****

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**BÁO CÁO ĐỒ ÁN CUỐI KỲ**

**MÔN: AN TOÀN VÀ BẢO MẬT   
HỆ THỐNG THÔNG TIN**

**| Thành viên |**

**Võ Đại Nam 18120213**

**Phạm Hồ Ngọc Trâm 18120247**

**Phạm Hoàng Việt 18120261**

Thành phố Hồ Chí Minh – Tháng 7 năm 2021

****

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**BÁO CÁO ĐỒ ÁN CUỐI KỲ**

**MÔN: AN TOÀN VÀ BẢO MẬT   
HỆ THỐNG THÔNG TIN**

**| Giáo viên hướng dẫn |**

**TS. Phạm Thị Bạch Huệ**

**ThS. Lương Vĩ Minh**

Thành phố Hồ Chí Minh – Tháng 7 năm 2021

LỜI CÁM ƠN

Để hoàn thành báo cáo này, lời đầu tiên chúng em xin cảm ơn chân thành đến toàn thể thầy cô trong trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Thành phố Hồ Chí Minh nói chung và các thầy cô trong khoa Công nghệ thông tin, bộ môn An toàn và bảo mật Hệ thống thông tin nói riêng, những người đã tận tình hướng dẫn, dạy dỗ và trang bị cho chúng em những kiến thức bổ ích trong học kì vừa qua.

Đặc biệt chúng em xin chân thành gửi lời cảm ơn sâu sắc đến TS Phạm Thị Bạch Huệ,   
ThS Lương Vĩ Minh, ThS Tiết Gia Hồng, những người đã tận tình hướng dẫn, trực tiếp chỉ bảo và tạo mọi điều kiện giúp đỡ chúng em trong ngày học vừa qua.

Sau cùng chúng em xin gửi lời cảm ơn chân thành tới gia đình, bạn bè đã động viên, cổ vũ và đóng góp ý kiến trong quá trình học tập, nghiên cứu cũng như quá trình làm bài báo cáo.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

[LỜI CÁM ƠN 3](#_Toc76340319)

[MỤC LỤC 4](#_Toc76340320)

[CHƯƠNG 1: GIỚI THIỆU 5](#_Toc76340321)

[CHƯƠNG 2: PHÂN CÔNG VÀ YÊU CẦU ĐỒ ÁN 6](#_Toc76340322)

[YÊU CẦU ĐỒ ÁN 6](#_Toc76340323)

[PHÂN CÔNG CÔNG VIỆC 6](#_Toc76340324)

[CHƯƠNG 3: LƯỢC ĐỒ CƠ SỞ DỮ LIỆU 7](#_Toc76340325)

[CHƯƠNG 4: LƯỢC ĐỒ QUAN HỆ 8](#_Toc76340326)

[CHƯƠNG 5: PHÂN TÍCH CÁC CHÍNH SÁCH BẢO MẬT 9](#_Toc76340327)

[ACCESS CONTROL 9](#_Toc76340328)

[1. DAC (Discretionary Access Control) 9](#_Toc76340329)

[2. RBAC (Role-bases Access Control) 9](#_Toc76340330)

[VPD (Virtual Private Database) 10](#_Toc76340331)

[OLS (Oracle Label Security) 11](#_Toc76340332)

[Mã hóa 12](#_Toc76340333)

[Audit 13](#_Toc76340334)

[CHƯƠNG 6: PHÂN TÍCH YÊU CẦU ĐỒ ÁN 14](#_Toc76340335)

[DAC + RBAC 14](#_Toc76340336)

[1. DAC: tạo tài khoản user đăng nhập, tạo view. 14](#_Toc76340337)

[2. RBAC: chia role, phân quyền trên bảng theo role. 14](#_Toc76340338)

[VPD 14](#_Toc76340339)

[OLS 14](#_Toc76340340)

[Mã hóa 14](#_Toc76340341)

[Audit 15](#_Toc76340342)

[CHƯƠNG 7: THAM KHẢO 16](#_Toc76340343)

CHƯƠNG 1: GIỚI THIỆU

Ngày nay, cùng với sự bùng nổ của internet, thông tin và kỉ nguyên số, nhu cầu quản lý thông tin là nhu cầu gần như của mọi tổ chức từ nhỏ đến lớn, trải đều ở hầu hết các ngành nghề lĩnh vực trong cuộc sống. Nhận thấy sự quá tải của hệ thống bệnh viện công cùng với nhu cầu được chăm sóc sức khỏe ngày càng tăng của người dân ở khắp nơi, nhóm những sinh viên bộ môn Hệ thống thông tin chúng em mong muốn đưa ra một giải pháp để quản lý thông tin khám chữa bệnh của các cơ sở y tế một cách hiệu quả, tiết kiệm và dễ sử dụng hơn, nhằm tăng hiệu quả quản lý cũng như làm việc của đội ngũ y tế hiện tại và giúp cho công tác khám chữa bệnh diễn ra nhanh hơn, tốt hơn và chất lượng hơn.

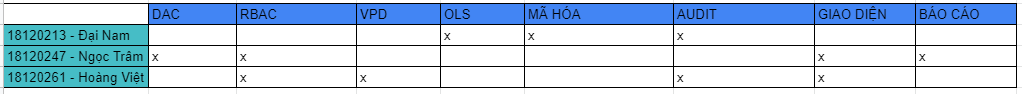
Phần mềm sử dụng công nghệ Windows Presentation Forms (WPF) để xây dựng kết hợp với hệ quản trị cơ sở dữ liệu Oracle và ngôn ngữ truy vấn SQL với các cơ chế điều khiển truy cập, mã hóa, kiểm soát để hiện thực hóa các yêu cầu về quản lý và điều phối dữ liệu bệnh viện dựa trên quyền của người dùng. Người dùng có thể thêm, xóa, sửa và tìm kiếm những thông tin cần thiết cho việc khám chữa bệnh, quản lý và truy xuất thông tin nhân viên và bệnh viện, từ đó đưa ra quyết định cho công tác điều phối nhân viên và điều trị bệnh nhân hiệu quả nhất.

CHƯƠNG 2: PHÂN CÔNG VÀ YÊU CẦU ĐỒ ÁN

YÊU CẦU ĐỒ ÁN



PHÂN CÔNG CÔNG VIỆC



CHƯƠNG 3: LƯỢC ĐỒ CƠ SỞ DỮ LIỆU

Ảnh có chứa văn bản, đen, ảnh chụp màn hình, vài

Mô tả được tạo tự động

CHƯƠNG 4: LƯỢC ĐỒ QUAN HỆ

NHANVIEN(MANV, TENNV, CHUCVU, SDT, LUONG, PHUCAP, MALOAINV, MAPB, MAKHOA)

LOAINHANVIEN(MALOAINV, TENLOAINV)

KHOA(MAKHOA, TENKHOA)

PHONGBAN(MAPB, TENPB)

CATRUC(MAPBENH, MANV, GIOBATDAU, GIOKETTHUC, MAPB)

BENHNHAN(MABN, TENBN, NGAYSINH, DIACHI, SODT)

HOSOBENHNHAN(MAHSBN, MABN, NGAYKB, MATT, MABS, TRIEUCHUNG, CHANDOAN, THUTUC, KETLUANCUABS)

CHITIET\_DICHVU(MACTDV, MAHSBN, MADV, MABS)

DICHVU(MADV, TENDV, DONGIA)

DONTHUOC(MADT, MAHSBN, NVPT, TONGTIEN)

CHITIETDONTHUOC(MACTDT, MADT, MATHUOC, SL)

THUOC(MATHUOC,TENTHUOC, DVT, DONGIA, LUUY)

HOADON(MAHD, MAHSBN, NGAYHD, MANV, NGAYLAP, TONGTIEN)

CTHDON(MAHD, MADV)

CHAMCONG(MANV, THANG,NAM, THOIGIAN)

CHƯƠNG 5: PHÂN TÍCH CÁC CHÍNH SÁCH BẢO MẬT

ACCESS CONTROL

1. DAC (Discretionary Access Control)

Điều khiển truy cập tùy quyền là khi một người chủ thể có quyền định nghĩa các loại truy cập và gán những quyền đó cho các người dùng khác.

Cách thức cơ bản của điều khiển truy cập tùy quyền bao gồm 2 thao tác: gán quyền và thu hồi quyền và 3 đối tượng chính: người dùng, các đối tượng CSD, các quyền: SELECT, INSERT, UPDATE, DELETE, REFERENCE.

Luật điều khiển truy cập định nghĩa: với mỗi chủ thể (subject) và đối tượng (object), sẽ có quy định các loại truy cập (a) mà người dùng được phép làm trên đối tượng đó. Có nghĩa là:

* Chủ thể s được quyền thực hiện loại truy cập a trên đối tượng o.

DAC bao gồm các mô hình sau:

* Mô hình ma trận truy cập (Access matrix model)
* Mô hình Take-Grant (Take-Grant model)
* Mô hình Acten (Action-Entity model)
* Mô hình Wood và cộng sự (Wool et al. model)

1. RBAC (Role-bases Access Control)

Là cơ chế phân quyền dựa vào vai. Khi một vai (role) được tạo, role sẽ được cấp các quyền thực thi action tới đối tượng (object). Và chủ thể (subject) sẽ được gán vào một hoặc nhiều vai tương ứng theo yêu cầu nghiệp vụ.

RBAC có 3 loại mô hình:

* RBAC0: mô hình cơ bản nằm ở dưới cùng cho thấy đó là yêu cầu tối thiểu cho bất kì một hệ thống nào hỗ trợ RBAC.
* RBAC1 có thêm khái niệm cấp bậc role (khi các role có thể kế thừa permission từ role khác).
* RBAC2 có thêm những ràng buộc (đặt ra các hạn chế chấp nhận các dạng của các thành tố khác nhau của RBAC). RBAC1 và RBAC2 không so sánh được với nhau.

VPD (Virtual Private Database)

VPD là 1 chính sách bảo mật cho phép nhiều người dùng truy cập vào một lược đồ duy nhất và ngăn chặn họ truy cập vào dữ liệu mà không liên quan đến họ. Về bản chất, VPD sẽ thực hiện tự động khi đối tượng(table, view hay synonym) được gọi, nó sẽ thêm câu lệnh WHERE (được trả về từ hàm tạo chính sách )vào câu truy vấn của người truy cập CSDL. VPD là sự kết hợp giữa 2 kỹ thuật: Fine-grained access control và application context. Các loại chính sách VPD thường được dùng có thể kế đến như là:

* Row-level Security: chính sách bảo vệ dữ liệu trên hàng.
* Column-level Security: chính sách bảo vệ dữ liệu theo mức cột.
* Column-masking Security: chính sách bảo vệ dữ liệu trên cột, khi người dùng thực hiện câu lệnh (chính sách này chỉ áp dụng được cho câu lệnh SELECT), dữ liệu trả về sẽ là tất cả các hàng, tuy nhiên sẽ trả về giá trị NULL đối với các dữ liệu nhạy cảm (tùy theo người tạo ra chính sách chỉ định)

OLS (Oracle Label Security)

Chính sách bảo mật dựa vào nhãn là một cơ chế dựa trên cơ chế kiểm soát truy cập bắt buộc (Mandatory Access Control – MAC). Đối với một bảng được bảo vệ bởi một chính sách OLS, người dùng muốn truy cập vào một hàng, đòi hỏi nhãn của họ phải thỏa mãn một số tiêu chuẩn đã được định nghĩa trước trong chính sách đó. OSL cung cấp khả năng kiểm soát linh hoạt quyền truy cập vào dữ liệu nhạy cảm và kiểm soát truy cập dữ liệu dựa trên danh tính và nhãn của người dùng, sự nhạy cảm và nhãn của dữ liệu.

Mỗi nhãn dữ liệu sẽ chứa thông tin về mức độ nhạy cảm của dữ liệu. Nó là 1 thuộc tính đơn gồm 3 thành phần:

* Level (thành phần bắt buộc): thành phần phân cấp biểu thị độ nhạy cảm của dữ liệu, chẳng hạn: HIGHLY\_SENSITIVE, SENSITIVE, CONFIDENTIAL, PUBLIC. Đối với mỗi level, ta cần định nghĩa 1 dạng số (numeric form) và 2 dạng chuỗi (chuỗi dài- long form và chuỗi ngắn – short form).
* Compartment (thành phần tùy chọn): thành phần không phân cấp giúp phân lớp dữ liệu chính xác hơn, việc phân loại dữ liệu được phân chia theo lĩnh vực, chuyên ngành, dự án,.… Tức là nếu ta có 2 dữ liệu thuộc 2 compartment C1 và C2, thì có nghĩa là 2 dữ liệu đó thuộc 2 lĩnh vực khác nhau là C1 và C2 và không có nghĩa dữ liệu thuộc C1 nhạy cảm hơn dữ liệu thuộc C2 (hay ngược lại).
* Group (thành phần tùy chọn) biểu diễn mối quan hệ sở hữu (thông thường nó thể hiện cơ cấu của công ty). Do vậy group có cấu trúc cây phân cấp “cha – con”. Một user có nhãn chứa một group cha thì có thể truy xuất dữ liệu thuộc group cha và tất cả các group con của group cha đó.

Mã hóa

Mã hóa dữ liệu là chuyển dữ liệu từ dạng này sang dạng khác hoặc sang dạng code mà chỉ có người có quyền truy cập vào khóa giải mã hoặc có mật khẩu mới có thể đọc được nó.

Các phương pháp mã hóa chủ yếu:

* Phương pháp Mã hóa đối xứng (Symmetric Cryptography). Một số thuật toán phổ biến:
  + Block Cipher
  + Stream Cipher
* Phương pháp Mã hóa bất đối xứng (Asymmetric Cryptography(Public-key Cryptography)). Một số thuật toán phổ biến:
  + Diffie-Hellman key exchange
  + Rivest-Shamir-Adleman (RSA)
  + Digital Signature Algorithms (DSA)
  + ElGamal
  + Elliptic Curve Cryptography (ECC)
  + Paillier cryptosystem
* Phương pháp Mã hóa lai
* Phương pháp Hàm băm mật mã (Cryptographic Hash Function). Một số hàm băm mật mã phổ biến:
  + MD5
  + SHA-0, SHA-1, SHA-224, SHA-256, SHA-512

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. 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 audit:

* Để chắc chắn rằng user chỉ thực hiện truy cập dữ liệu trong quyền hạn của họ.
* Dữ liệu audit giúp phát hiện lỗ hổng trong chính sách bảo mật.
* Ngăn chặn hành vi xấu có thể xảy ra của user.

Các phương pháp audit:

* Application server logs.
* Application auditing.
* Trigger auditing.
* Standard auditing.
* Fine-grained auditing.

CHƯƠNG 6: PHÂN TÍCH YÊU CẦU ĐỒ ÁN

DAC + RBAC

1. DAC: tạo tài khoản user đăng nhập, tạo view.
2. RBAC: chia role, phân quyền trên bảng theo role.

VPD

Bác sĩ chỉ có thể thêm hoặc sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân mà bác sĩ chịu trách nhiệm điều trị. Bác sĩ không được xem hoặc chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống.

Nhân viên bán thuốc chỉ được quyền xem đơn thuốc mà họ được phân công.

OLS

Level: chia thành 3 mức level (HIGHLY\_SENSITIVE(cao nhất), Sensitive (bình thường), confidential (thấp nhất).

Compartment: chia theo các phòng ban (PB01,PB02,PB03,PB04,PB05,PB06,PB07)

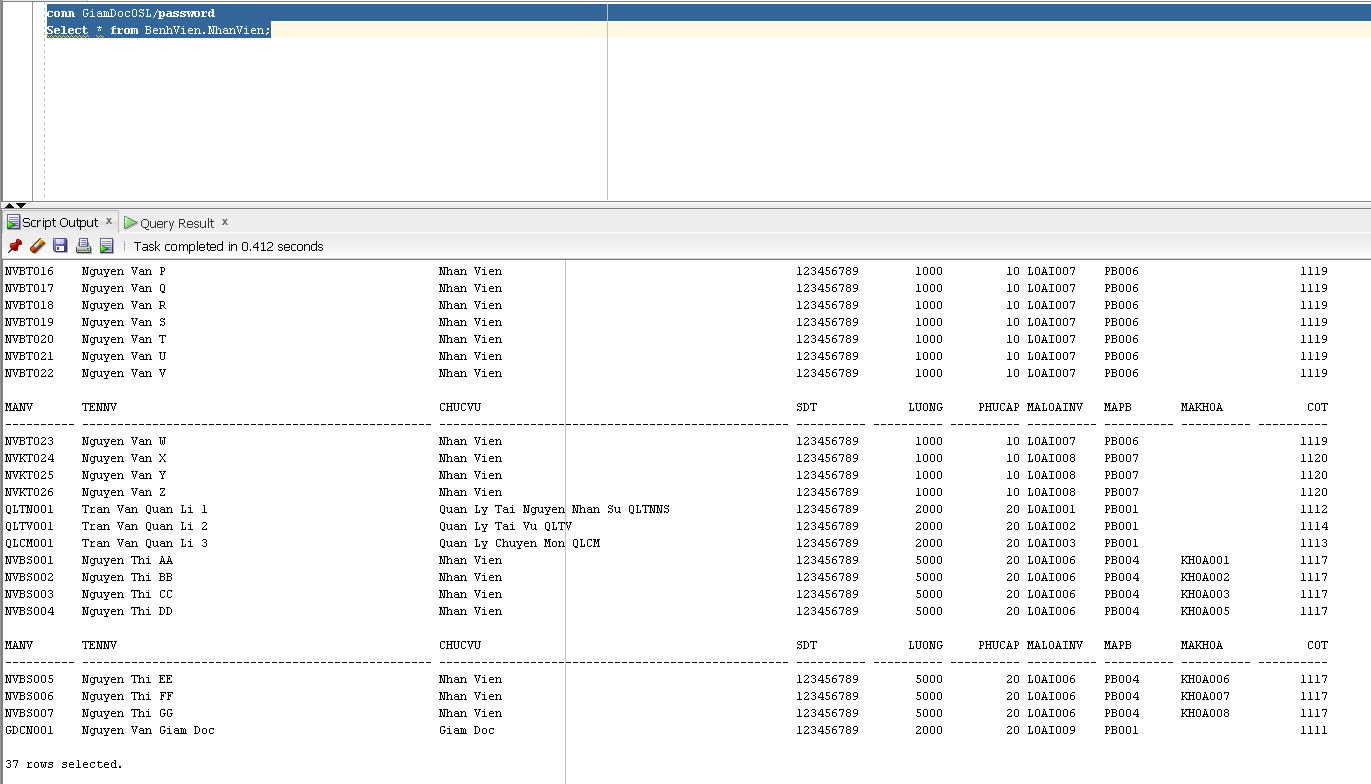
Group: chia thành các group như (quản lý – dành cho user giám đốc, bác sĩ – dành cho user quản lý các bác sĩ, nhân viên – dành cho user quản lý các nhân viên trừ giám đốc)

Lable:

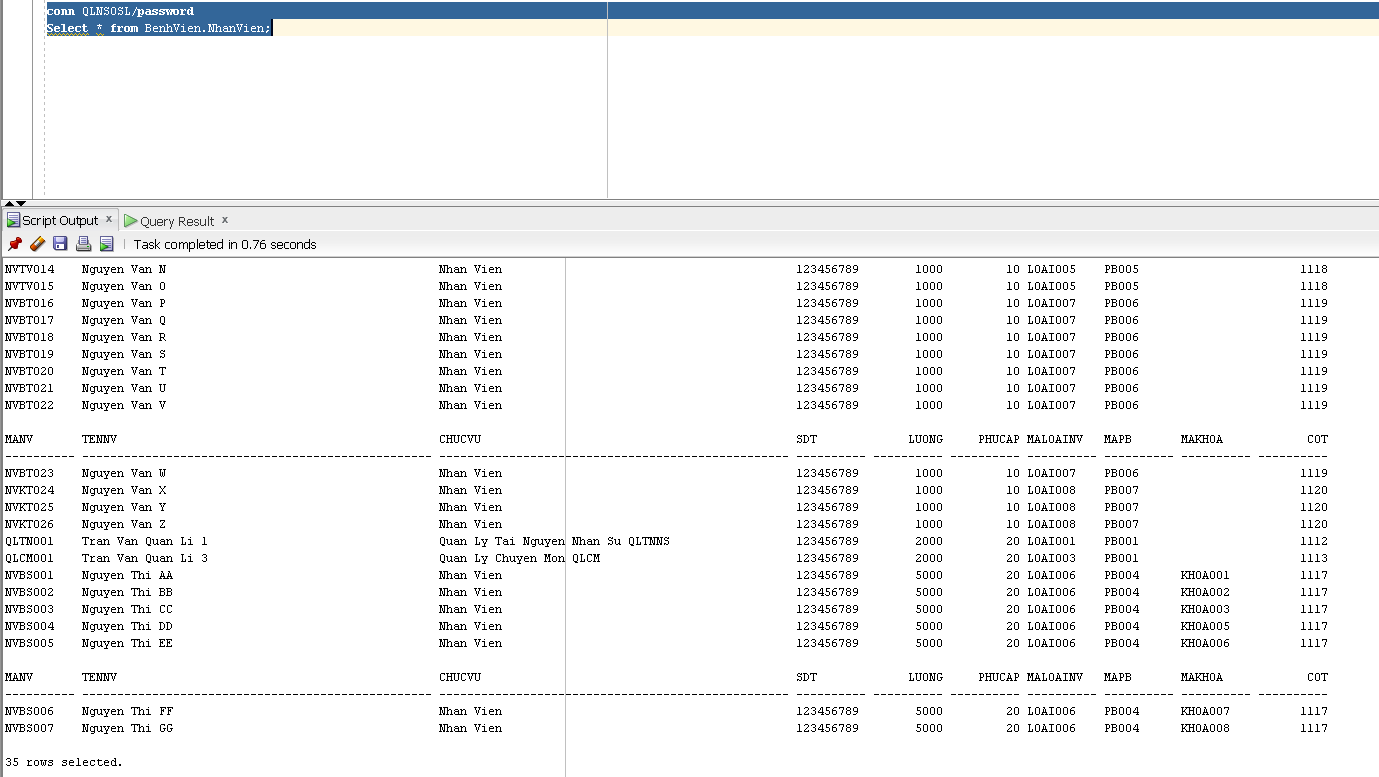
* Với user giám đốc có value: level: Highlysensitive, CompartMent: từ phòng ban 01 -> phòng ban 07, Group: Quản lý.
* Với user quản lý nhân viên có value: level: Sensitive, CompartMent: từ phòng ban 01 -> phòng ban 07, Group: Bác sĩ,Nhân viên.
* Với user quản lý bác sĩ có value: level: Sensitive, CompartMent: Phòng ban 04, Group: Bác sĩ.

Kết quả:

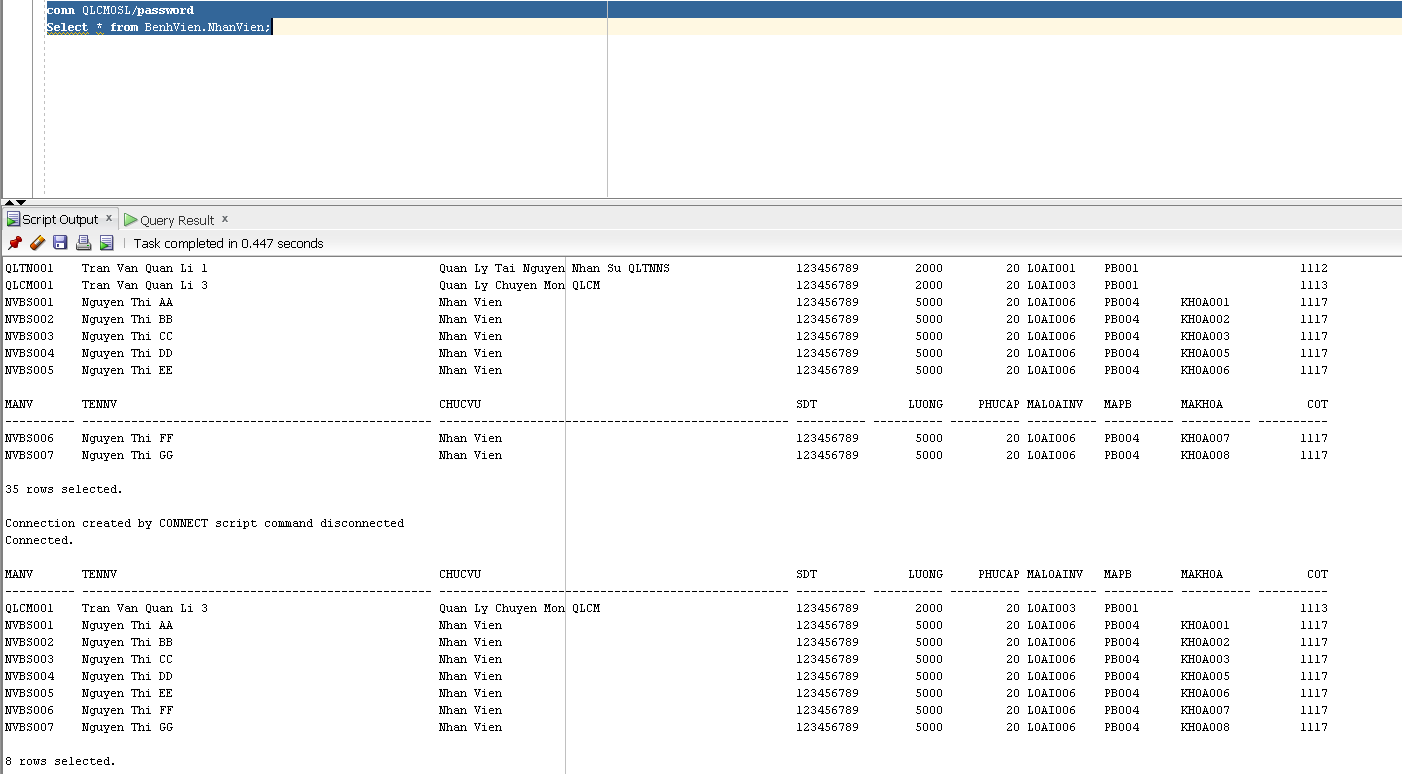
Với user Giám đốc:



Với user QuanLyTNNS:



Với user QuanLyCM:

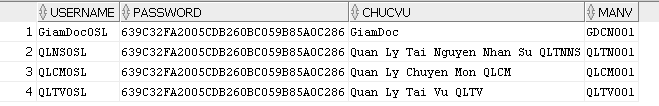


Mã hóa

- Chính sách sử dụng thuật toán DES để quản lý key và sử dụng package để xây dựng thuật toán mã hóa, giải mã.

- Khóa được sử dụng trong package phải là 8 bytes hoặc hơn (ở đây em sử dụng khóa có tên: “MESSYKICHGOAL”.

+ Hình ảnh minh họa bảng được mã hóa



Chính sách mã hóa được quản lý và bảo vệ bằng câu lệnh wrap của oracle, tức là khi người ta vào xem chính sách thì sẽ không thấy nội dung của chính sách mà chỉ là những dãy số.

+ Hình ảnh package được mã hóa để không bị thấy nội dung:



Audit

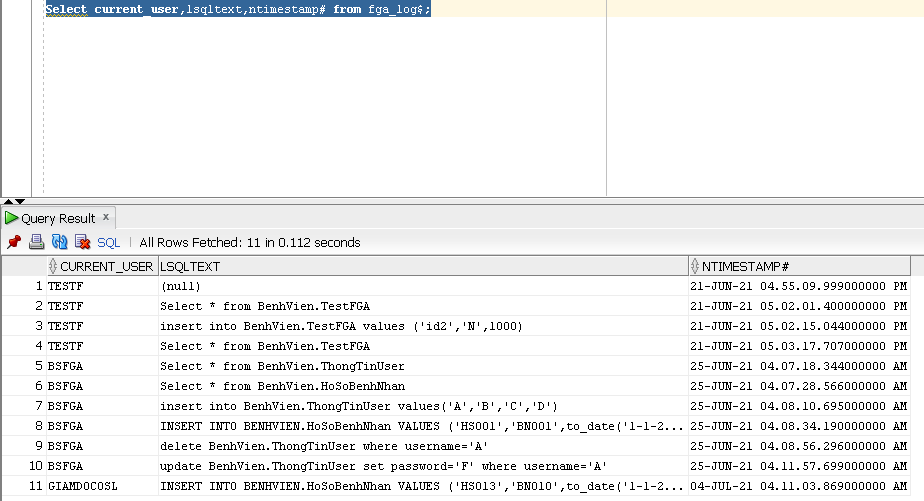
Chính sách 1:

* Chính sách được áp dụng tại bảng Thông Tin user.
* Các thuộc tính được sử dụng để ép chính sách: password, chucvu (vì đây là 2 thuộc tính thường thay đổi trong table nhưng vô cùng quan trọng).
* Các hành động sẽ được ghi lại: Select,insert,update,delete.
* Audit trail: db + extended (để ghi lại được cả sql text).

Chính sách 2:

* Chinh sách được áp dụng tại bảng HoSoBenhNhan.
* Các thuộc tính được sử dụng để ép chính sách: NgayKham,TrieuChung,ChanDoan,KetLuanBS (vì đây là những thuộc tính thường thay đổi trong table nhưng vô cùng quan trọng).
* Các hành động sẽ được ghi lại: Select,insert,update,delete.
* Audit trail: db + extended (để ghi lại được cả sql text).

Các hoạt động sẽ được kiểm tra qua câu lệnh sau:



CHƯƠNG 7: THAM KHẢO

http://antoanthongtin.gov.vn/giai-phap-khac/co-che-an-toan-dua-vao-nhan-va-csdl-tren-oracle-100946

https://docs.oracle.com/database/121/DBSEG/vpd.htm#DBSEG14001

Oracle®, Oracle Label Security Administrator’s Guide 11g Release 2 (11.2), 2013.

Các lỗi xảy ra trong quá trình làm bài, tham khảo ở các trang:

stackoverflow.com

codeproject.com