دانشگاه صنعتی شریف دانشکده مهندسی کامپیوتر	**بسمه تعالی** **پروژه عملیاتی** **موعد تحویل: ۹۱/۴/۲۰**	نام درس: امنیت پایگاه داده نیم‌سال دوم ۹۱-۹۲ مدرس: دکتر رسول جلیلی صفحه ۱

عنوان پروژه:

آشنایی با مدل کنترل دسترسی سمپاد **PostgreSQL** در محیط عملیاتی

لطفاً به نکات زیر توجه فرمایید:

- پاسخ‌های خود را حداکثر تا ۹۱/۴/۲۰ به آدرس Mahdi1001@gmail.com با عنوان [DBSEC:Project_SN1_SN2] ارسال نمایید. تأخیر در ارسال پاسخ مشمول کسر نمره خواهد بود.
- این پروژه را می‌توانید در غالب گروه‌های دو نفره (که بسیار بر گروهی بودن توصیه می‌شود) انجام دهید.
- در صورت استفاده از مرجعی خاص در گزارش نهایی خود، به آن ارجاع دهید.

۱ توضیحات و تشریح مسئله

سیستم مدیریت پایگاه داده (سمپاد) PostgreSQL[1] یکی از قدرتمندترین سمپادهای متن باز است که در اغلب دانشگاه‌های معتبر از آن برای تعریف پروژه‌های آموزشی استفاده می‌شود. بر این اساس و با توجه به نیازی که به آشنایی دانشجویان درس امنیت پایگاه داده با یک محیط عملیاتی حس می‌شد این پروژه تعریف گردید. این پروژه شامل فازهای زیر است:

۱. آشنایی کلی با این سمپاد و نصب و پیکربندی آن
۲. آشنایی با مدل کنترل دسترسی این سمپاد که در حقیقت یک مدل کنترل دسترسی نقش مبنا است.
۳. ایجاد پایگاه داده Medical_DB که در بخش بعدی معرفی می‌شود.
۴. تعریف نقش‌ها، و اعمال خط مشی امنیتی درخواستی پروژه با توجه به دانشی که در فاز دوم کسب کرده‌اید.
۵. تست و ارزیابی پرس‌وجوهای درخواستی
۶. آماده کردن گزارش و تحویل حضوری

۱,۱ پایگاه داده

پایگاه داده‌ای که در این پروژه مورد استفاده قرار می‌گیرد دارای جداول زیر است.

Patient(pid INTEGER, fname VARCHAR(20), lname VARCHAR(20), age INT, street VARCHAR(20), city VARCHAR(10), zipcode VARCHAR(5))
Disease(pid INTEGER, disease VARCHAR(20))
Doctor(did INTEGER, fname VARCHAR(20), lname VARCHAR(20), specialty VARCHAR(20))
Sees(pid INTEGER,did INTEGER)
Product(eid INTEGER, description VARCHAR(20))
Stock(eid INTEGER, quantity INTEGER)
Supplier(sid INTEGER, name VARCHAR(20), street VARCHAR(20), city VARCHAR(10), zipcode VARCHAR(5))
Supplies(eid INTEGER,sid INTEGER)

[1] http://www.postgresql.org/

۱,۲ توضیحات مربوط به جداول

- جداول Doctor و Patient اطلاعات پزشکان و بیماران را نگهداری می‌کنند.
- جدول Disease بیماری هر بیمار را نمایش می‌دهد.
- جدول Sees نشان می‌دهد بیماران توسط کدام دکترها معاینه شده‌اند.
- جدول Product اطلاعاتی را درباره‌ی محصولات پزشکی وسایل جانبی مهیا می‌کند.
- جدول Stock ، تعداد هر محصول را نگهداری می‌کند.
- در جدول Supplier اطلاعاتی درباره‌ی شرکت‌های تامین کننده مواد مورد نیاز بیمارستان ذخیره می‌شود.
- جدول Supplies نشان می‌دهد هر محصول توسط چه شرکت‌هایی تولید می‌شود.

در هر جدول، زیرِ خصیصه‌هایی که کلید اصلی آن جدول را تشکیل می‌دهند، خط کشیده شده است. در ضمن کلیدهای خارجی این جداول به صورت زیر است:

- Disease.pid کلید خارجی برای Patient.pid
- Sees.pid کلید خارجی برای Patient.pid
- Sees.did کلید خارجی برای Doctor.did
- Stock.eid کلید خارجی برای Product.eid
- Supplies.eid کلید خارجی برای Product.eid
- Supplies.sidکلید خارجی برای Supplier.sid

۱,۳ نقش‌های موجود و طبقه‌بندی اطلاعات

نقش‌ها:

- کاربر عادی (PublicUser)
- پرستار (Nurse)
- پزشک (Physician)
- مدیر بخش پزشکی(MedicalManager)
- مسئول انبار (Storekeeper)
- مدیر بیمارستان (Administrator)

از طرفی اطلاعات بیمارستان به سه دسته کلی تقسیم می‌شود:

۱. اطلاعات پزشکی: اطلاعات درباره‌ی پزشکان، بیماران، و بیماری‌ها
۲. اطلاعات اجناس: اطلاعات محصولات، تامین کننده‌گان آنها و موجودی محصولات در بیمارستان.
۳. اطلاعات عمومی: نام پزشکان، تخصصشان، بیماری‌های قابل درمان در این بیمارستان، و نام تولید کننده‌گان برای بیمارستان.

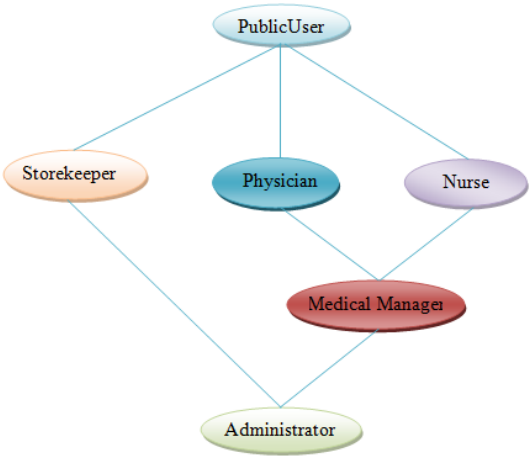
توجه کنید که هیچ کدام از اطلاعات بیماران عمومی نیست.

۱,٤ خط‌مشی کنترل دسترسی

خط‌مشی کنترل دسترسی این پایگاه داده شامل قواعد زیر است:

۱. افراد عادی فقط حق خواندن اطلاعات عمومی را دارند. همه نقش‌ها شامل مدیر، پزشک، و پرستار حق دسترسی عمومی را دارند.
۲. کاربرانی که نقش پزشک را دارند حق خواندن و بروزرسانی روی داده‌های پزشکی را دارند، اما حق ایجاد و حذف آن را ندارند. همچنین پزشکان حق بروزرسانی، حذف، و یا ایجاد اطلاعات پزشکان را ندارند.
۳. پرستارها حق خواندن نوشتن، بروزرسانی، و حذف روی داده‌های پزشکی دارند. آنها نمی توانند اطلاعات پزشکان را بروزرسانی، حذف، و یا ایجاد نمایند.
۴. کاربران مدیر بخش پزشکی هم حق‌های پزشک و هم حق‌های پرستاران را دارند. و حق خواندن، بروزرسانی، حذف، و ایجاد اطلاعات جدول پزشکان را دارند.
۵. کاربرانی که نقش مسئول انبار را دارند فقط حق خواندن، بروزرسانی، حذف، و ایجاد اطلاعات مربوط به موجودی انبار و تولیدکنندگان را دارد.
۶. مدیر بیمارستان نیز به همه‌ی حق‌های کاربران دیگر را دارد کامل دارد.

(راهنمایی: با استفاده از مدل سلسله مراتب زیر باید از وراثت استفاده نمایید.)



۱,۵ مسئله اول

در قدم اول این پروژه لازم است که موارد زیر انجام شود(**توجه کنید که هر دستور SQL ای را که اجرا می‌کنید به همراه هدف اجرای آن و نتیجه آن به صورت کامنت در فایل access-control.sql ذخیره کرده و به همراه گزارش نهایی خود ارسال نمایید**) :

۱. ایجاد پایگاه داده با نام Medical_DB و ایجاد جداول با همان نام‌ها در این پایگاه داده
۲. ایجاد نقش‌های معرفی شده و اعطای و گرفتن مجوزهای بیان شده
۳. با توجه به اطلاعات موجود در جدول زیر، کاربران درخواستی را ایجاد نمائید.

نام کاربر	نقش	پسورد
PUser1	PublicUser	123456
Nurse1	Nurse	123456
Physician1	Physician	123456
SKeeper1	Storekeeper	123456
MManager1	MedicalManager	123456
Admin1	Administrator	123456

۴. با ورود به سیستم در نقش کاربران ایجاد شده در قدم سوم و طراحی پرس‌وجوهای مناسب و اجرای آنها نشان دهید که خط‌مشی کنترل دسترسی را به درستی پیاده کرده‌اید(ثبت پرس‌وجوهایی که اجرا می‌کنید فراموش نشود)

۱,۶ مسئله دوم

یک یا چند دید ازپایگاه داده بسازید که فقط اطلاعات عمومی را نمایش دهند. حق دسترسی دیدن این دیدها را به نقش ها اعطا نمایید.**آیا اعطای دسترسی به همه نقش‌ها بصورت صریح لازم هست؟؟؟**

همه دیدهای لازم را بسازید و حق دسترسی متناسب با آن را به نقش آن بدهید. در برخی مواقع ممکن است نیازی به تعریف دید نباشد و شاید لازم باشد که حق دسترسی را به خود جدول بدهید.

۱,۷ مسئله سوم

مشکل گمنامی:

گاهی لازم است بیمارستان‌ها اطلاعات خود را برای محققین در دسترس آنها قرار دهند. برای اینکار بیمارستان‌ها تنها کدپستی، سن، نام بیماری را در اختیار محققین قرار می‌دهند. یک نقش محقق (Researcher) ایجاد نمایید و یک کاربر آزمایشی (Researcher1) از آن بسازید. دیدی را با نام DiseaseResearch که دارای فیلدهایی است که محققین به ان دسترسی دارند ایجاد نمائید و حق دسترسی به ان را به نقش محقق اعطا کنید. همانند مسئله اول با طراحی پرس‌وجوهای مناسب و ورودی به سیستم با عنوان کاربر Reserecher1 بررسی کنید که محققین فقط می‌توانند به این اطلاعات دسترسی داشته باشد.

حال اگر بیمارستان یک انتخابات الکترونیکی برای انتخاب بهترین دکتر و پرستار برگزار نماید، که در پایگاه داده‌ی آن مشخصات افراد : نام، نام خانوادگی، سن، کد پستی ذخیره می‌شود و حق خواندن برای همه باز است. نشان دهید چگونه یک محقق می‌تواند بیماری افراد را با مشخصات‌شان بدست آورد. **راه حل شما برای جلوگیری از این مشکل چیست؟؟؟**

۱,۸ نحوه‌ی تحویل پروژه

در این پروژه لازم است کارهای انجام شده را در قالب یک مستند شرح دهید و در کنار آن همانطور که توضیح داده شده است فایل **access-control.sql** را که توسط شما تکمیل می‌شود را ارسال نمایید. برای تحویل حضوری اطلاعات پایگاه داده در اختیارتان قرار داده می‌شود و کارهای انجام شده را بر روی پایگاه‌داده نمایش می‌دهید.

هر گونه سوال یا ابهام در رابطه با این پروژه را می‌توانید از آقای اسحاقی (Mahdi1001@gmial.com) بپرسید.