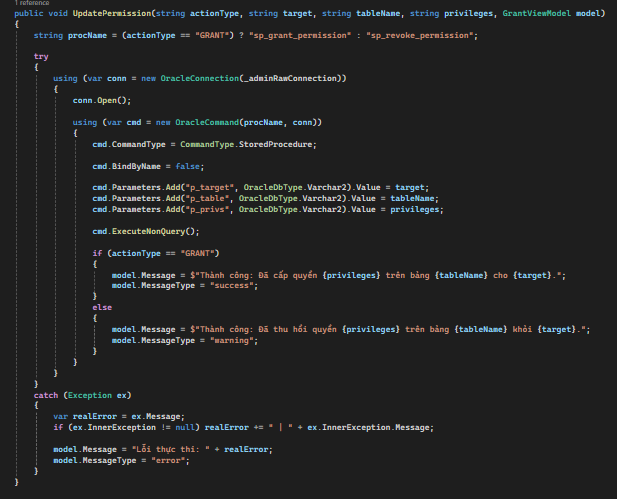


Hình 50 thu hồi quyền

#### **3.2.2. Xử lý nghiệp vụ tại tầng Ứng dụng (C# Backend)**

Tại tầng Controller và Repository, ứng dụng tiếp nhận yêu cầu từ giao diện, xác định loại hành động (Cấp/Thu hồi) và gọi thủ tục lưu trữ tương ứng.

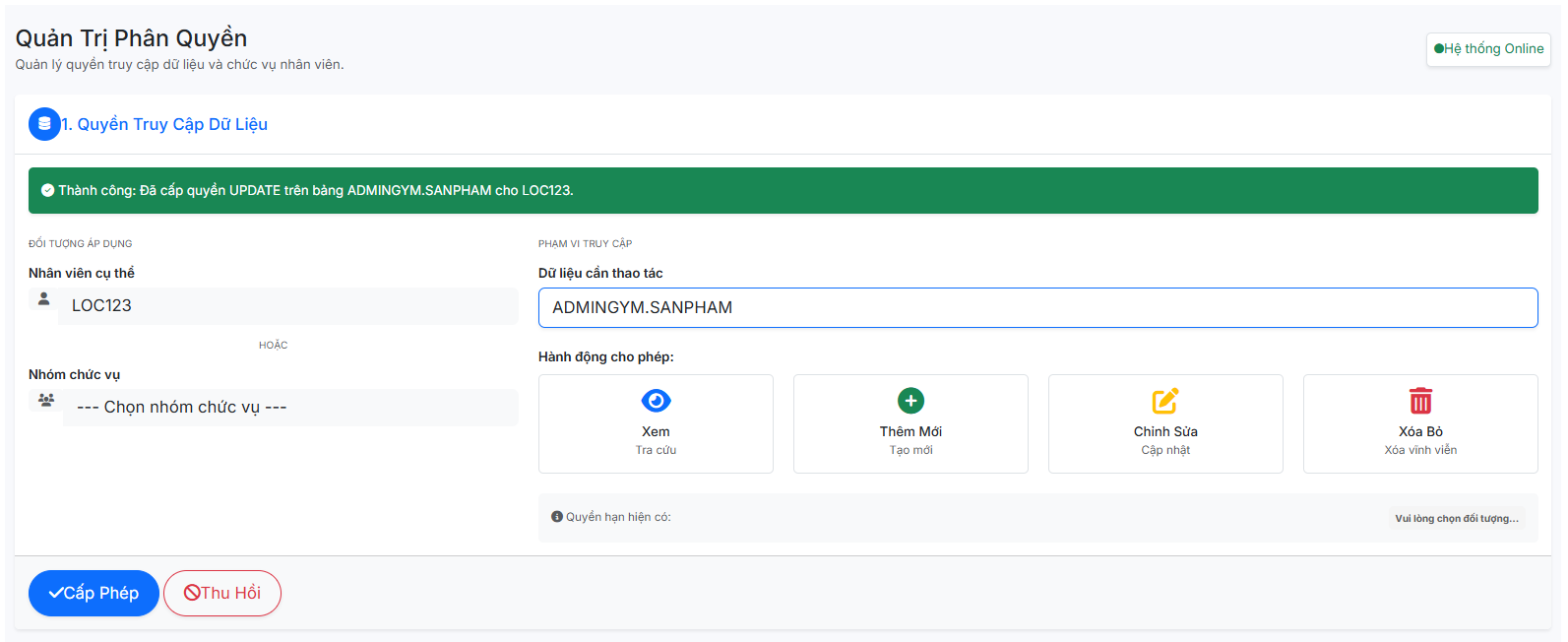
**Hàm xử lý cập nhật quyền (Repository):**



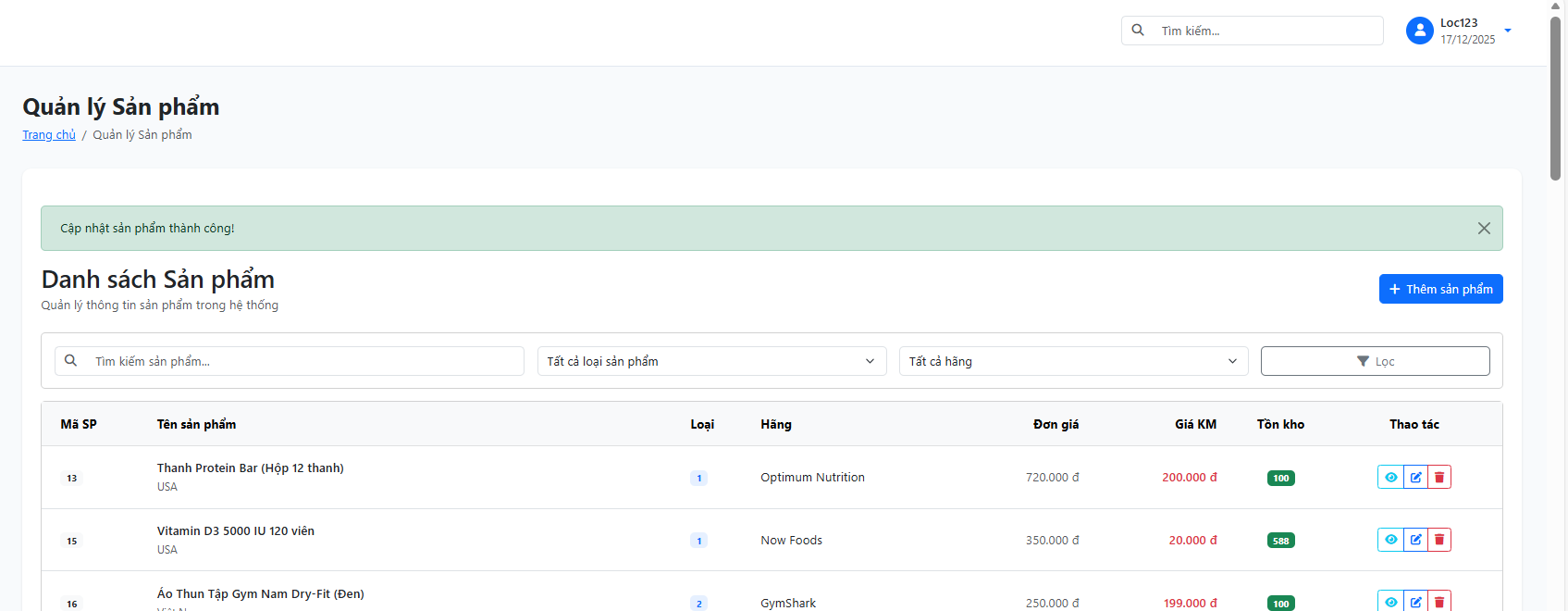
Hình 51 hàm cập nhật quyền

#### **3.2.3. Giao diện Quản trị Phân quyền**

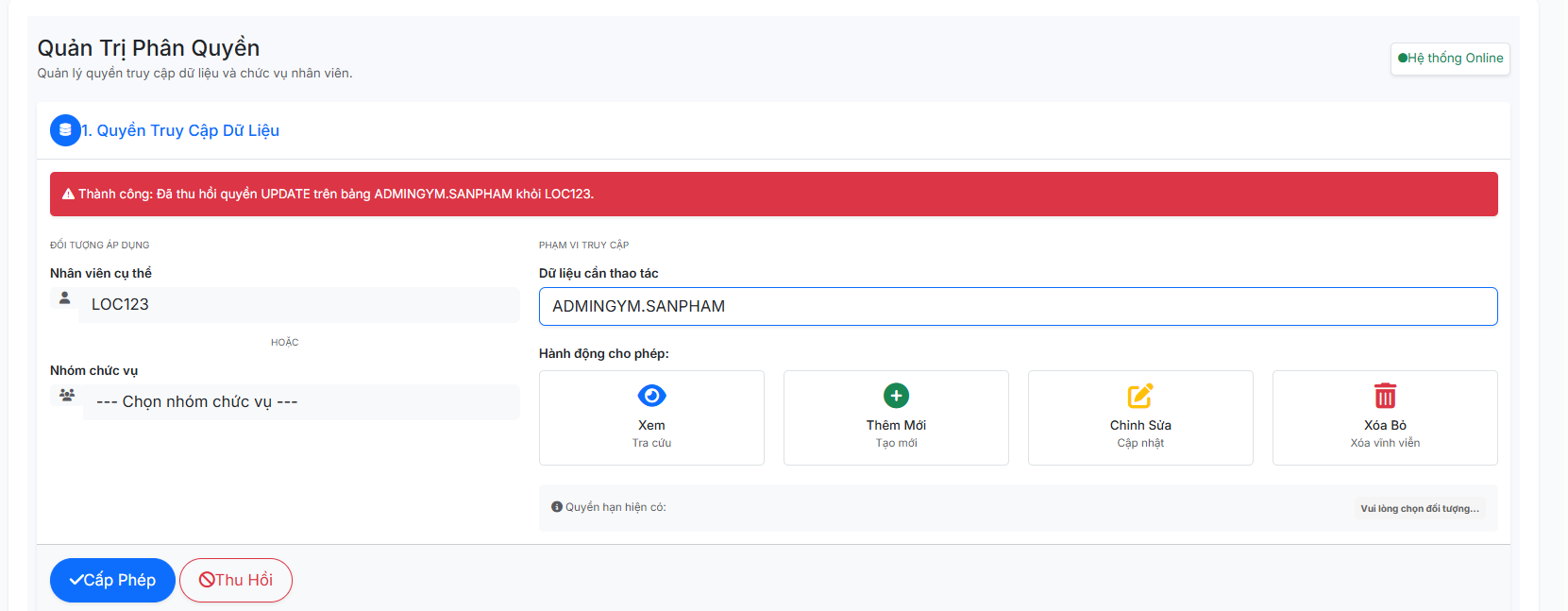
Giao diện được thiết kế để Admin dễ dàng chọn đối tượng (Nhân viên/Nhóm), chọn bảng dữ liệu và tích chọn các hành động cho phép (Xem, Thêm, Sửa, Xóa).



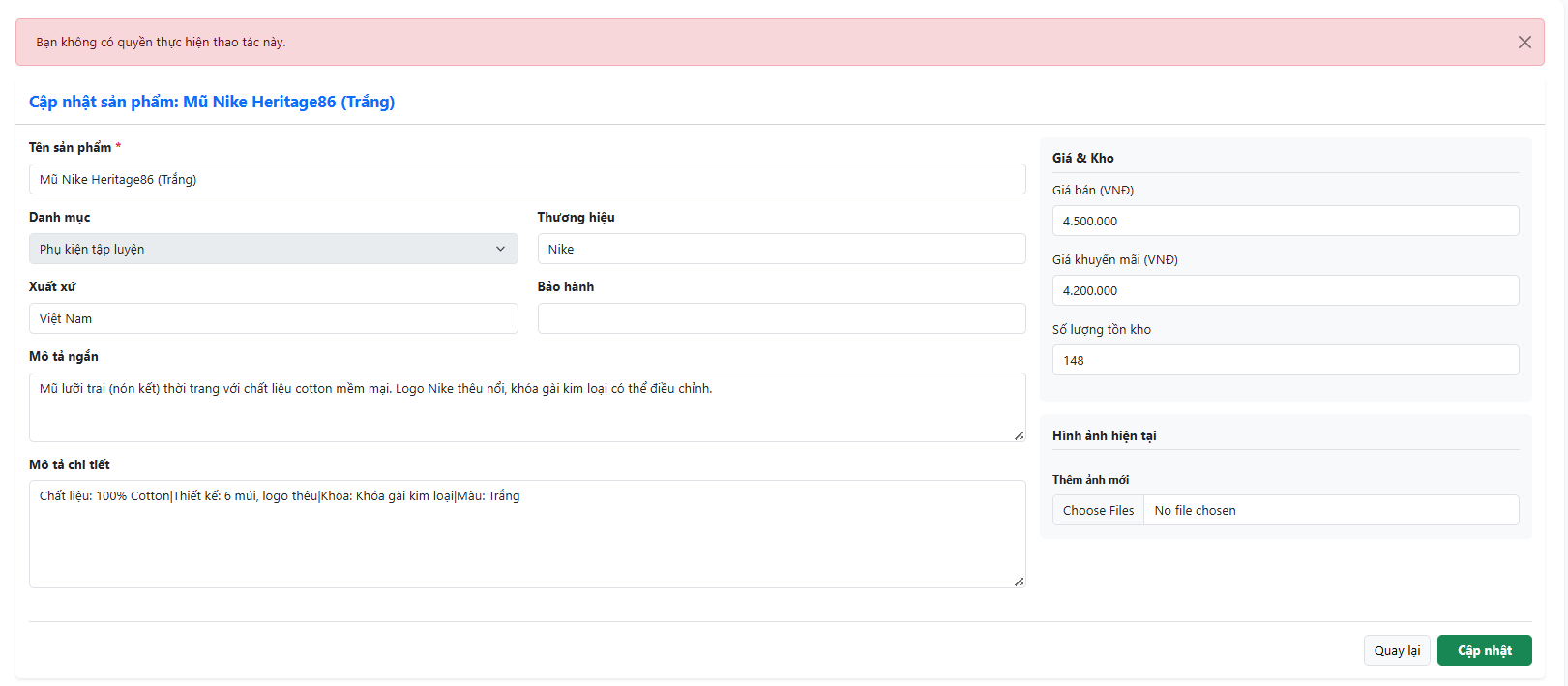
Hình 52 giao diện phân quyền



Hình 53 giao diện quản lý sản phẩm



Hình 54 quản trị phân quyền



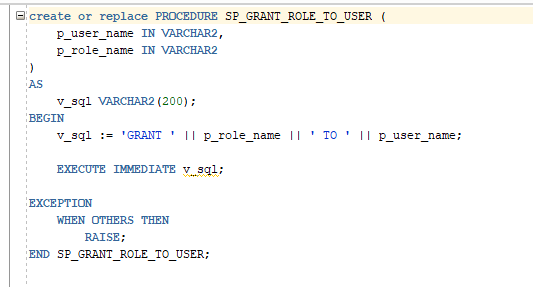
Hình 55 cập nhật sản phẩm

### **3.2.1. Chức năng Bổ nhiệm và Quản lý Nhóm quyền (Role Management)**

**a. Mục đích** Thay vì cấp từng quyền nhỏ lẻ, hệ thống cho phép quản trị viên "Bổ nhiệm" (Grant Role) hoặc "Bãi nhiệm" (Revoke Role) nhân viên vào các nhóm chức vụ cụ thể (Ví dụ: SANPHAMROLE, MANAGERROLE). Điều này giúp việc quản lý phân quyền trở nên gọn gàng và nhất quán.

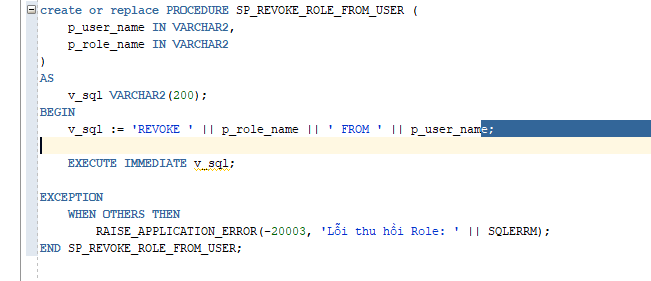
**b. Xây dựng Thủ tục cấp Role động (Database Layer)** Do lệnh GRANT và REVOKE Role là các lệnh DDL, chúng không thể chạy trực tiếp trong khối PL/SQL tĩnh mà phải sử dụng kỹ thuật **Dynamic SQL** (EXECUTE IMMEDIATE).

**Thủ tục Bổ nhiệm (Grant Role):**



Hình 56 thủ tục bổ nhiệm

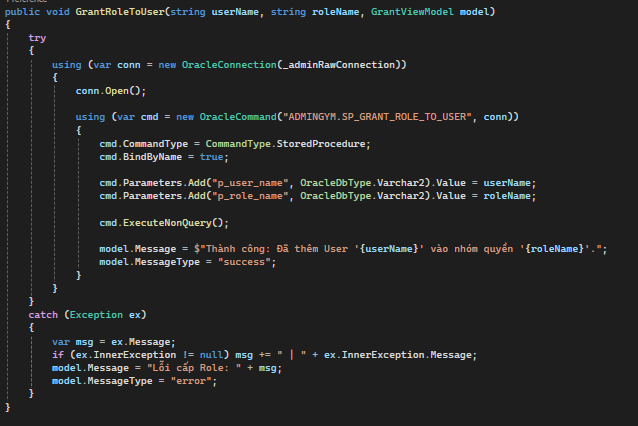
**Thủ tục Bãi nhiệm (Revoke Role):**



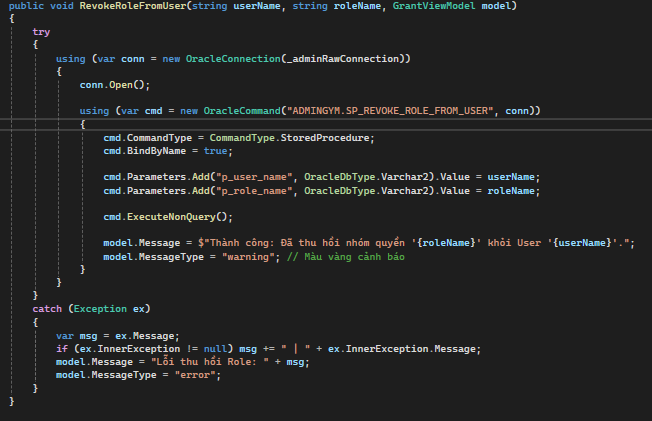
Hình 57 thủ tục bãi nhiệm

**c. Xử lý nghiệp vụ tại Ứng dụng (Application Layer)** Controller tiếp nhận yêu cầu từ giao diện, xác định hành động là "GRANT" hay "REVOKE" để gọi thủ tục tương ứng.

**Đoạn mã xử lý tại Repository:**

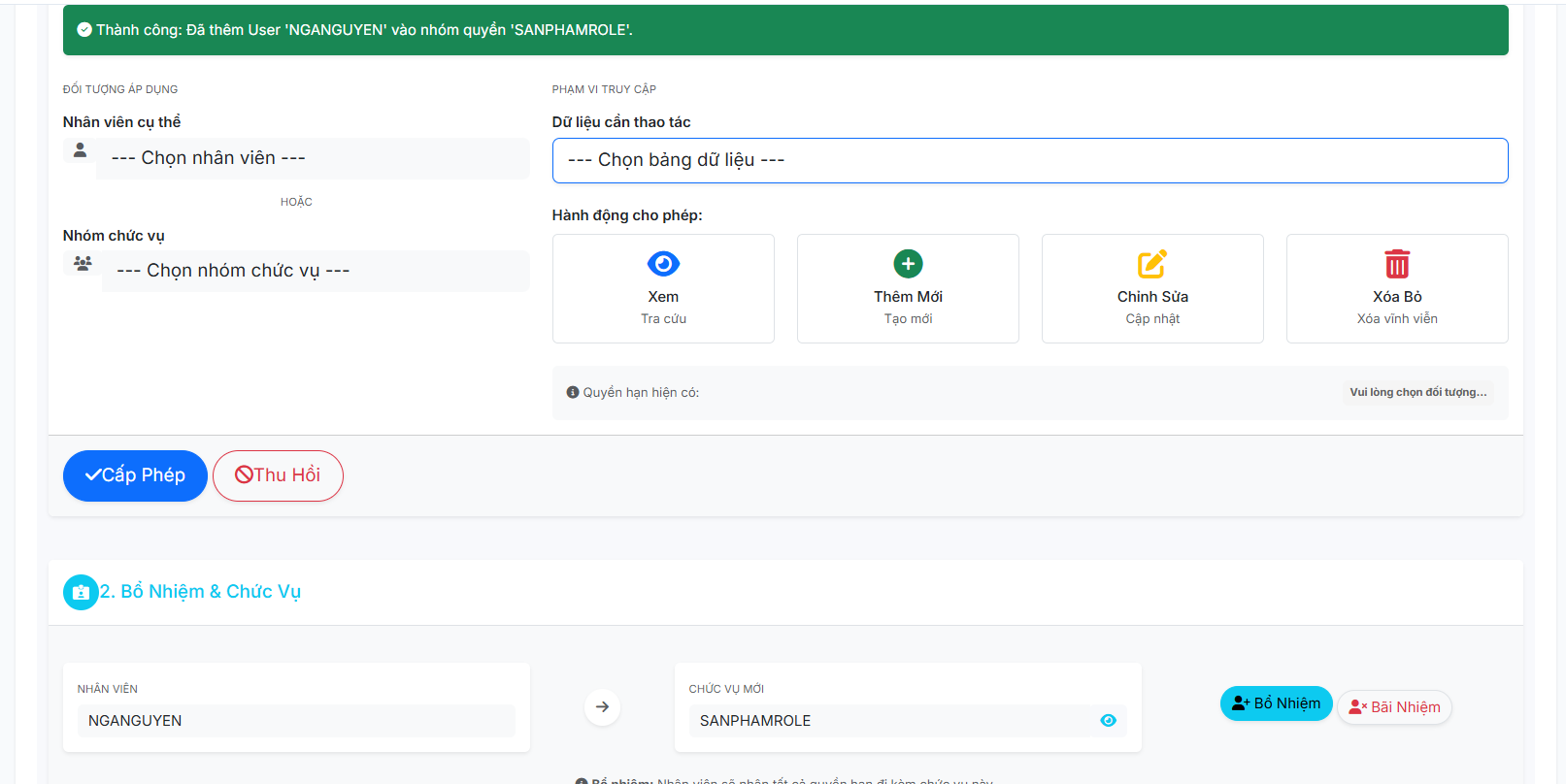


Hình 58 hàm bổ nhiệm

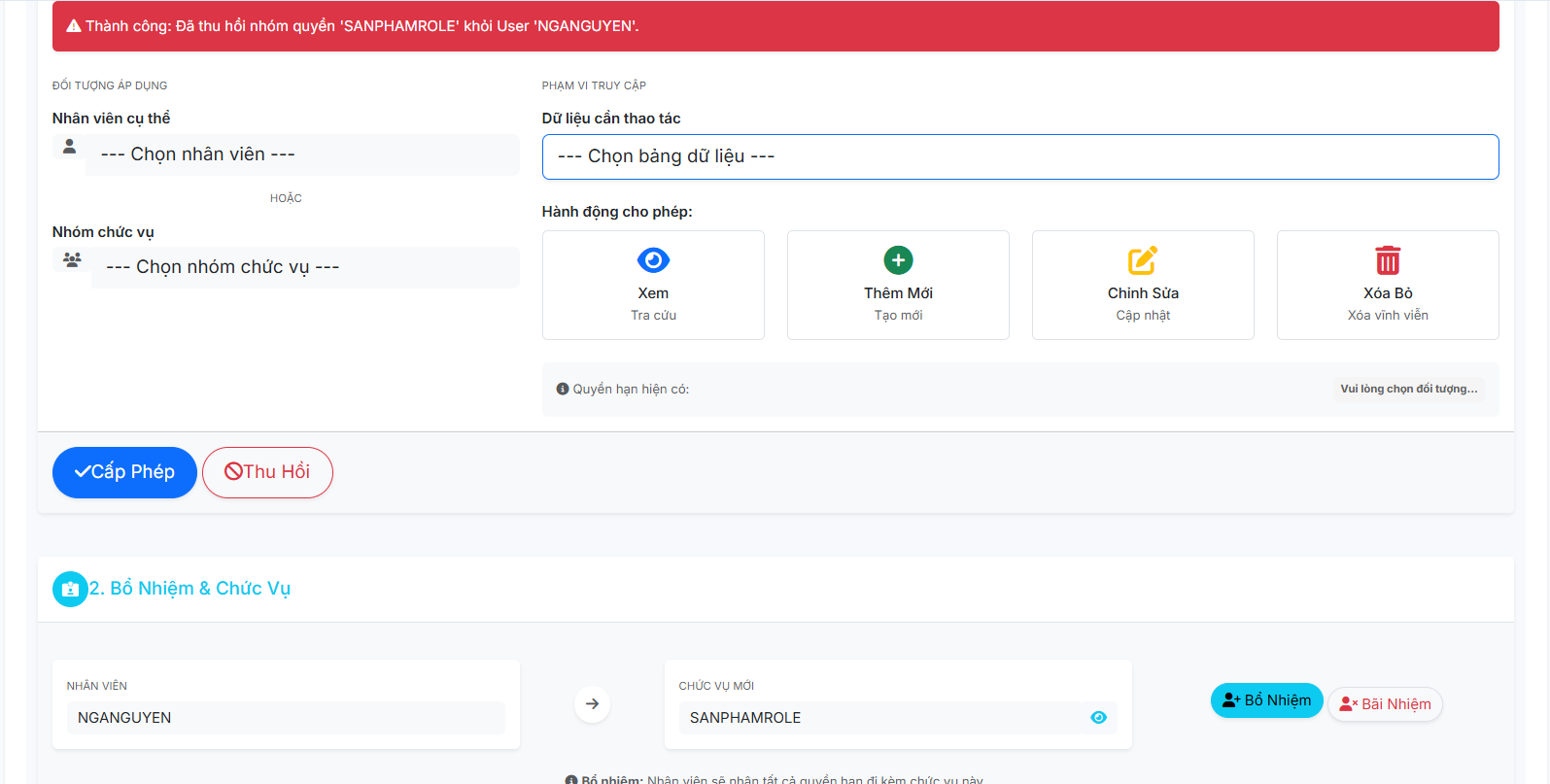


Hình 59 hàm bãi nhiệm

**d. Giao diện thực hiện Bổ nhiệm** Giao diện được thiết kế đơn giản với quy trình 2 bước: Chọn Nhân viên -> Chọn Chức vụ mới -> Bấm nút Bổ nhiệm.



Hình 60 giao diện bổ nhiệm



Hình 61 giao diện bãi nhiệm

## **3.3 Dùng công cụ FGA cài đặt VPD, cài đặt OLS**

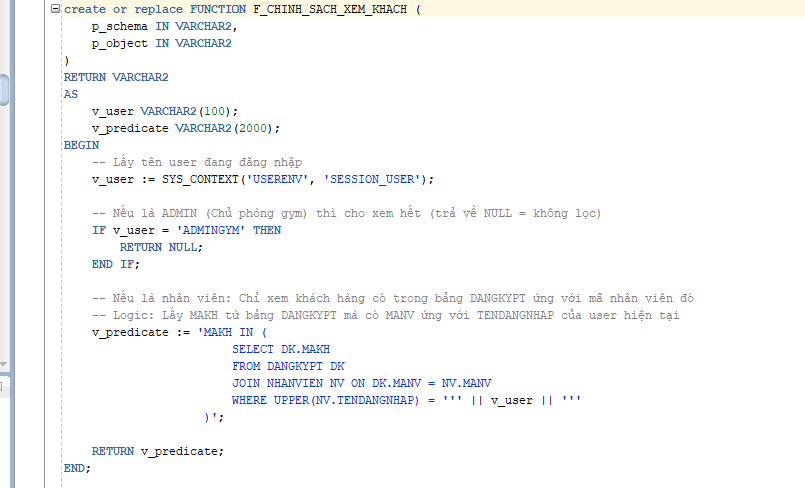
### **3.3.1. Cài đặt VPD**

**a. Mục đích** Trong hệ thống phòng Gym, dữ liệu khách hàng là tài sản quan trọng. Để tránh việc nhân viên (PT) lấy thông tin khách hàng của nhau (tranh giành khách), hệ thống áp dụng VPD để đảm bảo:

**ADMIN:** Xem được toàn bộ danh sách khách hàng.

**NHANVIEN (PT):** Chỉ nhìn thấy thông tin của những khách hàng đã đăng ký tập luyện (DANGKYPT) với chính nhân viên đó.

**b. Xây dựng hàm chính sách (Policy Function):** Hàm này có nhiệm vụ tự động tạo ra câu điều kiện WHERE để lọc dữ liệu dựa trên người dùng đang đăng nhập.



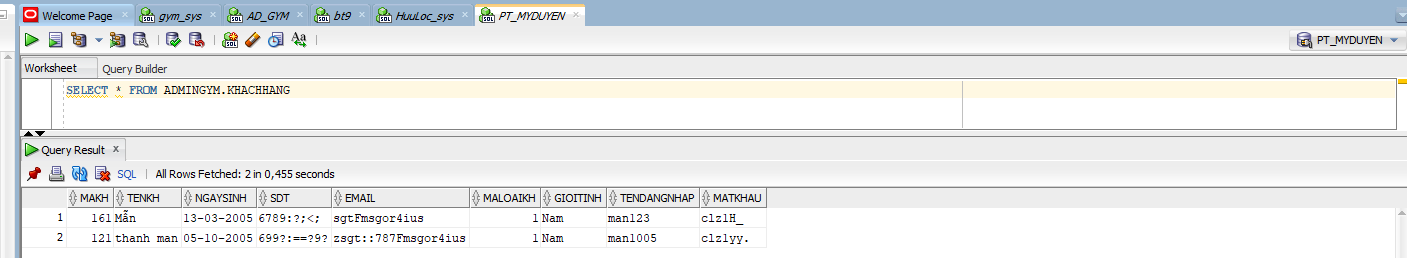
Hình 62 hàm chính sách

**c. Gán chính sách vào bảng (Add Policy):** Sử dụng gói DBMS\_RLS để áp dụng hàm trên vào bảng KHACHHANG cho các câu lệnh SELECT.



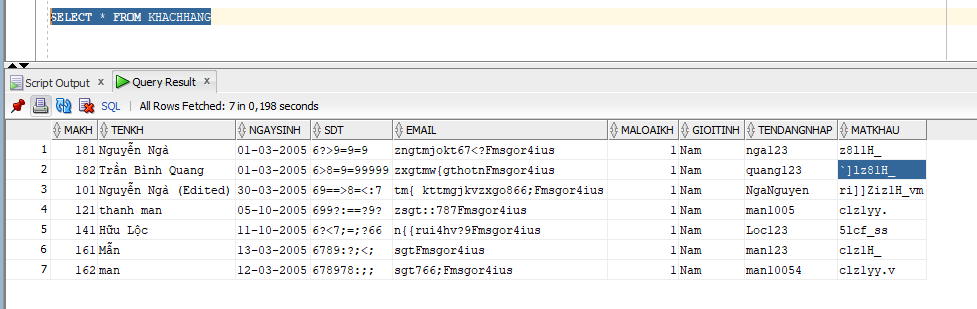
Hình 63 gán chính sách vào bảng

Góc nhìn Staff PT chỉ thấy những khách hàng mà mình dạy:



Hình 64 góc nhìn StaffPt

Góc nhìn Admin thấy tất cả khách hàng:

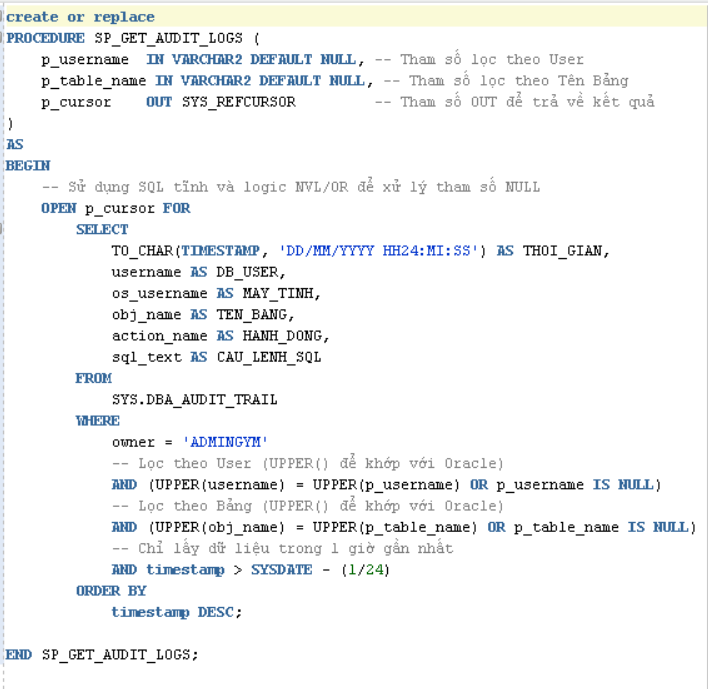


Hình 65 góc nhìn admin

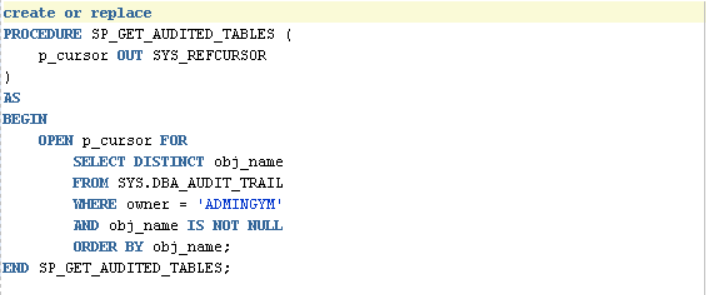
### **3.3.2. Cài đặt FGA**

* Mục tiêu: Xây dựng các thủ tục để quản trị viên có thể theo dõi các hành động nhạy cảm trên hệ thống. Việc sử dụng SYS\_REFCURSOR giúp trả về một tập kết quả linh hoạt để hiển thị lên các bảng dữ liệu (GridView) trên giao diện phần mềm.

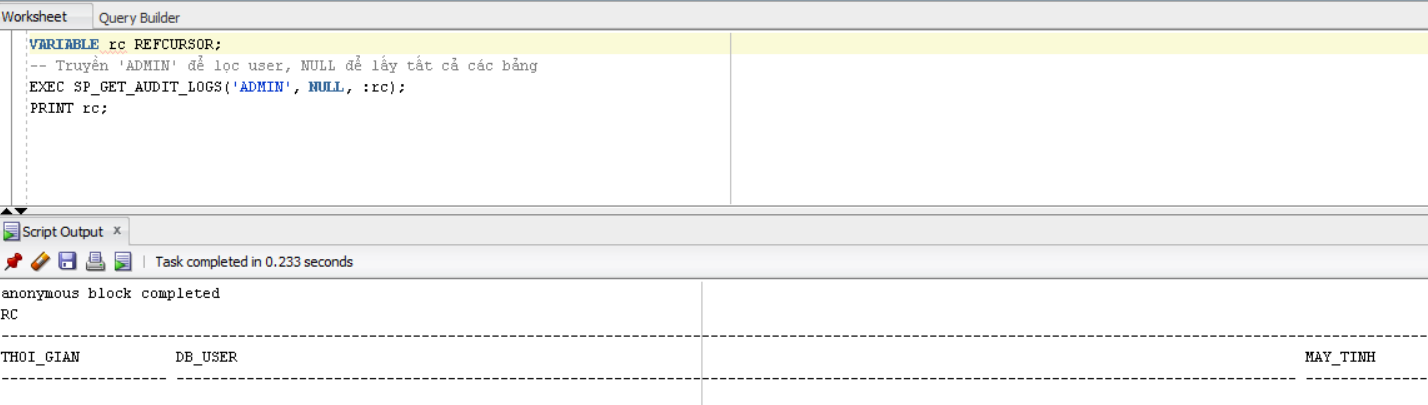
SP\_GET\_AUDIT\_LOGS: Dùng để lấy chi tiết nhật ký (Ai làm? Làm gì? Lúc nào? Câu lệnh gì?).



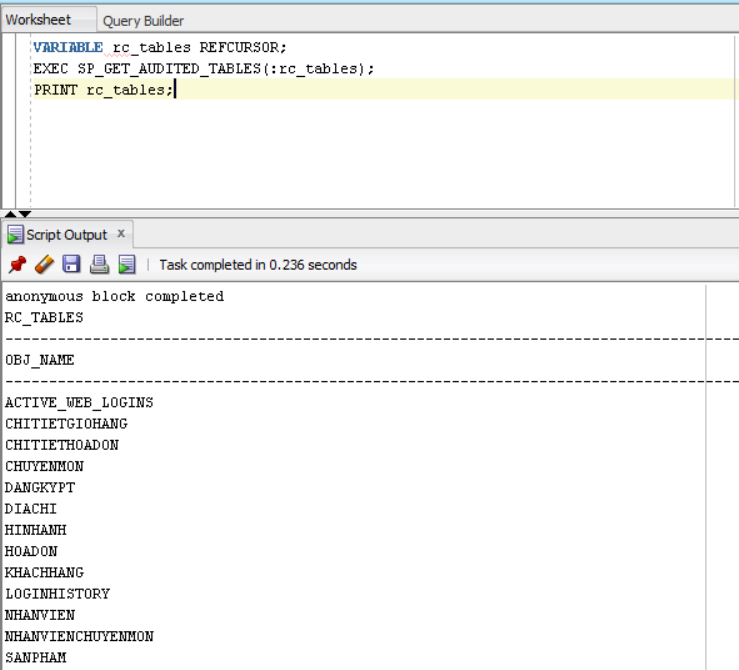
SP\_GET\_AUDITED\_TABLES: Dùng để lọc danh sách các bảng đã có phát sinh nhật ký.



* Tham số đầu vào (p\_username, p\_table\_name): Cho phép lọc linh hoạt. Nếu để trống (NULL), hệ thống sẽ tự động lấy tất cả nhờ logic (UPPER(username) = UPPER(p\_username) OR p\_username IS NULL).
* Tham số đầu ra (p\_cursor): Sử dụng kiểu SYS\_REFCURSOR để trả về một tập dữ liệu (Table) thay vì một giá trị đơn lẻ.
* Giới hạn thời gian: Điều kiện timestamp > SYSDATE - (1/24) giúp tối ưu hiệu năng bằng cách chỉ truy xuất các hành động xảy ra trong 1 giờ gần nhất.
* Nguồn dữ liệu: Truy vấn trực tiếp từ View hệ thống SYS.DBA\_AUDIT\_TRAIL.
* Chạy thử thủ tục lấy nhật ký



* Chạy thử thủ tục lấy danh sách các bảng bị giám sát

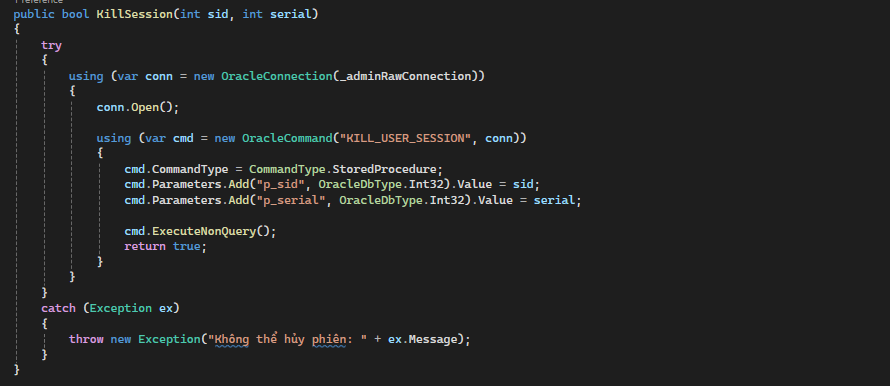


# **CHƯƠNG 4: KIỂM TOÁN**

## **4.1 Cài đặt ứng dụng có tính năng giám sát người dùng**

### **4.1.1 Cơ chế hoạt động (Technical Mechanism):**

* Định danh phiên: Hệ thống không chỉ quản lý phiên ở tầng Web (Cookies), mà quản lý trực tiếp phiên kết nối vào Database. Mỗi kết nối được định danh bởi cặp khóa chính: SID (Session ID) và SERIAL# (Số sê-ri để phân biệt các phiên dùng lại cùng một SID).
* Ngắt kết nối (Kill Session):
* Khi Admin bấm nút "Hủy phiên", AdminController gọi hàm UserService.KillSession(sid, serial).
* Hàm này gọi Stored Procedure KILL\_USER\_SESSION.
* Giải thích chuyên sâu (để viết vào báo cáo): "Bên dưới Database, thủ tục này sẽ thực thi lệnh hệ thống ALTER SYSTEM KILL SESSION 'sid, serial' để ngắt ngay lập tức kết nối của người dùng, buộc họ phải đăng xuất."

****

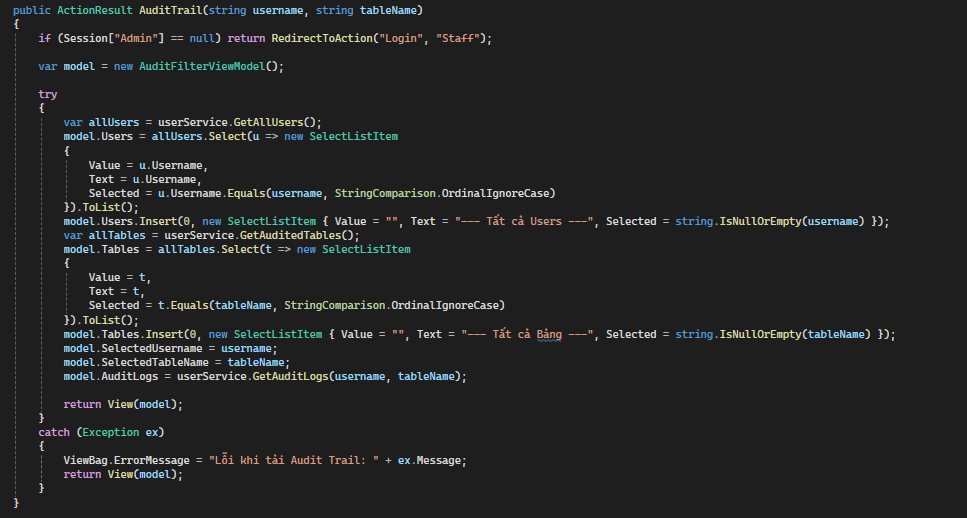
Hình 66 kill session

* Thu thập dữ liệu: Hệ thống sử dụng cơ chế Standard Auditing hoặc Unified Auditing của Oracle để tự động ghi lại các hành động nhạy cảm.
* Truy xuất nhật ký:
* Hàm UserService.GetAuditLogs gọi Stored Procedure ADMINGYM.SP\_GET\_AUDIT\_LOGS.
* Dữ liệu trả về bao gồm các thông tin tối quan trọng cho việc điều tra (Forensic):
* DB\_USER: Tài khoản Database thực hiện.
* TEN\_BANG: Đối tượng bị tác động.
* HANH\_DONG: Loại thao tác (INSERT, UPDATE, DELETE).
* CAU\_LENH\_SQL: (Điểm ăn tiền) Chi tiết câu lệnh SQL mà người dùng đã chạy.

****

Hình 67 get auditlog

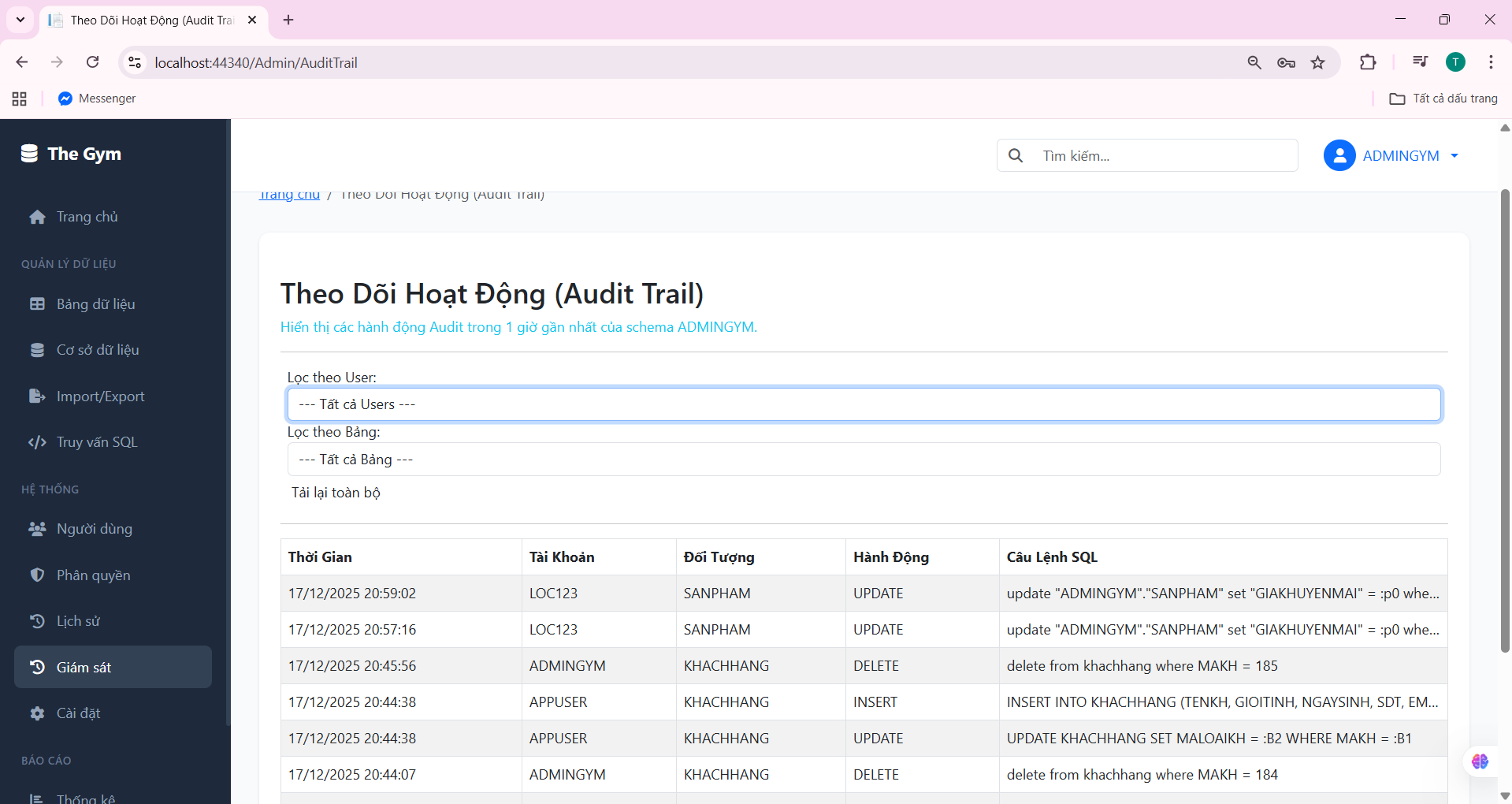
* Áp dụng vào AdminController



Hình 68 audittrail

### **4.1.2 Giao diện**

* Sau khi đăng nhập bằng tài khoản ADMINGYM có thể giám sát được các hoạt động về thời gian, tài khoản, đối tượng bảng, hành động, câu lệnh SQL



Hình 69 giao diện giám sát

# **KẾT LUẬN**

**1. Kết quả đạt được**

Đồ án đã xây dựng thành công "Hệ thống Quản lý Phòng Gym" hoàn chỉnh trên nền tảng Oracle Database.

Về nghiệp vụ: Đáp ứng đầy đủ quy trình quản lý khép kín: Quản lý hội viên, Đăng ký gói tập, Kiểm soát ra vào (Check-in), Bán hàng (POS) và Quản lý lịch tập PT.

Về kỹ thuật: Hệ thống vận hành ổn định, cơ sở dữ liệu được thiết kế chặt chẽ và tối ưu hóa hiệu năng thông qua các Stored Procedures.

**2. Ưu điểm**

Đồ án vượt trội so với các ứng dụng quản lý thông thường nhờ tích hợp các giải pháp bảo mật và quản trị nâng cao:

Bảo mật đa lớp: Triển khai thành công trọn bộ các giải thuật mã hóa:

Mã hóa đối xứng (DES): Bảo vệ mã xác thực (OTP) trong Database.

Mã hóa bất đối xứng (RSA): Ký số (Digital Signature) đảm bảo tính toàn vẹn cho hóa đơn điện tử.

Quản trị hệ thống: Xây dựng thành công chức năng Giám sát phiên (Kill Session) và Kiểm toán (Audit Trail) để theo dõi và xử lý các kết nối bất thường.

Cơ chế xác thực: Ứng dụng kỹ thuật Database Authentication, sử dụng chính tài khoản Oracle của người dùng để định danh chính xác.

# **DANH MỤC TÀI LIỆU THAM KHẢO**