ЛАБОРАТОРНАЯ РАБОТА №2

Цель работы

Получение навыков составления запросов и защиты от SQL – инъекций в СУБД.

Задание на работу

Варианты выполнения лабораторной работы представлены ниже

1. Реализовать представленные запросы (таблица вариантов выполнения 1). При этом:
    a. Заданные данные оформить в виде входной переменной любого типа
    b. Каждый пункт «выбрать» необходимо выполнить в виде одного SQL – запроса без промежуточных таблиц (структура with).
    c. Обратите внимание, что формулировки и уточнения к запросам направлены на то, чтобы вы правильно поняли, что от вас требуется, но НЕ подсказывают способ решения.
2. Изучить представленный код (SQL - файл из папки «ЛР2 варианты»). Обратите внимание, что вариантов этого задания БОЛЬШЕ, чем схем в таблице 1. Можно модифицировать под свою СУБД.
3. Составить и реализовать цепочку SQL – инъекций к доступным процедурам (процедуре) для получения пароля администратора, заданного в коде и хранящегося в СУБД.
4. Составить набор методов защиты от инъекций для данного примера. Продемонстрировать его эффективность.
5. Предложите по крайней мере один пример инъекции, которая осталась возможна.

Содержание отчета

1. Титульный лист.
2. Цель работы.
3. Задание на работу (целиком, с указанием данных конкретного варианта).
4. Схема данных.
5. Разработанные запросы в виде:
    5.1. Словесный текст запроса из задания
    5.2. SQL – код запроса из задания
    5.3. Пример данных и корректной работы кода (учтите особенности третьего запроса при подборе для него тестовых данных)
6. Цепочка SQL – инъекций для получения пароля администратора. Для каждого этапа (инъекции) укажите:
    6.1. Описание этапа

6.2. Код инъекции
6.3. Результат (скриншот)

7. Методы защиты. Для каждого метода укажите:
   7.1. Какая выявленная уязвимость закрывается
   7.2. Метод закрытия (включая код при необходимости)
   7.3. Результат попытки проведения инъекции после установки данного этапа защиты
8. Выводы по работе.
9. Список литературы.

Вариант	Описание данных	Описание запросов
1.	Отношение 1 Номер рецепта(PK), Код заболевания, ФИО пациента(AK1), Дата выписки (AK1), ФИО врача, Срок действия в днях если есть, Наименование лекарства, Код лекарства, Признак того что рецепт использован, Номер аптеки (FK) Отношение 2 Номер аптеки (PK), ФИО провизора (AK), Город аптеки, Адрес аптеки	*Заданные данные оформить в виде входной переменной любого типа* Выбрать ФИО всех пациентов заданного врача, у которых выписано любыми врачами в сумме больше трех рецептов. Выбрать все номера рецептов, срок действия которых не в интервале от 10 до 30 дней Выбрать ФИО пациентов, у которых рецепты были использованы во всех аптеках, которые вообще реализовали хотя бы один рецепт за исключением пациентов, которые при этом являются провизорами.
2.	Отношение 1 Номер кабинета (AK1), Код заболевания, ФИО пациента(PK), Дата и время приема (PK, AK1, AK2), ФИО врача (AK2), Дата следующего приема если есть, Описание диагноза Отношение 2 Код анализа (PK), ФИО пациента (PK, FK1), Дата и время назначения анализа (PK, FK1), Признак готовности анализа, описание результата анализа	*Заданные данные оформить в виде входной переменной любого типа* Выбрать ФИО всех пациентов заданного врача, у которых у любых врачей в сумме больше трех приемов. Выбрать ФИО всех пациентов, дата следующего приема которых не в течении заданных месяцев (в общем случае нескольких). Выбрать ФИО пациентов, у которых присутствуют все коды заболевания (проставленные любым врачом), которые когда либо ставил заданный врач, за исключением пациентов, никогда не сдававших анализов.
3.	Отношение 1 Номер партии лекарства, Код лекарства, Серийный номер пачки лекарства (PK), Число единиц лекарства в пачке, Производитель, Дата окончания срока годности, температура хранения если указана, Признак наркотического содержимого Отношение 2 ФИО врача (PK), Дата выписки, ФИО пациента кому назначено, Серийный номер	*Заданные данные оформить в виде входной переменной любого типа* Выбрать все коды лекарств заданного производителя, у которых на складе хранится более трех пачек (вне зависимости от производителя этих пачек). Выбрать все коды лекарств, у которых температура хранения не входит в заданный интервал. Выбрать ФИО всех пациентов, которым назначены все лекарства (любым врачом), которые когда либо назначал заданный

Вариант	Описание данных	Описание запросов
	пачки лекарства (FK, PK), сколько единиц выдано	врач, за исключением ФИО пациентов, которые при этом являются врачами.
4.	Отношение 1 Дата и время вызова (AK1, PK), Дата и время приезда к пациенту (AK2, AK3), ФИО пациента(AK2), Адрес пациента (PK), Номер бригады скорой помощи (FK, AK1, AK3), Диагноз пациента, Признак госпитализации пациента, Действия на месте если были выполнены, ФИО дежурного диспетчера Отношение 2 Номер бригады скорой помощи (PK), ФИО врача бригады, Должность врача в бригаде	*Заданные данные оформить в виде входной переменной любого типа* Выбрать адреса пациентов, к которым скорая приезжала наибольшее число раз. Выбрать информацию по всем вызовам скорой, когда на месте не выполнялись заданные действия (в общем случае несколько). Выбрать номера бригад, которые хотя бы раз выезжали по указанию каждого из указанных в базе данных дежурных диспетчеров или включают в бригаде врача в заданной должности.
5.	Отношение 1 ФИО сотрудника(PK), Номер документа сотрудника(AK1), Телефон сотрудника(AK2), Дата рождения, Число несовершеннолетних детей, Семейное положение, Уровень образования, Отдел, Общий стаж в годах, Дата приема на работу, Сведения о повышении квалификации Отношение 2 ФИО сотрудника(PK, FK), дата приема на должность(PK), дата окончания работы в должности если есть, название должности	*Заданные данные оформить в виде входной переменной любого типа* Выбрать все отделы, у которых наибольшее число сотрудников с несовершеннолетними детьми. Выбрать ФИО всех сотрудников, дата окончания работы в должности которых не в течении заданных месяцев (в общем случае нескольких). Выберите ФИО сотрудников, успевших поработать в организации на всех возможных должностях и ФИО сотрудников у которых контракт не закончился ни разу (запись о работе только одна без окончания срока действия).
6.	Отношение 1 Название подразделения(PK), Номер отдела (PK, AK1), ФИО руководителя (AK1, FK), Число ставок в отделе, Зарплатный фонд отдела, Число занятых ставок в отделе Отношение 2 ФИО сотрудника (PK), Название подразделения(FK1), Номер отдела (FK1),	*Заданные данные оформить в виде входной переменной любого типа* Выбрать ФИО всех сотрудников и все названия их должностей, которые работают в сумме больше, чем на 1 ставку. Выбрать все номера отделов, число занятых ставок в которых не находится в заданном интервале. Выбрать ФИО сотрудников, работающих во всех подразделениях организации

Вариант	Описание данных	Описание запросов
	доля занимаемой ставки, название должности, характеристика	одновременно и ФИО сотрудников которые не руководят ни одним отделом.
7.	Отношение 1 Код проекта (PK), Название проекта (AK1), Наименование задачи (PK, AK1), ФИО исполнителя (FK), Трудоемкость в часах, Плановая дата выполнения, Реальная дата выполнения если есть, Описание задачи, Отметка о принятии задачи руководителем Отношение 2 ФИО сотрудника(PK), Должность, Подразделение, Код проекта которым руководит сотрудник если он есть	*Заданные данные оформить в виде входной переменной любого типа* Выберите все коды и названия проектов, в которых больше трех задач, еще не принятых руководителем. Выберите все наименования задач и ФИО их исполнителей, у которых реальная дата выполнения не лежит в заданном интервале. Выберите ФИО сотрудников, поработавших на всех проектах и ФИО сотрудников, выполнивших все задачи хотя бы одного своего проекта.
8.	Отношение 1 Тип документа, Номер документа (PK), ФИО ответственного, Содержимое документа (JSON) (AK), Выпустившее подразделение, Дата ввода в действие, Дата окончания действия если есть, Степень секретности если есть Отношение 2 ФИО сотрудника(PK), Номер документа (PK, FK), Дата изменения(PK), Операция с документом	*Заданные данные оформить в виде входной переменной любого типа* Выберите ФИО ответственных, которые отвечают более чем за один секретный документ заданной степени. Выберите номера документов и ФИО ответственных для документов, срок окончания действия которых не в течении заданных месяцев (в общем случае нескольких). Выберите ФИО сотрудников, совершавших с каким-либо документом все возможные операции или отвечающих за документы, но не выполнивших с этими документами ни одной операции.
9.	Отношение 1 Инвентарный номер (PK), Наименование (AK1), ФИО материально ответственного, Помещение где размещено (AK1), Дата принятия на баланс, Дата снятия с баланса если есть, Срок службы если есть, Балансовая стоимость Отношение 2	*Заданные данные оформить в виде входной переменной любого типа* Выберите ФИО материально ответственных, которые отвечают за объекты учета с суммарной балансовой стоимостью больше заданной. Выберите инвентарные номера объектов и ФИО ответственных для объектов, срок службы которых не находится в заданном интервале.

Вариант	Описание данных	Описание запросов
	Код помещения (PK), Код помещения в которое входит данное если оно есть (FK), ФИО ответственного за помещение	Выберите ФИО материально ответственных лиц, объекты которых располагаются во всех без исключения помещениях и при этом не являющихся ответственными за помещение.
10.	Отношение 1 Код инцидента безопасности (PK), Подразделение, Критичность инцидента по классификатору, Дата и время инцидента безопасности (PK, AK1), ФИО заведшего запись об инциденте (AK1, FK1), ФИО ответственного за расследование (FK2), Дата закрытия инцидента если есть, Сумма установленного ущерба если есть, Статус инцидента Отношение 2 ФИО сотрудника (PK), Должность, Подразделение	*Заданные данные оформить в виде входной переменной любого типа* Выберите ФИО ответственных за инциденты, суммарная сумма ущерба инцидентов которых больше заданной. Выберите код, дату и время, ФИО ответственных для инцидентов, дата закрытия которых не в течении заданных месяцев (в общем случае нескольких). Выберите ФИО сотрудников, которые работают во всех без исключения подразделениях, за исключением ФИО сотрудников, имеющих не закрытые инциденты.