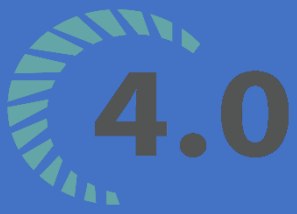
BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN

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

ĐẠI HỌC QUỐC GIA TP HCM

BÁO CÁO ĐỒ ÁN MÔN HỌC



Sinh viên thực hiện:

19120481	Đàm Hồng Đức
19120583	Lê Thái Bình Minh
19120416	Nguyễn Anh Tuấn
19120529	Nguyễn Phước Huy

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 2021 - 2022

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
227 Nguyễn Văn Cừ, Phường 4, Quận 5, TP.HCM
Điện Thoại: (08) 38.354.266 - Fax:(08) 38.350.096

BẢNG THÔNG TIN CHI TIẾT NHÓM

Mã nhóm:	ATBMCQ-05			
Số lượng:	**4**			
MSSV	**Họ tên**	**Email**	**Điện thoại**	**Nhóm trưởng**
19120481	Đàm Hồng Đức	19120481@student.hcmus.edu.vn	0355211735	
19120583	Lê Thái Bình Minh	19120583@student.hcmus.edu.vn	0852576282	x
19120416	Nguyễn Anh Tuấn	19120416@student.hcmus.edu.vn	0348379575	
19120529	Nguyễn Phước Huy	19120529@student.hcmus.edu.vn	0917966026	

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**
• Tạo form chức năng **Cấp quyền, thu hồi quyền từ người dùng/ role, Gán Role cho User/Role.** • Quay video demo.	19120416 - Nguyễn Anh Tuấn	100%	10/10
• Tạo form chức năng **Login, Main, Thu hồi Role của User/Role, Gán Role cho User/Role, Kết nối Oracle Database to C#.** • Phân công công việc. • Quay video demo.	19120481 - Đàm Hồng Đức	100%	10/10
• Tạo form chức năng **Xem danh sách người dùng trong hệ thống, Kiểm tra quyền của User/Role trên các đối tượng dữ liệu.** • Quay video demo.	19120529 - Nguyễn Phước Huy	100%	10/10
• Tạo form chức năng **Tạo mới, xóa, hiệu chỉnh user; Tạo, xoá role.** • Làm báo cáo. • Quay video demo.	19120583- Lê Thái Bình Minh	100%	10/10
		Toàn phân hệ:	**100%**

PHÂN HỆ 2			
Công việc thực hiện	**Người thực hiện**	**Mức độ hoàn thành**	**Đánh giá của nhóm**
• Thực hiện TC#7 với Mã hoá dữ liệu. • Demo OLS trên Oracle, SQL Developer. • Làm báo cáo chính sách OLS và chính sách Encrypt. • Quay video demo.	19120416 - Nguyễn Anh Tuấn	100%	10/10
• Thực hiện TC#1, TC#2 và Audit. • Phân công công việc. • Làm giao diện TC#1, TC#2 và Audit. • Làm báo cáo chính sách RBAC và Audit. • Quay video demo.	19120481 - Đàm Hồng Đức	100%	10/10
• Thực hiện TC#3, TC#4, TC#6. • Làm giao diện TC#3, TC#4, TC#6. • Làm báo cáo chính sách RBAC, VPD. • Quay video demo.	19120529 - Nguyễn Phước Huy	100%	10/10
• Viết script khởi tạo database và insert dữ liệu mẫu. • Tổng hợp các file script chính sách. • Vẽ lược đồ CSDL và đặc tả. • Thực hiện TC#5. • Làm giao diện TC#5. • Làm báo cáo chính sách RBAC. • Tổng hợp và hoàn thiện báo cáo. • Quay video demo.	19120583- Lê Thái Bình Minh	100%	10/10
		Toàn phân hệ:	**100%**

Mục Lục

YÊU CẦU ĐỒ ÁN

Loại bài tập	**☐ Lý thuyết ☑ Thực hành ☑ Đồ án ☐ Bài tập**
Ngày bắt đầu	**30/03/2022**
Ngày kết thúc	**28/06/2022**

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.

PHÂN HỆ 2: Sở y tế tỉnh/ thành phố X cần gom dữ liệu về kho dữ liệu D (cấp sở), gồm hồ sơ bệnh án (và một số dữ liệu liên quan) từ các cơ sở y tế trong tỉnh/ thành phố và quản lý chuyên môn về việc khám chữa bệnh của các cơ sở y tế thông qua một hệ thống thông tin quản lý S.

HSBA (<u>MÃHSBA</u>, MÃBN, NGÀY, CHẨNĐOÁN, MÃBS, MÃKHOA, MÃCSYT,

KẾTLUẬN): mỗi hồ sơ bệnh án (HSBA) có một mã duy nhất (MÃHSBA), liên quan đến một bệnh nhân (MÃBN), được lập vào một ngày (NGÀY), có chẩn đoán (CHẨNĐOÁN) của bác sĩ điều trị (MÃBS), được tiếp nhận khám và điều trị tại khoa (MÃKHOA), của cơ sở y tế (có mã là MÃCSYT), với kết luận của bác sĩ (KẾTLUẬN).

HSBA_DV (MÃHSBA, MÃDV, NGÀY, MÃKTV, KẾTQUẢ): ghi nhận lại các dịch vụ (thông qua MÃDV) đã sử dụng theo chỉ định của bác sĩ điều trị (ví dụ các loại xét nghiệm, chụp hình, ...), người thực hiện dịch vụ (MÃKTV) và kết quả (KẾTQUẢ).

BỆNHNHÂN (MÃBN, MÃCSYT, TÊNBN, CMND, NGÀYSINH, SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN, TỈNHTP, TIỀNSỬBỆNH, TIỀNSỬBỆNHGĐ, DỊỨNGTHUỐC): mỗi bệnh nhân được cơ sở y tế có mã là MÃCSYT cấp mã duy nhất (MÃBN), có tên (TÊNBN), ngày sinh (NGÀYSINH), địa chỉ (SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN), và tiền sử bệnh của bệnh nhân (TIỀNSỬBỆNH) và gia đình (TIỀNSỬBỆNHGĐ), cũng như tình trạng dị ứng thuốc (nếu có, DỊỨNGTHUỐC).

CSYT (MÃCSYT, TÊNCSYT, ĐCCSYT, SĐTCSYT): ghi nhận thông tin về các cơ sở y tế thuộc tỉnh/ thành phố gồm mã, tên, địa chỉ, số điện thoại.

NHÂNVIÊN (MÃNV, HỌTÊN, PHÁI, NGÀYSINH, CMND, QUÊQUÁN, SỐĐT, CSYT, VAITRÒ, CHUYÊNKHOA): Quan hệ NHÂNVIÊN chứa dữ liệu về các nhân viên trực thuộc cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S. Mỗi nhân viên có mã (MÃNV) do đơn vị quản lý trực tiếp cấp, giả sử các mã này không trùng nhau trong phạm vi toàn tỉnh/ thành phố. Ngoài ra cũng cần ghi lại thông tin họ tên (HỌTÊN), phái (PHÁI), ngày sinh (NGÀYSINH), số chứng minh nhân dân (CMND), quê quán, số điện thoại, thuộc cơ sở y tế nào (CSYT). Thuộc tính VAITRÒ nhận một trong các giá trị sau: “Thanh tra”, “Cơ sở y tế”, “Y sĩ/ bác sĩ”, “Nghiên cứu”. Với các nhân viên có vai trò “Y sĩ/ bác sĩ” hoặc “Nghiên cứu” thì cần lưu thêm thông tin về chuyên khoa (CHUYÊNKHOA) mà người đó được cấp bằng cấp chuyên môn. Cơ sở dữ liệu được cài

đặt trên Oracle. Hệ thống dùng chính sách đóng (người dùng u cần được cấp quyền p trên đối tượng dữ liệu o mới có thể thực hiện p trên o). DBA trong hệ thống S thực hiện việc cấp quyền cho nhân sự trong toàn hệ thống theo mô tả như sau:

TC#1: Ngoài DBA, tất cả người dùng trong hệ thống S gồm những nhân viên trong quan hệ NHÂNVIÊN và cả những bệnh nhân trong quan hệ BỆNHNHÂN. DBA tạo tài khoản cho tất cả những người dùng này. DBA không tự định nghĩa bảng (table) dùng để quản lý tài khoản người dùng mà sử dụng thông tin tài khoản do Hệ quản trị CSDL Oracle quản lý. Bằng cách nào DBA có thể kết nối một tên tài khoản với 1 dòng dữ liệu là người dùng tương ứng (trong quan hệ NHÂNVIÊN và BỆNHNHÂN) mà không phải truy cập dữ liệu từ nhiều hơn 1 bảng, đồng thời phải ép thỏa các chính sách bảo mật liên quan đến những người dùng này. DBA phụ trách thêm, cập nhật dữ liệu trong bảng CSYT và thêm dữ liệu trong NHÂNVIÊN, gồm những nhân viên thuộc các cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S.

TC#2: Có 5 nhân viên thuộc sở y tế với vai trò "Thanh tra". Các nhân viên giữ vai trò thanh tra có thể đọc dữ liệu trên tất cả các quan hệ được mô tả để kết xuất báo cáo định kỳ, mà không có quyền thêm, xóa, sửa trên bất cứ quan hệ nào.

TC#3: Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên kho dữ liệu D. Có 50 nhân viên thuộc 50 cơ sở y tế trong tỉnh/ thành phố được cử để sử dụng tài khoản được cấp. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa dữ liệu phát sinh từ chính cơ sở y tế mà nhân viên này trực thuộc, trong tháng hiện tại từ ngày 5 đến 27 dương lịch hàng tháng, liên quan các nghiệp vụ:

a. Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)

b. Thêm, xóa dòng dịch vụ (HSBA_DV) liên quan 1 hồ sơ bệnh án.

TC#4: Có 500 nhân viên giữ vai trò "Y sĩ/ bác sĩ" trực tiếp khám chữa bệnh cho bệnh nhân ở các cơ sở y tế thuộc tỉnh/ thành phố. Y sĩ/ Bác sĩ có quyền xem hồ sơ bệnh án (HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA_DV) và thông tin bệnh nhân (BỆNHNHÂN) khi nhập thông tin mã bệnh nhân hoặc số CMND.

TC#5: Có 50 nhân viên ở vai trò "Nghiên cứu" ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án (bảng HSBA và HSBA_DV) được điều trị tại cùng cơ sơ y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.

TC#6: Hệ thống hiện tại có khoảng 10000 bệnh nhân. Trên hệ thống S, trừ những người giữ vai trò thanh tra (và DBA), mỗi nhân viên hoặc bệnh nhân đăng nhập chỉ có thể xem thông tin của chính mình, (trên bảng NHÂN VIÊN nếu là nhân viên, trên bảng BỆNH NHÂN nếu là bệnh nhân), và có thể chỉnh sửa các trường (trừ trường mã) liên quan đến chính người đó.

TC#7: Dựa vào chuyên môn, kỹ thuật của đơn vị mà Sở y tế tỉnh/ thành phố X chia các cơ sở y tế trực thuộc thành 3 tuyến:

+ "Điều trị ngoại trú": các cơ sở khám chữa bệnh ban đầu, điều trị ngoại trú.

+ "Điều trị nội trú": các bệnh viện với các kỹ thuật chuyên khoa cơ bản và nâng cao.

+ "Điều trị chuyên sâu": các bệnh viện đa khoa và chuyên khoa thực hiện được các kỹ thuật chuyên sâu.

Ngoài ra, tùy vào vị trí địa lý của cơ sở y tế mà Sở y tế tỉnh/ thành phố X chia ra làm 3 vùng: trung tâm, cận trung tâm, ngoại thành. Có sự phân chia vai trò người dùng theo 03 cấp bậc: Giám đốc sở, Giám đốc cơ sở y tế và Y/ Bác sĩ. Sở cần gửi những dòng trong quan hệ THÔNGBÁO, gồm các trường NỘIDUNG, NGÀYGIỜ và ĐỊAĐIỂM về những cuộc họp khẩn đến các vai trò liên quan ở các cơ sở y tế. Dùng OLS (Oracle Label Security). Hãy thiết lập hệ thống nhãn và thiết lập 5 loại người dùng khác nhau. Cho minh họa cách phát tán dữ liệu.

Yêu cầu:

1. Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các chính sách bảo mật đặt ra ở các TC#i, 1 <= i <= 6

Ở tiêu chí TC#7, sinh viên hãy đề ra bối cảnh sử dụng cơ chế OLS của Oracle. Nhãn

gồm đầy đủ 3 thành phần: level, compartment và group. Hãy gán nhãn cho dữ liệu, người dùng và minh họa cho các kịch bản đã nêu, và các kịch bản khác (nếu có thể).

2. Sinh viên hãy đề xuất bối cảnh vận dụng cơ chế mã hóa trong ứng dụng trên, và dùng thư viện hỗ trợ mã dữ liệu của Oracle. Cho biết mục đích, đối tượng dữ liệu cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản lý khóa.

3. Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (audit, chỉ yêu cầu thực hiện mức HQT CSDL Oracle):

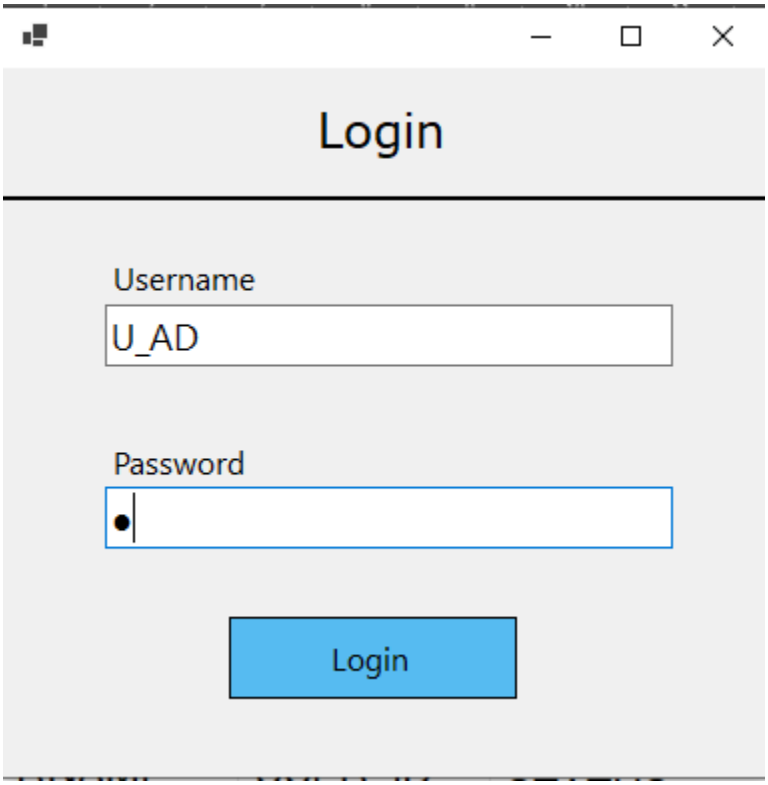
- Kích hoạt việc ghi nhật ký toàn hệ thống.
- Thực hiện ghi nhật ký hệ thống dùng standard audit: theo dõi hành vi của những user nào trên những đối tượng cụ thể, trên các đối tượng khác nhau (table, view, stored procedure, function), hay chỉ định theo dõi các hành vi hiện thành công hay không thành công.
- Thực hiện Fine-grained Audit một số tình huống và cho kịch bản minh họa.
- Kiểm tra dữ liệu nhật ký hệ thống.

4. Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế trong ngữ cảnh ứng dụng trên thì sẽ được xem xét cộng điểm.

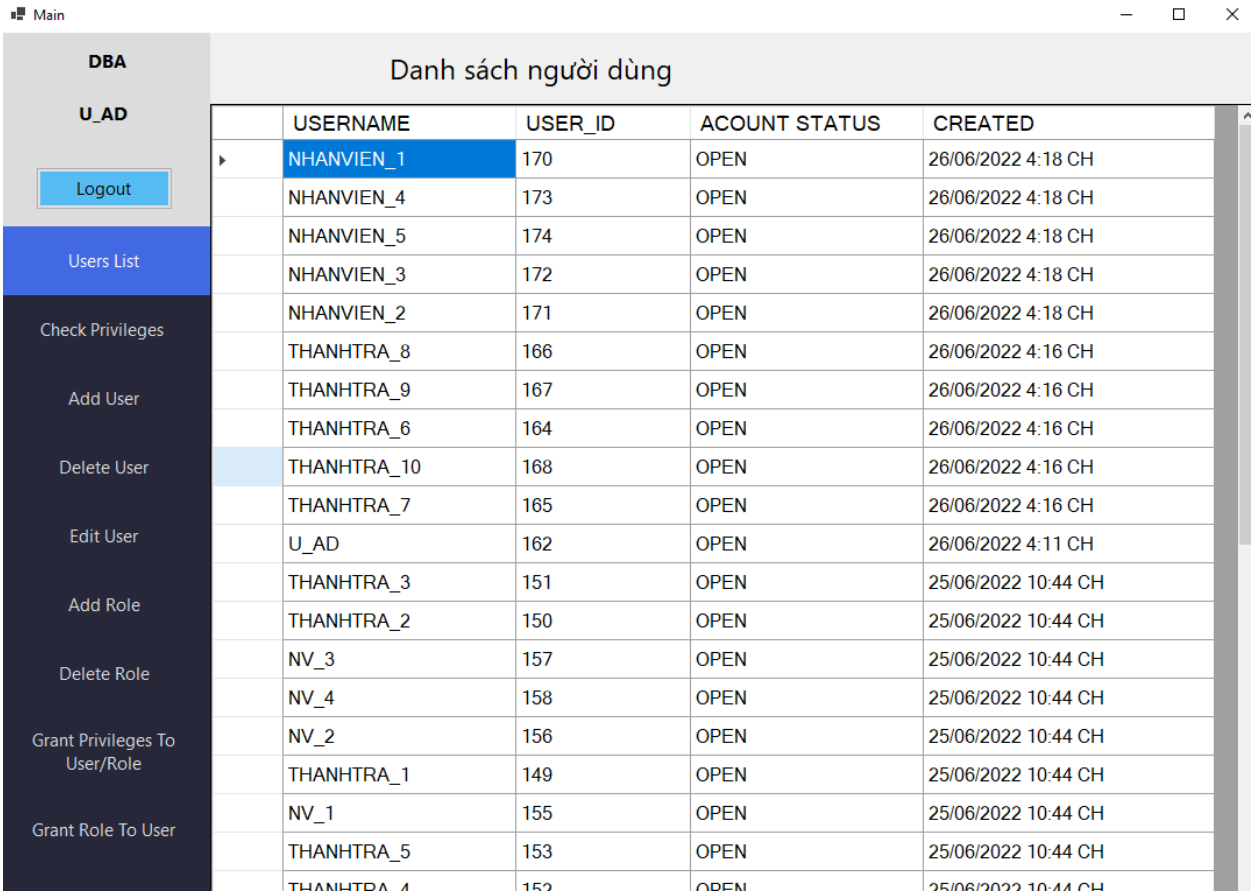
Kết quả thực hiện

Phân hệ 1:

1/ Giao diện đăng nhập:



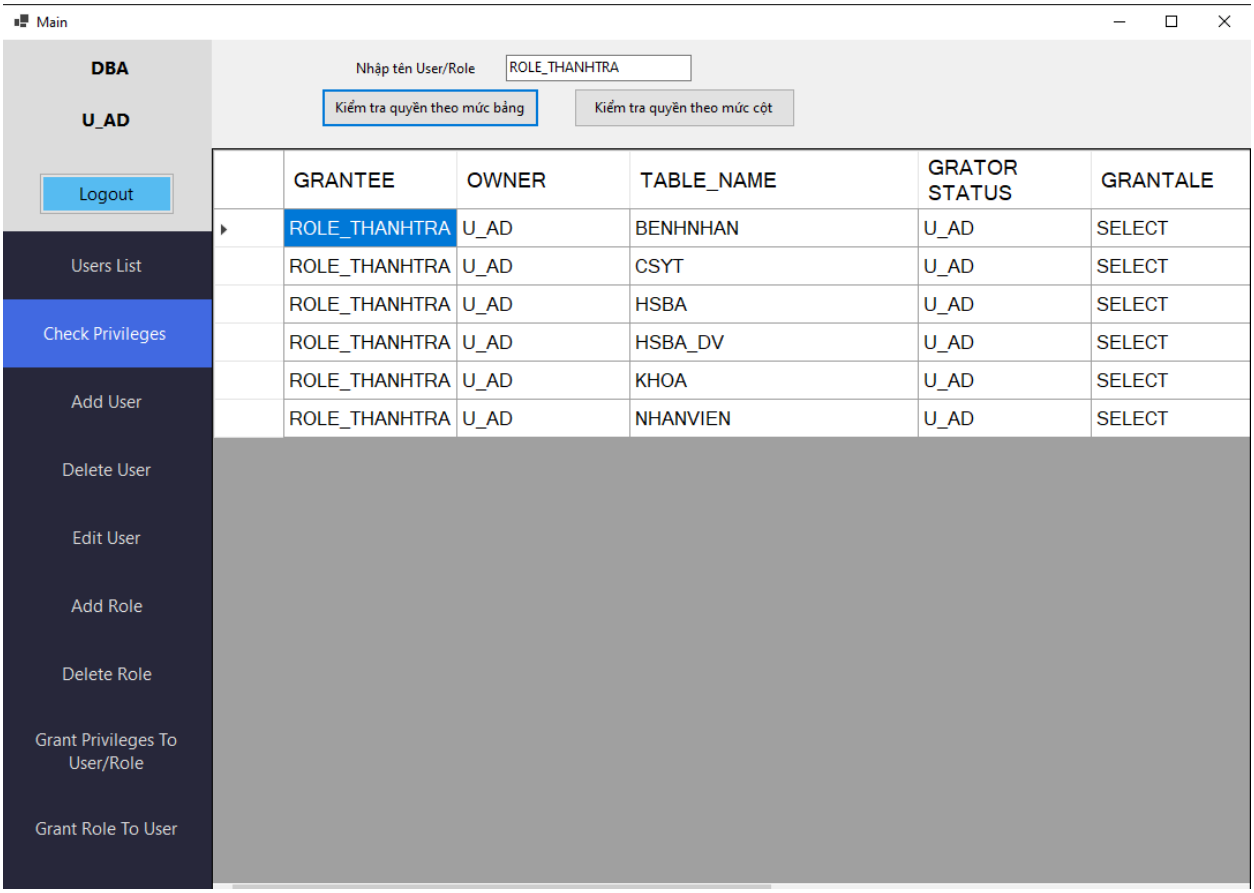
2/ Xem danh sách User trong hệ thống:



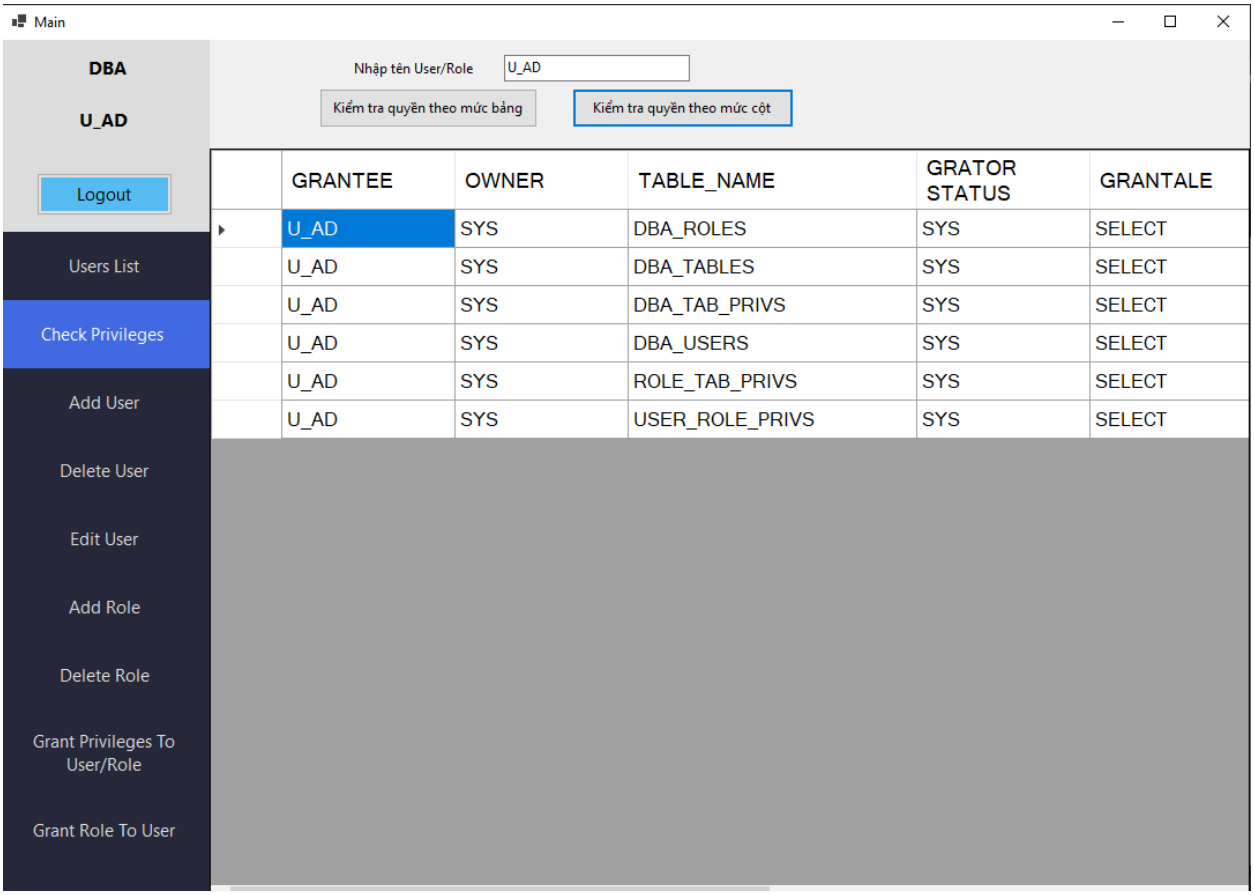
USERNAME	USER_ID	ACOUNT STATUS	CREATED
NHANVIEN_1	170	OPEN	26/06/2022 4:18 CH
NHANVIEN_4	173	OPEN	26/06/2022 4:18 CH
NHANVIEN_5	174	OPEN	26/06/2022 4:18 CH
NHANVIEN_3	172	OPEN	26/06/2022 4:18 CH
NHANVIEN_2	171	OPEN	26/06/2022 4:18 CH
THANHTRA_8	166	OPEN	26/06/2022 4:16 CH
THANHTRA_9	167	OPEN	26/06/2022 4:16 CH
THANHTRA_6	164	OPEN	26/06/2022 4:16 CH
THANHTRA_10	168	OPEN	26/06/2022 4:16 CH
THANHTRA_7	165	OPEN	26/06/2022 4:16 CH
U_AD	162	OPEN	26/06/2022 4:11 CH
THANHTRA_3	151	OPEN	25/06/2022 10:44 CH
THANHTRA_2	150	OPEN	25/06/2022 10:44 CH
NV_3	157	OPEN	25/06/2022 10:44 CH
NV_4	158	OPEN	25/06/2022 10:44 CH
NV_2	156	OPEN	25/06/2022 10:44 CH
THANHTRA_1	149	OPEN	25/06/2022 10:44 CH
NV_1	155	OPEN	25/06/2022 10:44 CH
THANHTRA_5	153	OPEN	25/06/2022 10:44 CH

3/ Kiểm tra quyền của User/Role:

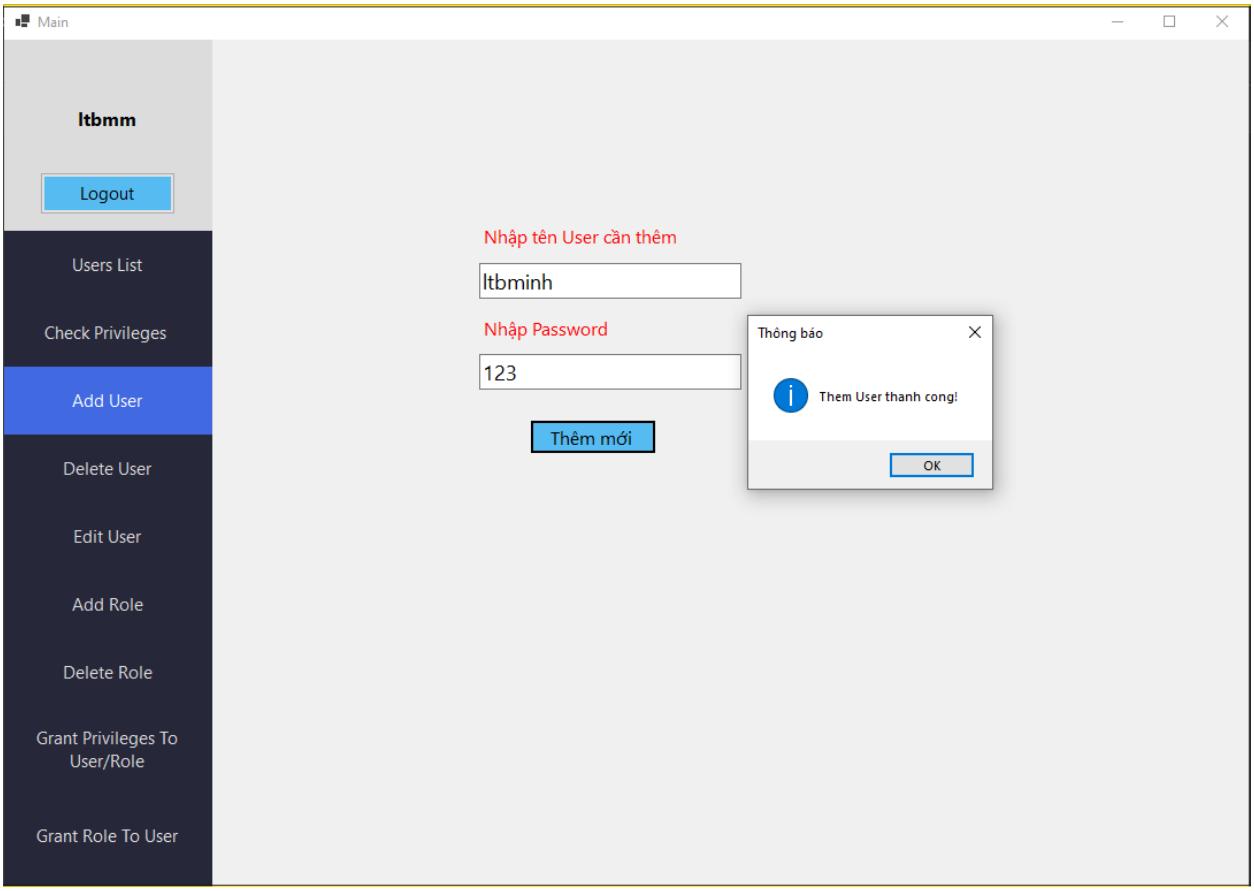
- Theo mức bảng:



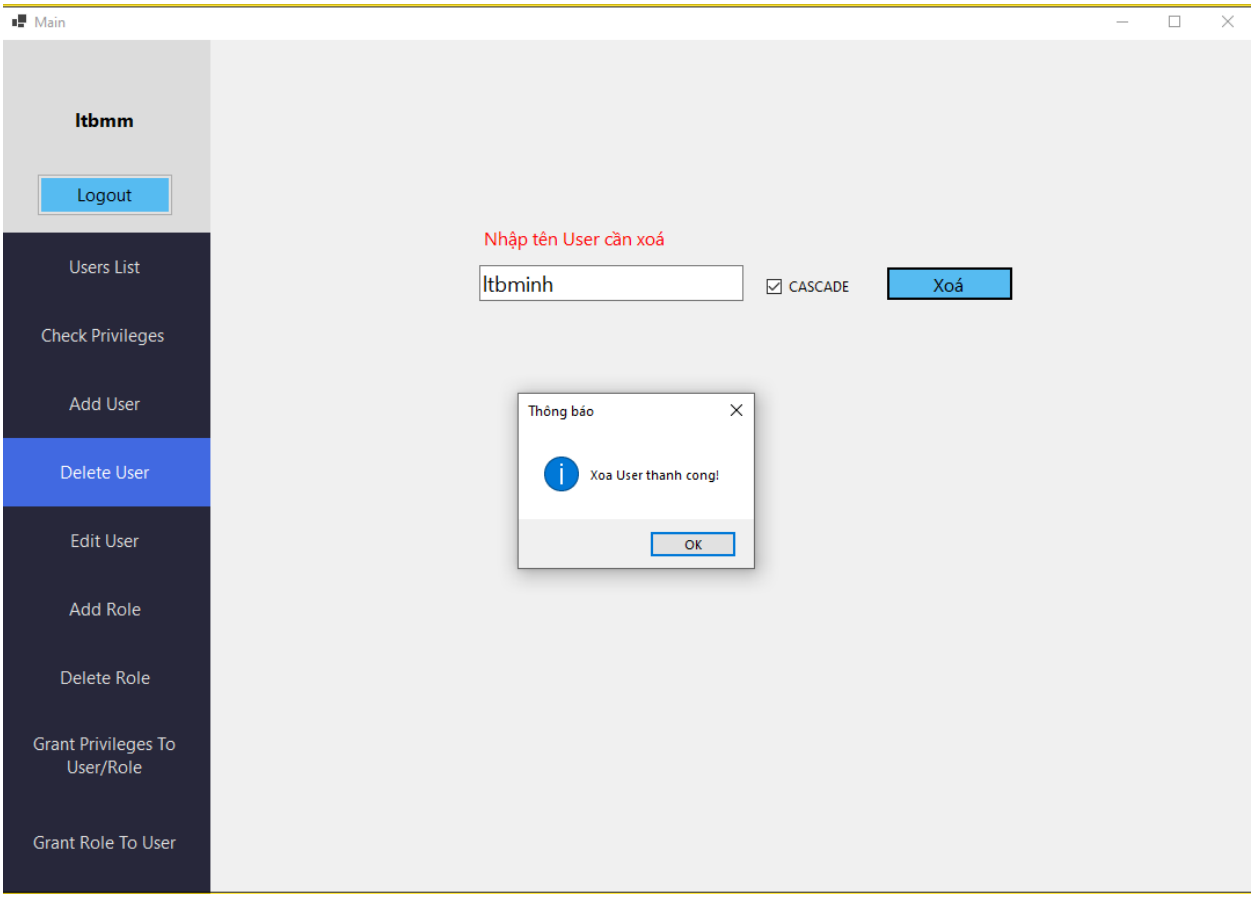
- Theo mức cột:


Main
DBA
U_AD
Logout
Users List
Check Privileges
Add User
Delete User
Edit User
Add Role
Delete Role
Grant Privileges To User/Role
Grant Role To User
Nhập tên User/Role
U_AD
Kiểm tra quyền theo mức bảng
Kiểm tra quyền theo mức cột
GRANTEE
OWNER
TABLE_NAME
GRATOR STATUS
GRANTALE
U_AD SYS DBA_ROLES SYS SELECT
U_AD SYS DBA_TABLES SYS SELECT
U_AD SYS DBA_TAB_PRIVS SYS SELECT
U_AD SYS DBA_USERS SYS SELECT
U_AD SYS ROLE_TAB_PRIVS SYS SELECT
U_AD SYS USER_ROLE_PRIVS SYS SELECT

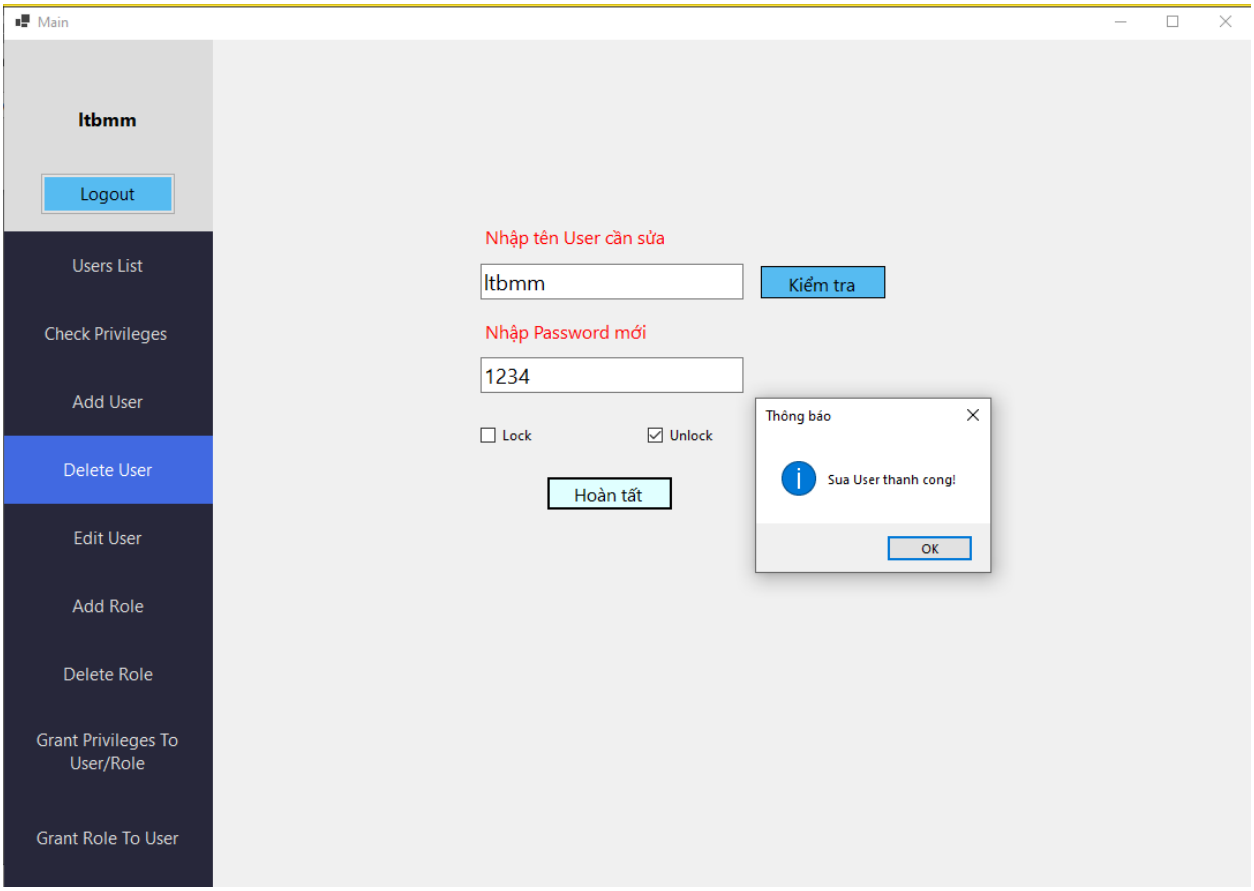
4/ Tạo User mới:



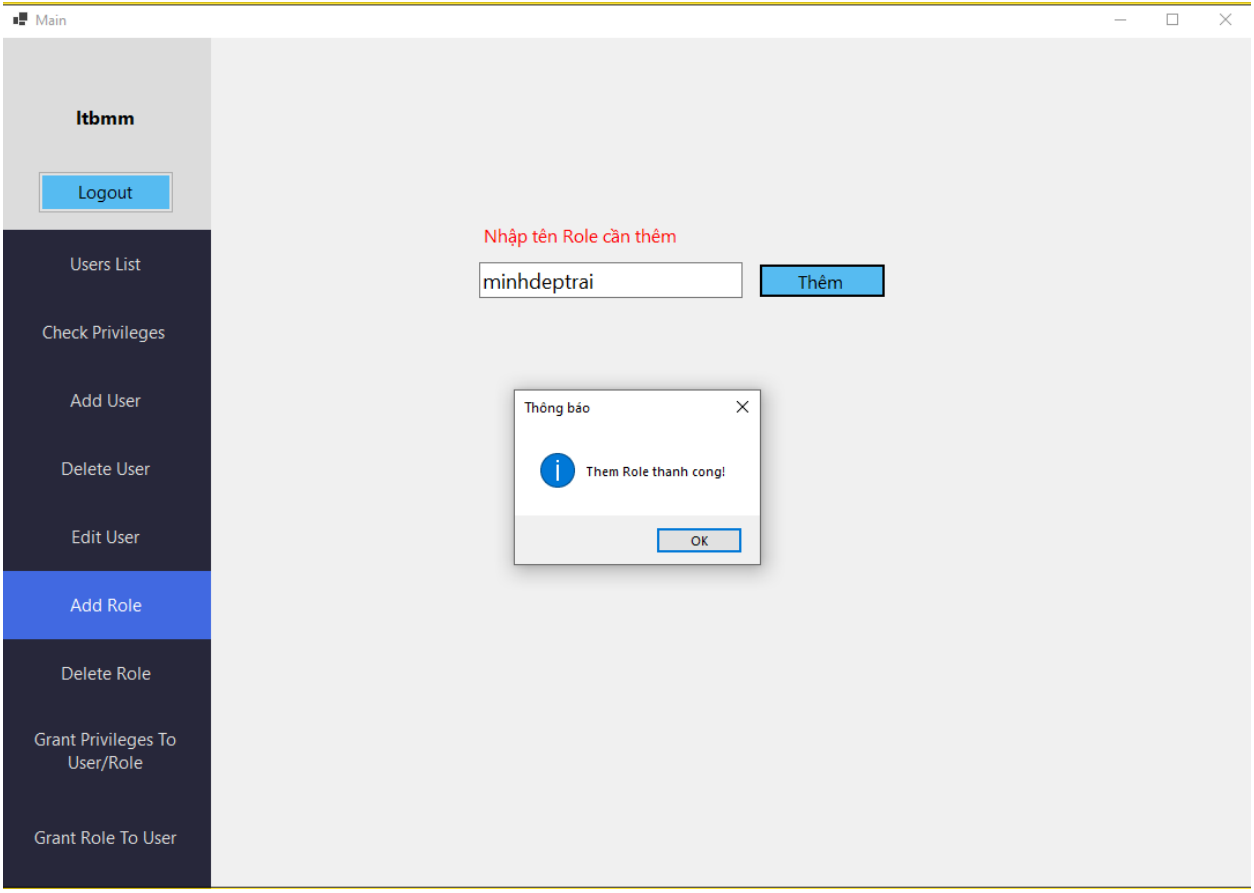
5/ Xoá User:


Main
ltbmm
Logout
Users List
Check Privileges
Add User
Delete User
Edit User
Add Role
Delete Role
Grant Privileges To User/Role
Grant Role To User
Nhập tên User cần xoá
ltbminh
CASCADE
Xoá
Thông báo
Xoa User thanh cong!
OK

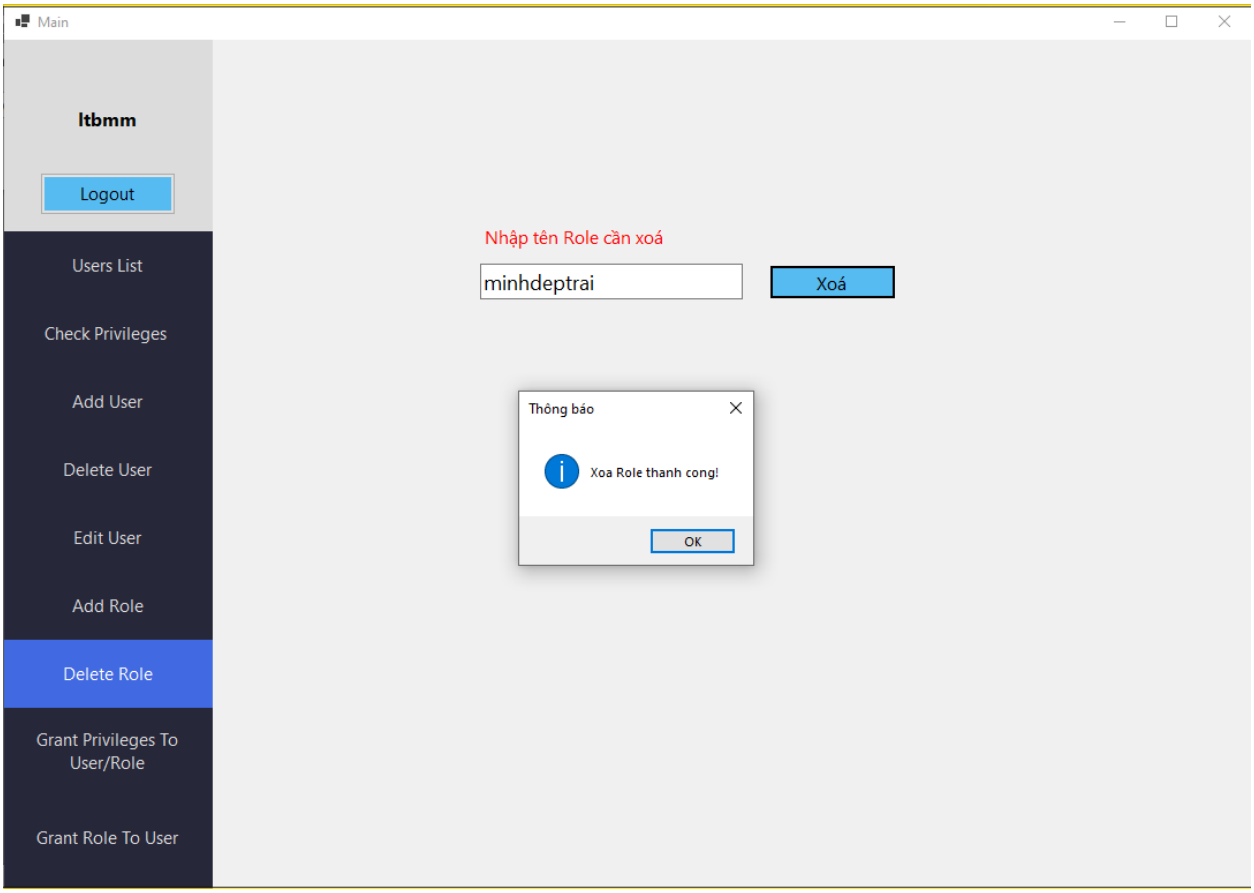
6/ Hiệu chỉnh User:



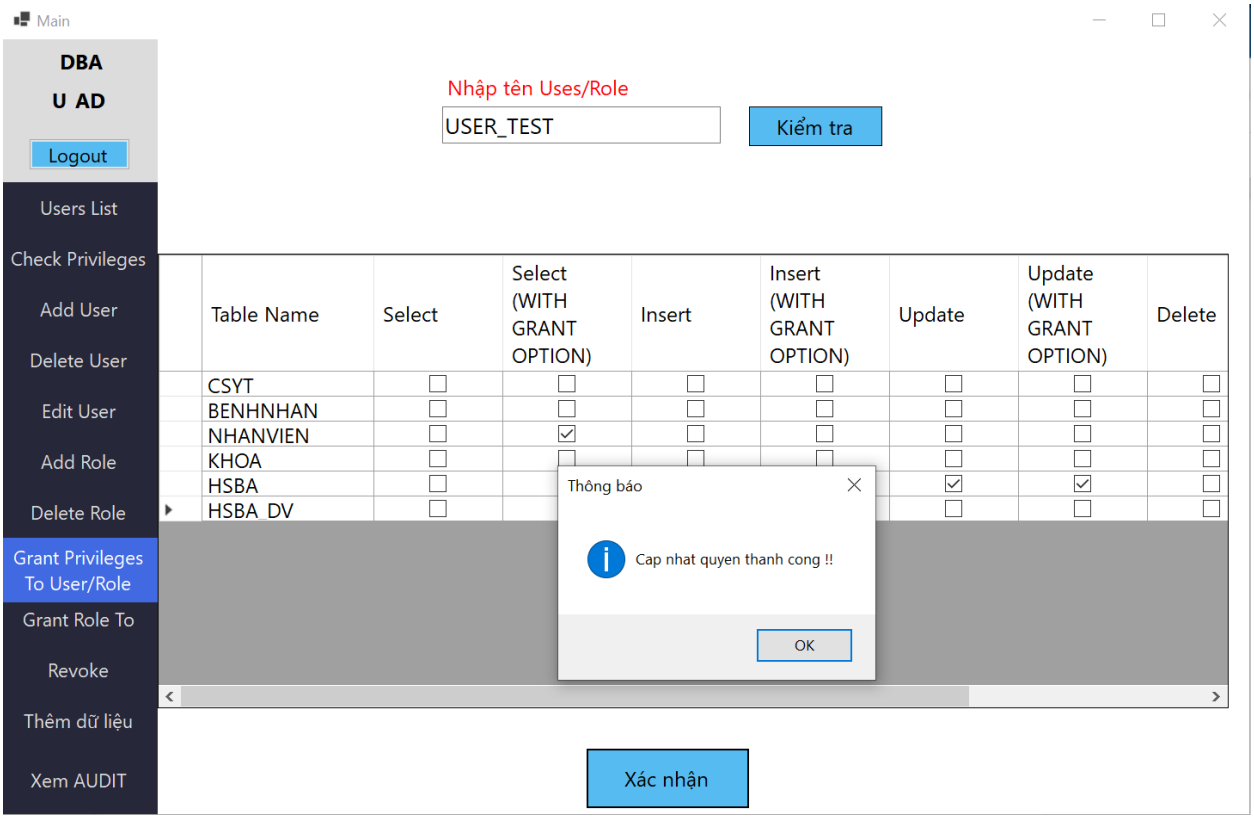
7/ Tạo Role mới:



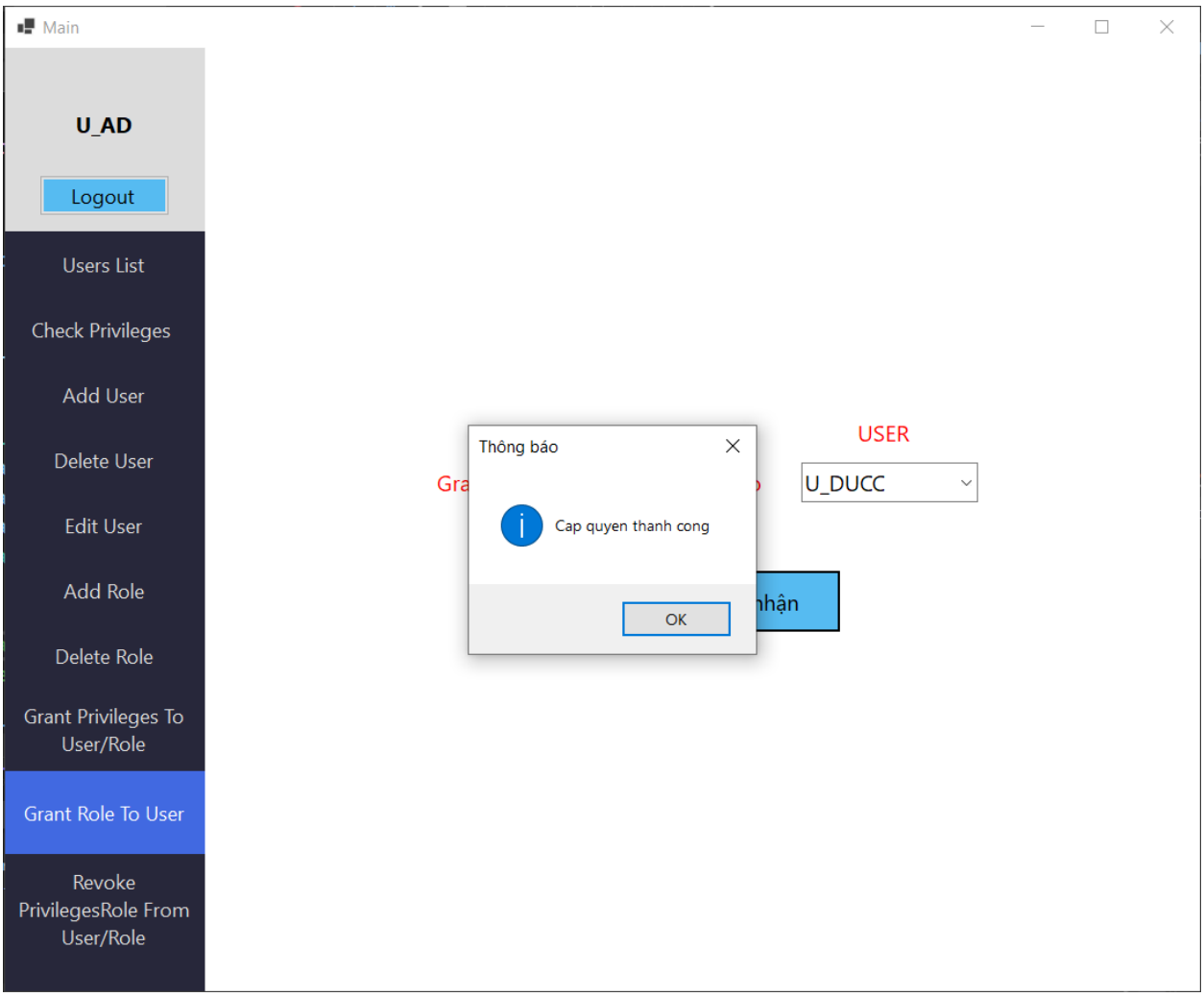
8/ Xoá Role:


Main
ltbmm
Logout
Users List
Check Privileges
Add User
Delete User
Edit User
Add Role
Delete Role
Grant Privileges To User/Role
Grant Role To User
Nhập tên Role cần xoá
minhdeptrai
Xoá
Thông báo
Xoa Role thanh cong!
OK

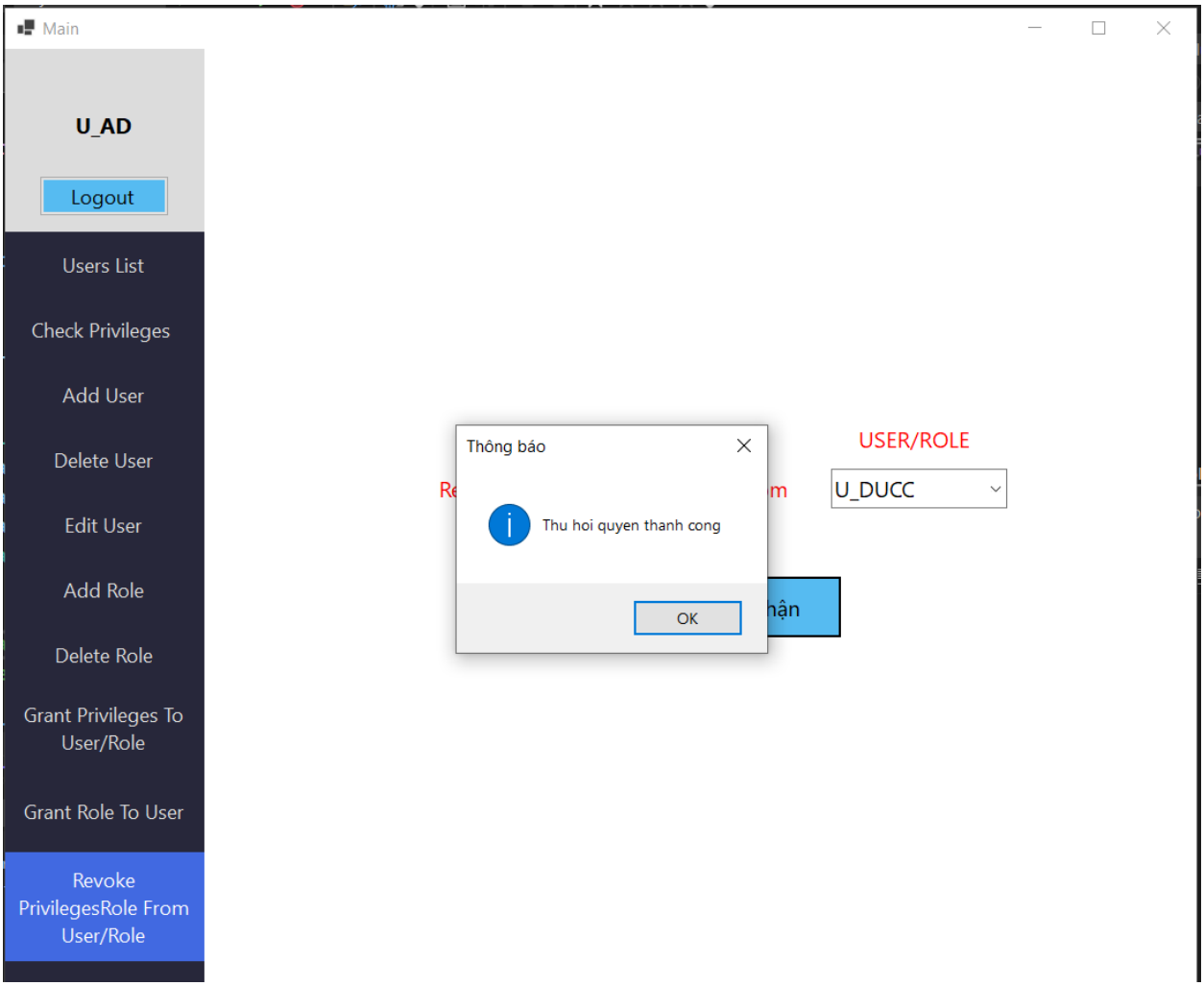
9/ Cấp quyền cho User/Role:



10/ Cấp Role cho User:

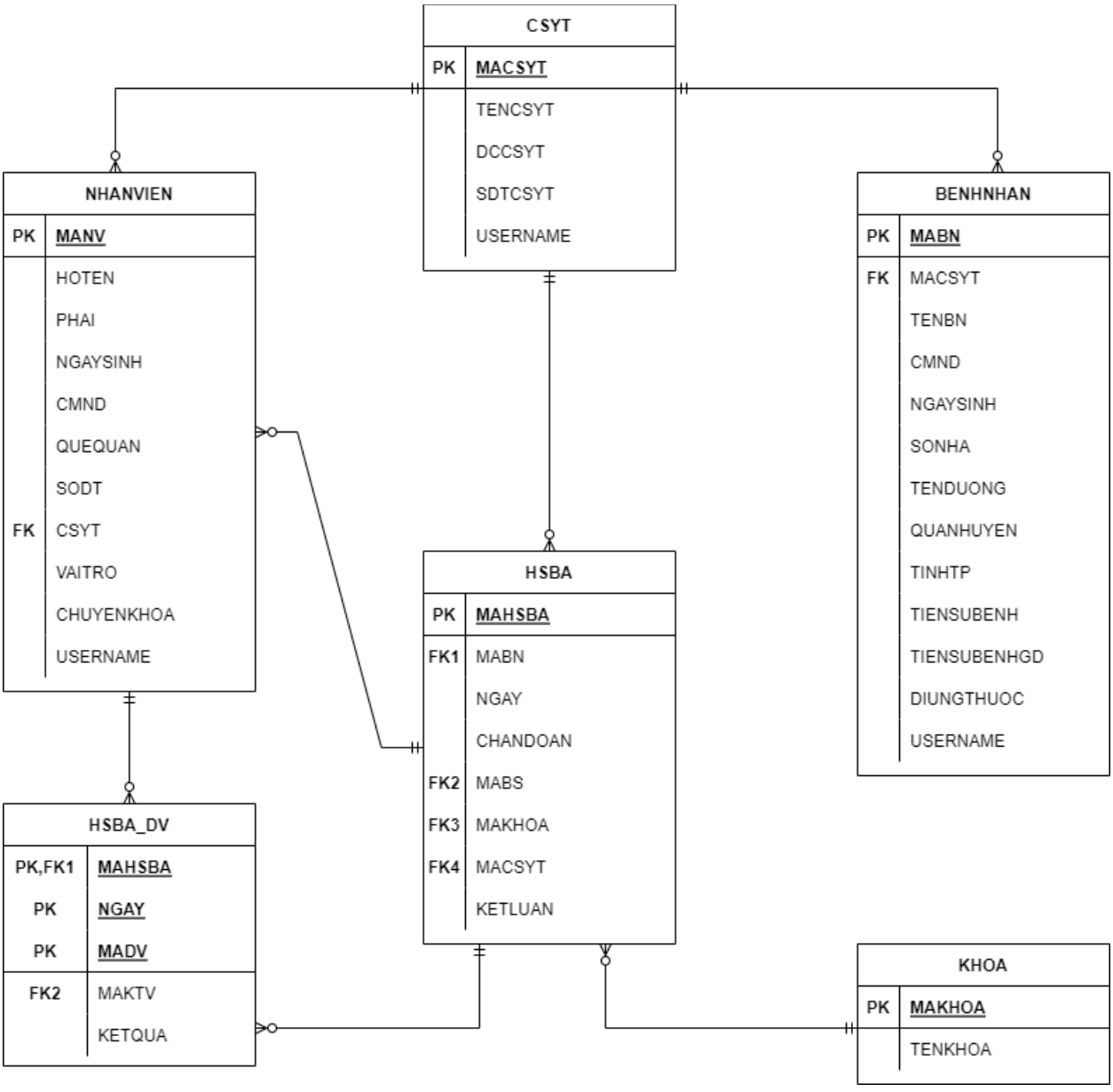


10/ Thu hồi Role khỏi User:



Phân hệ 2

I/ Mô hình cơ sở dữ liệu



II/ Đặc tả dữ liệu

Chú thích: Khoá chính, Khoá ngoại

CSYT	KIỂU DỮ LIỆU	LƯU TRỮ THÔNG TIN CƠ SỞ Y TẾ THUỘC TỈNH/ THÀNH PHỐ
MACSYT	NUMBER	Mã duy nhất của mỗi cơ sở y tế phân biệt với các cơ sở y tế khác trong cùng tỉnh/thành phố.
TENCSYT	NVARCHAR2(50)	Tên cơ sở y tế
DCCSYT	NVARCHAR2(255)	Địa chỉ của cơ sở y tế
SDTCSYT	VARCHAR(15)	Số điện thoại của cơ sở y tế
USERNAME	VARCHAR(50)	Tên đăng nhập vào CSDL của CSYT.

BENHNHAN	KIỂU DỮ LIỆU	LƯU TRỮ THÔNG TIN MỖI BỆNH NHÂN
MABN	NUMBER	Mã duy nhất của mỗi bệnh nhân dùng để phân biệt với các bệnh nhân khác trong cùng một cơ sở y tế
MACSYT	NUMBER	Mã cơ sở y tế
TENBN	NVARCHAR2(50)	Tên bệnh nhân
CMND	NVARCHAR(255)	Chứng minh nhân dân của bệnh nhân
NGAYSINH	DATE	Ngày sinh của bệnh nhân
SONHA	NVARCHAR(50)	Số nhà của bệnh nhân
TENDUONG	NVARCHAR2(50)	Tên đường nhà của bệnh nhân
QUANHUYEN	NVARCHAR2(50)	Quận, huyện nơi ở của bệnh nhân
TINHTP	NVARCHAR2(50)	Tỉnh, thành phố nơi ở của bệnh nhân
TIENSUBENH	NVARCHAR2(255)	Tiền sử bệnh của bệnh nhân

TIENSUBENHGD	NVARCHAR2(255)	Tiền sử bệnh của gia đình bệnh nhân
DIUNGTHUOC	NVARCHAR2(255)	Dị ứng thuốc của bệnh nhân
USERNAME	VARCHAR(50)	Tên đăng nhập vào CSDL của bệnh nhân

NHANVIEN	**KIỂU DỮ LIỆU**	**LƯU TRỮ THÔNG TIN MỖI NHÂN VIÊN**
MANV	NUMBER	Mã duy nhất của mỗi nhân viên dùng để phân biệt với các nhân viên khác trong cùng một tỉnh/thành phố.
HOTEN	NVARCHAR2(50)	Họ tên của nhân viên
PHAI	NVARCHAR2(3)	Giới tính của nhân viên
CMND	NVARCHAR(255)	Chứng minh nhân dân của nhân viên
NGAYSINH	DATE	Ngày sinh của nhân viên
QUEQUAN	NVARCHAR(50)	Quê quán của nhân viên
SDT	VARCHAR(15)	Số điện thoại của nhân viên
CSYT	NUMBER	Cơ sở y tế mà nhân viên đang làm việc
VAITRO	NUMBER	Vai trò của nhân viên. Chỉ nhận một trong các giá trị sau: 1 – Thanh tra 2 – Cơ sở y tế 3 – Y sĩ/ Bác sĩ 4 – Nghiên cứu
CHUYENKHOA	NVARCHAR2(255)	Tên chuyên khoa mà nhân viên được cấp bằng chuyên môn
USERNAME	VARCHAR(50)	Tên đăng nhập vào CSDL của nhân viên

KHOA	KIỂU DỮ LIỆU	LƯU TRỮ THÔNG TIN CÁC CHUYÊN KHOA
MAKHOA	NUMBER	Mã duy nhất của mỗi chuyên khoa dùng để phân biệt với các nhân viên khác trong CSDL.
TENKHOA	NVARCHAR2(255)	Tên chuyên khoa

HSBA	KIỂU DỮ LIỆU	LƯU TRỮ THÔNG TIN CÁC HỒ SƠ BỆNH ÁN
MAHSBA	NUMBER	Mã duy nhất của mỗi hồ sơ bệnh án dùng để phân biệt với các hồ sơ bệnh án khác trong CSDL.
MABN	NUMBER	Mã bệnh nhân tiếp nhận điều trị
NGAY	DATE	Ngày lập hồ sơ
CHANDOAN	NVARCHAR2(255)	Chẩn đoán của bác sĩ
MABS	NUMBER	Mã bác sĩ điều trị
MACSYT	NUMBER	Cơ sở y tế mà bệnh nhân điều trị
MAKHOA	NUMBER	Mã khoa mà bệnh nhân được tiếp đón và điều trị
KETLUAN	NVARCHAR2(255)	Kết luận của bác sĩ

HSBA_DV	KIỂU DỮ LIỆU	LƯU TRỮ THÔNG TIN CÁC HỒ SƠ BỆNH ÁN DỊCH VỤ ĐÃ SỬ DỤNG THEO CHỈ ĐỊNH CỦA BÁC SĨ ĐIỀU TRỊ
MAHSBA	NUMBER	Mã hồ sơ bệnh án.
MADV	NUMBER	Mã duy nhất của mỗi dịch vụ dùng để phân biệt với các dịch vụ khác trong CSDL.
NGAY	DATE	Ngày lập hồ sơ
MAKTV	NUMBER	Mã người thực hiện dịch vụ
KETQUA	NVARCHAR2(255)	Kết quả

III/ Ràng buộc toàn vẹn

- Các thuộc tính của bảng CSYT không nhận giá trị NULL.
- Các thuộc tính của bảng KHOA không nhận giá trị NULL.
- Các thuộc tính của bảng HSBA không nhận giá trị NULL.
- Các thuộc tính của bảng HSBA_DV không nhận giá trị NULL.
- Thuộc tính VAITRO của bảng NHANVIEN chỉ nhận 1 trong 4 giá trị: 1, 2, 3, 4.

IV/ Xác định và phân quyền các loại người dùng

		Nhân viên				Bệnh nhân	U_AD (DBA)
		Thanh tra	Cơ sở y tế	Y/bác sĩ	Nghiên cứu		
NHANVIEN	I						X
	R	X	X	X	X		X
	U		X	X	X		X
	D						X
BENHNHAN	I						X
	R	X		X		X	X
	U					X	X
	D						X

CSYT	I						X
	R	X					X
	U						X
	D						X
HSBA	I		X				X
	R	X	X	X	X		X
	U						X
	D		X				X
HSBA_DV	I		X				X
	R	X	X	X	X		X
	U						X
	D		X				X
KHOA	I						X
	R	X			X		X
	U						X
	D						X

V/ Các chính sách bảo mật

1. 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.

2. 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: quản lý người dùng có vai trò là Nhân viên, gồm 6 Role "con":

- ROLE_THANHTRA: quản lý người dùng có vai trò là Thanh tra.
- ROLE_CSYT: quản lý người dùng có vai trò là Cơ sở y tế.
- ROLE_YBACSI: quản lý người dùng có vai trò là Y bác sĩ.
- ROLE_NGHIENCUU: quản lý người dùng có vai trò là Nghiên cứu

▪ ROLE_BENHNHAN: quản lý người dùng có vai trò là Bệnh nhân.

- TC2: Nhân viên có vai trò là "Thanh tra" thì sẽ được quyền truy đọc dữ liệu trên tất cả các bảng (HSBA_DV, HSBA, NHANVIEN, BENHNHAN, KHOA, CSYT). Nhưng không có quyền thêm, xoá, sửa.
- TC3: Mỗi cơ sở y tế được cấp một tài khoản, tài khoản này thuộc ROLE_CSYT. Nhân viên sử dụng tài khoản này có thể thêm hoặc xóa dữ liệu phát sinh từ chính cơ sở y tế mà nhân viên này trực thuộc, trong tháng hiện tại từ ngày 5 đến ngày 27 dương lịch hàng tháng, liên quan đến các nghiệp vụ:
  - Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)
  - Thêm, xóa dòng dịch vụ (HSBA_DV) liên quan đến hồ sơ bệnh án
  - Role ROLE_CSYT được cấp quyền execute trên 4 stored procedure:
    - DELETE_HSBA: Xóa một dòng hồ sơ bệnh án dựa trên MAHSBA
    - DELETE_HSBA_DV: Xóa một dịch vụ dựa trên MAHSBA_DV, MADV, NGAY
    - INSERT_HSBA: Thêm một dòng trên hồ sơ bệnh án (HSBA)
    - INSERT_HSBA_DV: Thêm một dòng dựa trên hồ sơ bệnh án dịch vụ (HSBA_DV)
- TC4: Nhân viên ở vai trò "Y sĩ/ Bác sĩ" thuộc role ROLE_YBACSI ở mỗi cơ sở y tế có quyền xem hồ sơ bệnh án (HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA_DV) và thông tin bệnh nhân (BENHNHAN). Role ROLE_YBACSI có quyền select trên các view sau:
  - View_YBacSi_Select_HSBA: Y sĩ/ bác sĩ xem thông tin hồ sơ bệnh án mà chính họ đã chữa trị.
  - View_YBacSi_Select_KetQua_HSBADV: Y sĩ/ bác sĩ xem thông tin hồ sơ bệnh án và kết quả dịch vụ mà chính họ đã chữa trị.

- View_YBacSi_Select_BenhNhan: Y sĩ/ bác sĩ xem thông tin bệnh nhân (BENHNHAN)

- TC5: Nhân viên ở vai trò "Nghiên cứu" ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án (bảng HSBA và HSBA_DV) được điều trị tại cùng cơ sở y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.
  Role Nhân viên được cấp quyền Select trên View xem hồ bệnh án.

3. 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.

- VPD được sử dụng như sau:

  - TC6:

    - Trên bảng NHANVIEN: Ngoài DBA và những nhân viên có vai trò là "Thanh tra" thì những nhân viên còn lại chỉ có quyền xem thông tin của chính mình, chỉ có quyền sửa các trường (trừ trường mã) liên quan đến chính người đó.

    - Trên bảng BENHNHAN: Chỉ có quyền xem thông tin của chính mình, chỉ có quyền sửa các trường (trừ trường mã) liên quan đến bản thân mình.

4. 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:*

  - GDS: Giám đốc sở (level_num = 1000).

  - GDCS: Giám đốc cơ sở y tế (level_num = 100).

- YBS: Y bác sĩ (level_num = 10).

- *Compartment:*
  - TT: Trung tâm.
  - CTT: Cận trung tâm.
  - NT: Ngoại thành.
- *Group:*
  - CSAU: Điều trị chuyên sâu.
  - NTRU: Điều trị nội trú (parent_group = 'CSAU').
  - NGTRU: Điều trị ngoại trú (parent_group = 'NTRU').

➢ *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 yêu cầu của TC#7, ta sẽ tạo ra 3 levels tương ứng với 3 cấp bậc người dùng (Giám đốc sở, Giám đốc cơ sở y tế và Y/Bác sĩ). Trong đó level *GDS* tương ứng với "Giám đốc sở" sẽ là level cao nhất và level *YBS* tương ứng với "Y/Bác sĩ" sẽ là level thấp nhất.
- Về *Compartment*: ta thấy theo yêu cầu của TC#7 thì các cơ sở y tế được chia theo vị trí địa lý thành 3 vùng khác nhau đo đó ta tạo 3 compartments khác nhau tương ứng với 3 vùng này.
- Về *Group*: ta thấy theo yêu cầu của TC#7 thì các cơ sở y tế được phân loại theo chuyên môn, kỹ thuật trí thành 3 tuyến khác nhau đo đó ta tạo 3 groups khác nhau tương ứng với 3 tuyến này. Hơn nữa, do cơ sở y tế "Điều trị chuyên sâu" thì có thể "Điều trị nội trú" và "Điều trị ngoại trú", đồng thời cơ sở y tế "Điều trị nội trú" thì có thể "Điều trị ngoại trú" được nên ta tiến hành thêm thuộc tính parent_group của NTRU, NGTRU lần lượt là CSAU và NTRU.

➢ *Thiết lập hệ thống nhãn tương ứng với 5 loại người dùng khác nhau thỏa TC#7:*

- Giám đốc sở:
  - Lý do thiết lập người dùng này: Bắt buộc phải có "Giám đốc sở" vì đây là người dùng có quyền tạo ra các cuộc họp khẩn, có quyền tham gia bất

cứ cuộc họp nào, có quyền xem toàn bộ dữ liệu trong bảng THONGBAO.

- Nhãn tương ứng với người dùng: *GDS:TT, CTT, NT:CSAU*

- Thanh tra:

  - Lý do thiết lập người dùng này: Bắt buộc phải có "Thanh tra" vì đây là người dùng có quyền tạo ra các cuộc họp khẩn, có quyền tham gia bất cứ cuộc họp nào, có quyền xem toàn bộ dữ liệu trong bảng THONGBAO.

  - Nhãn tương ứng với người dùng: *GDS:TT, CTT, NT:CSAU*

- Giám đốc cơ sở y tế:

  - Lý do thiết lập người dùng này: Bắt buộc phải có "Giám đốc cơ sở y tế" vì trong thực tế có thể có trường hợp Giám đốc sở muốn họp khẩn với các lãnh đạo ở các cơ sở y tế hoặc trong trường hợp Giám đốc sở muốn họp với toàn bộ nhân viên y tế trong thành phố nhưng điều đó là gần như không thể nên cần phải thay thế điều đó bằng cách họp với các Giám đốc cơ sở y tế và các Giám đốc cơ sở này sẽ về họp lại với các nhân viên trong cơ sở của họ.

  - Nhãn tương ứng với người dùng: *GDCS:TT, CTT, NT:CSAU*

- Y/Bác sĩ có chuyên môn là điều trị chuyên sâu:

  - Lý do thiết lập người dùng này: Vì trong thực tế có thể có trường hợp Sở yêu cầu một cuộc họp khẩn về một vấn đề quan trọng nào đó mà không chỉ cần họp với các Giám đốc cơ sở y tế mà còn với các Y/Bác sĩ có chuyên môn cao nhất (chuyên môn cao nhất trong TC#7 là Điều trị chuyên sâu).

  - Nhãn tương ứng với người dùng: *YBS:TT, CTT, NT:CSAU*

- Y/Bác sĩ ở các cơ sở trung tâm và có chuyên môn từ điều trị nội trú trở lên:

  - Lý do thiết lập người dùng này: Vì trong thực tế có thể có trường hợp Sở yêu cầu một cuộc họp khẩn về một vấn đề quan trọng nào đó các

Y/Bác sĩ có chuyên môn từ nội trú trở lên. Nhưng nếu mời hết các Y/Bác sĩ nội trú trong toàn thành phố thì số lượng là rất lớn do đó cần giới hạn lại vị trí cơ sở y tế mà các y/bác sĩ đó làm việc là "Trung tâm" – vì ở "Trung tâm" thường là các cơ sở y tế lớn nên kỹ năng của y/bác sĩ ở đây sẽ nhỉnh hơn ở "Cận trung tâm" hoặc "Ngoại thành".

- Nhãn tương ứng với người dùng: *YBS:TT:NTRU*

5. Chính sách Encrypt

➢ *Cơ chế mã hóa:*

- Nhóm chúng em sử dụng package mã hóa dữ liệu của Oracle là DBMS_CRYPTO. Trong package đó, nhóm em sử dụng một số phương pháp để hỗ trợ mã hóa dữ liệu như sau:
  - ENCRYPT_DES: Đây là thuật toán mã hóa DES – Data Encryption Standard. Block cipher. Sử dụng khóa có độ dài 56 bits.
  - CHAIN_CBC: Do quá trình mã hóa sẽ chia dữ liệu thành các khối(block) với kích thước định sẵn(block-size) tùy theo thuật toán mã hóa nên sau khi mã hóa thì cần phải hợp lại các khối này với nhau thành dữ liệu mã hóa theo các phương pháp khác nhau. CHAIN_CBC là một trong số những phương pháp chuyển đổi khối mật mã đó. CBC nghĩa là Cipher Block Chaining (khối plaintext kế tiếp được XOR với khối ciphertext trước đó trước khi nó được mã hóa, Vector khởi tạo (IV) được xem như khối plaintext đầu tiên).
  - PAD_PKCS5: Do các khối mã hóa phải đúng kích thước khối do thuật toán quy định, nếu không khối phải được đệm thêm (pad) cho đúng kích thước khối. PAD_PKCS5 là một trong số các phương pháp làm tăng kích thước, padding dữ liệu sau khi được mã hóa. Phương pháp này cung cấp cơ chế đệm theo tiêu chuẩn PKCS#5 Password-Based Cryptography Standard (thêm vào n số, chỉ n byte còn thiếu của khối cuối cùng, nếu khối cuối cùng đủ thì vẫn đệm thêm toàn bộ khối).

➢ *Các chính sách mã hóa dữ liệu mà nhóm đề ra:*

- Chính sách 1: Mã hóa dữ liệu cột KETLUAN trong bảng HSBA và cột KETQUA trong bảng HSBA_DV.

- Lý do: Do có thể xảy ra trường hợp bệnh nhân có thể là một yếu nhân (một người quan trọng như lãnh đạo cơ quan nhà nước,…) thì thông tin về bệnh nhân đó nên được mã hóa để đảm bảo những người không có phận sự hay liên quan đến bệnh nhân có thể biết được.
- Phương pháp tiến hành: Nhóm tiến hành cài đặt các trigger lên bảng HSBA và HSBA_DV, các trigger này có nhiệm vụ mỗi khi có sự kiện Insert hoặc Update trên bảng HSBA hoặc HSBA_DV thì các trigger này sự động mã hóa cột KETLUAN của HSBA hoặc cột KETQUA của HSBA_DV. Bệnh nhân hoặc các nhân viên có liên quan đến bệnh nhân sẽ được cấp quyền Select lên các view – các view này đã giải mã dữ liệu của cột KETLUAN, KETQUA.
- Quản lý khóa: Khóa sẽ được lưu trữ trên cơ sở dữ liệu. Việc mã hóa và giải mã cũng sẽ được thực hiện trên cơ sở dữ liệu.

- Chính sách 2: Mã hóa dữ liệu cột CMND trong bảng BENHNHAN và bảng NHANVIEN.
  - Lý do: Do chứng minh nhân dân là một thông tin quan trọng của mỗi người, từ chứng minh nhân dân có thể suy ra được rất nhiều thông tin nhạy cảm như về tín dụng, học vấn, người thân,….
  - Phương pháp tiến hành: Nhóm tiến hành cài đặt các trigger lên bảng BENHNHAN và NHANVIEN, các trigger này có nhiệm vụ mỗi khi có sự kiện Insert hoặc Update trên bảng BENHNHAN hoặc NHANVIEN thì các trigger này sự động mã hóa cột CMND của BENHNHAN hoặc NHANVIEN. Bệnh nhân hoặc các nhân viên có liên quan sẽ được cấp quyền Select lên các view – các view này đã giải mã dữ liệu của cột CMND.
  - Quản lý khóa: Khóa sẽ được lưu trữ trên cơ sở dữ liệu. Việc mã hóa và giải mã cũng sẽ được thực hiện trên cơ sở dữ liệu.

6. 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.

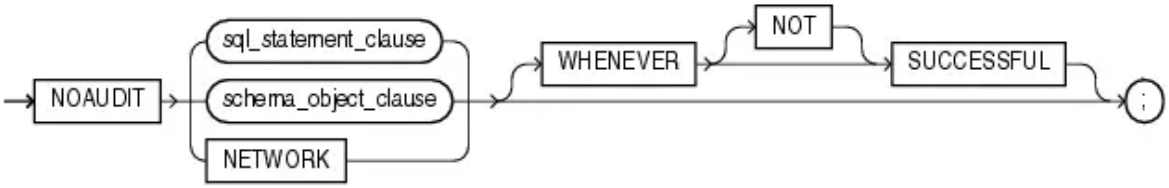
a) Kích hoạt audit toàn hệ thống

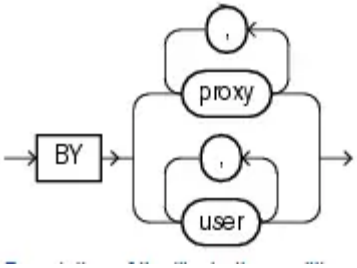
- Chức năng Audit mặc định không được kích hoạt, nhưng có thể kích hoạt bằng lệnh sau: alter system set audit_trail = DB,EXTENDED scope = spfile;
- Các giá trị của audit trail: audit_trail = {none | os | db | DB,EXTENDED | xml | xml, extended} trong đó:
  - none: tắt chế độ audit.
  - os: bật chế độ 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;

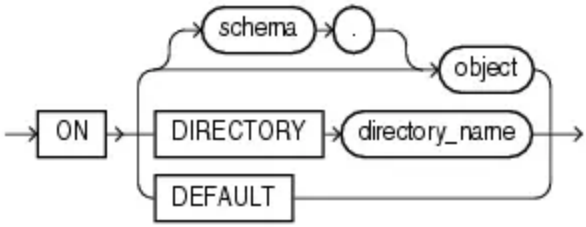
- Kích hoạt STANDARD AUDIT: lệnh AUDIT thiết lập lựa chọn giám sát câu lệnh và quyền thường đi sau mệnh đề "BY" để giới hạn tầm vực của câu lệnh và lựa chọn giám sát quyền:
    - BY ACCESS: Ghi một record cho mỗi câu lệnh và hoạt động được audit
    - BY SESSION: Ghi một record cho tất cả các câu lệnh 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;

b) 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:







- 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;

c) Standard audit

- Chính sách 1: Theo dõi hành vi(SELECT, UPDATE, DELETE, INSERT) của các user trên tất cả table.
- Chính sách 2: Theo dõi các hành vi thực hiện thành công.
- Chính sách 3: Theo dõi các hành vi thực hiện không thành công.

d) Fine-grained audit

- Chính sách 1: Theo nguyên tắc tất cả thông tin cá nhân và hồ sơ bệnh án của bệnh nhân phải được bảo vệ và giữ bí mật thì Fine – grained audit được cài đặt lên cột KETLUAN trong bảng HSBA để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.
- Chính sách 2: Theo nguyên tắc tất cả thông tin về dịch vụ khám bệnh mà bệnh nhân sử dụng phải được bảo vệ và giữ bí mật thì Fine – grained audit được cài đặt lên cột KETQUA trong bảng HSBA_DV để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.
- Chính sách 3: Hiện nay có rất nhiều tình trạng người dân bị rò rỉ CMND và bị mạo danh tài khoản,... Cho nên thông tin CMND của NHANVIEN phải được bảo vệ. Thì Fine – grained audit được cài đặt lên cột CMND trong bảng NHANVIEN để theo dõi hành vi của những người dùng trên đối tượng dữ liệu này.

VIDEO DEMO

PHÂN HỆ 1

(1) FIT HCMUS | AT&BM HTTT | Demo phân hệ 1 - YouTube

PHÂN HỆ 2

(5) FIT HCMUS | AT&BM HTTT | Demo phân hệ 2 - YouTube

SOURCE CODE + SCRIPT (GITHUB)

DAMHONGDUC/phan-he-1: FIT HCMUS | AT&BMHTTT (github.com)