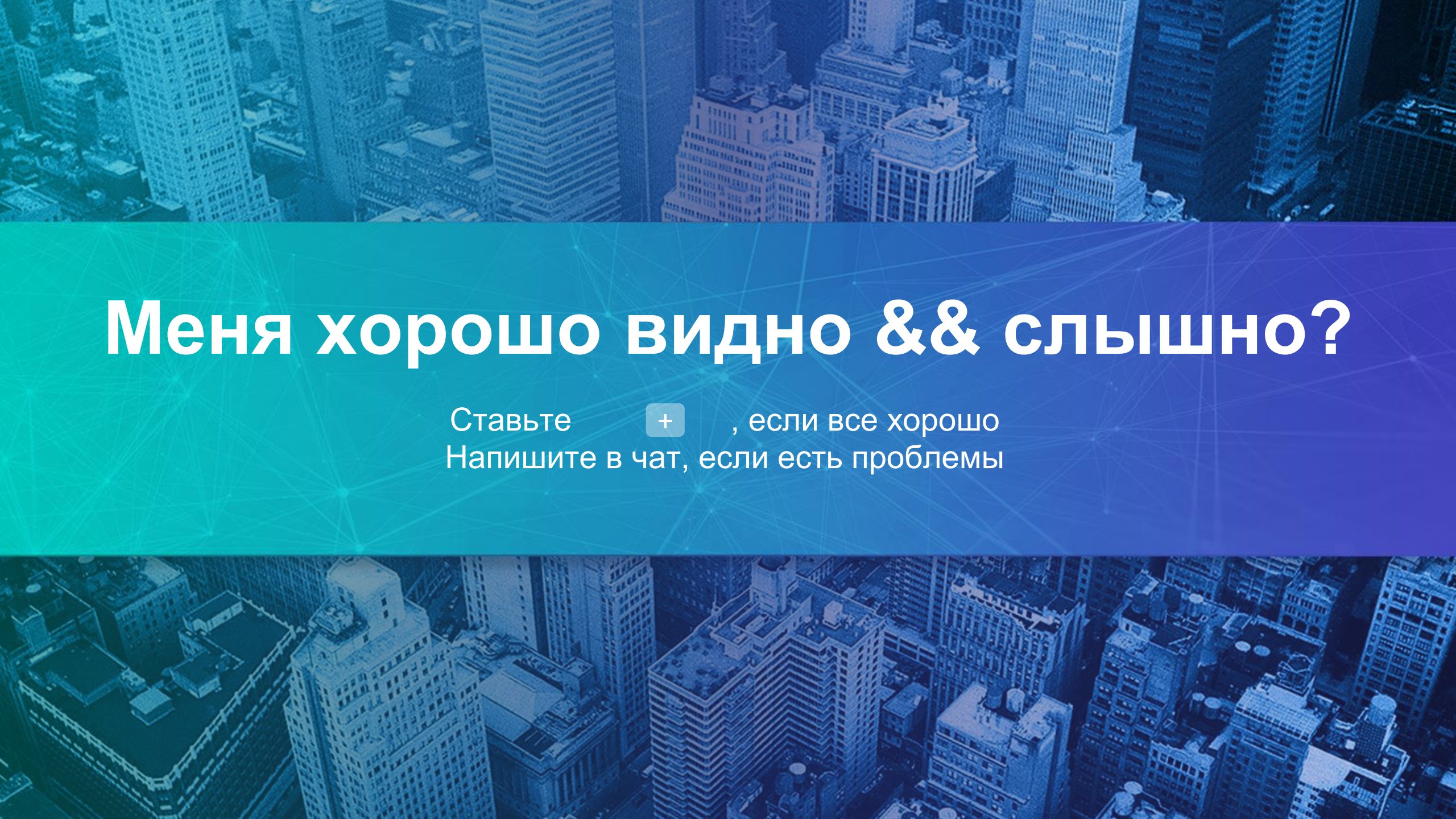
OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Не забыть включить запись!



Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

Тема “Динамический SQL”
Курс “SQL Server Developer”

Коробков Виктор Николаевич
email: korviktor01@gmail.com

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack

Вопросы вижу в чате, могу ответить не сразу

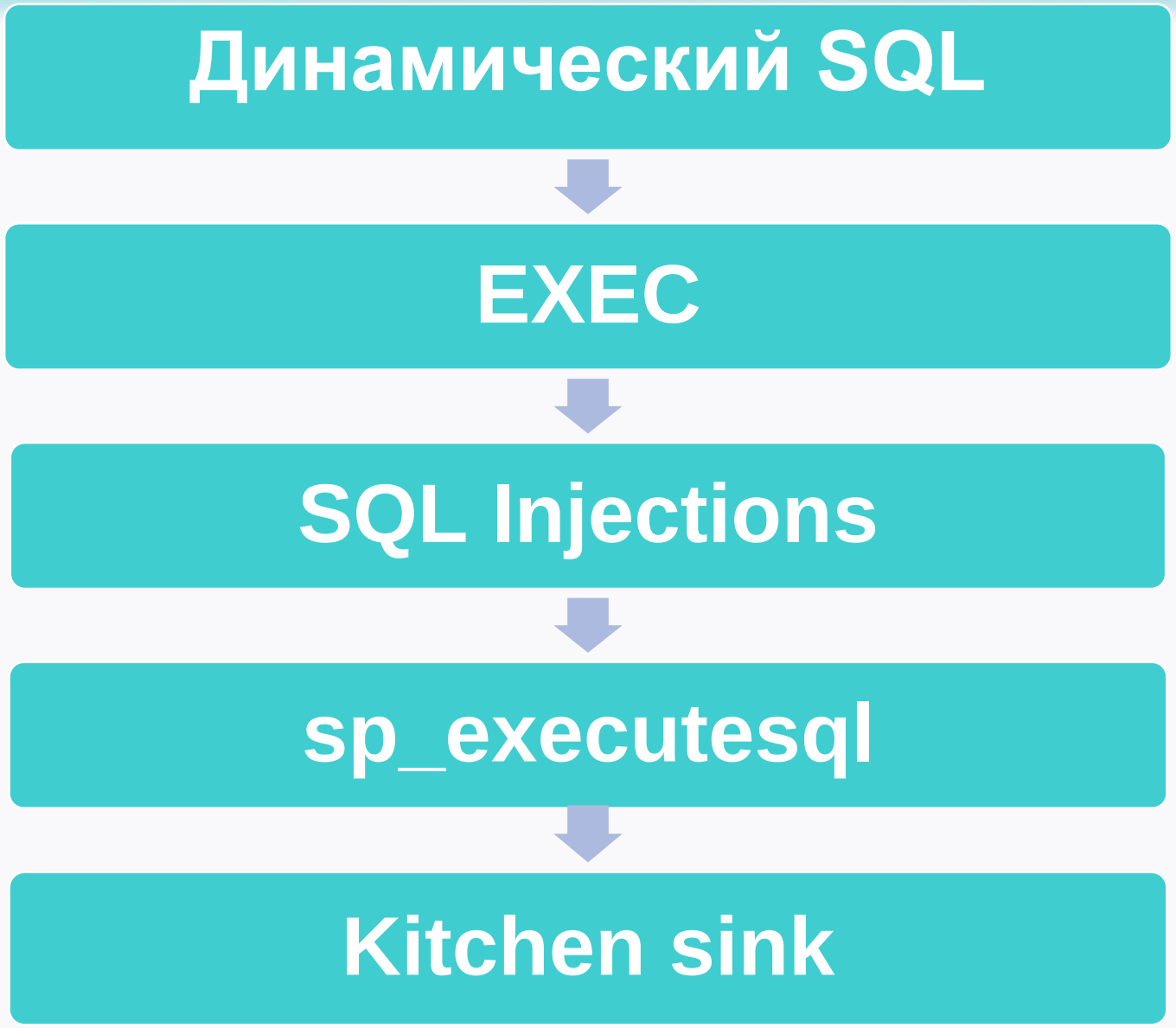
Цели вебинара | После занятия вы сможете

1. Создавать запросы с динамическим SQL
2. Объяснять разницу между exec и sp_executesql
3. Объяснять, что такое Kitchen sink

Смысл | Зачем это уметь

1. Для создания запросов, динамически формируемых в процессе выполнения программы

Маршрут вебинара



Переменные

Объявление переменной:

DECLARE @имя_переменной Тип_данных [= значение];

Инициализация переменной:

SET @имя_переменной = значение;

или

SELECT @имя_переменной = выражение FROM таблица;

Что такое динамический SQL ?

Динамический SQL – это просто текстовая строка, которая после преобразования и подстановки всех значений, исполняется сервером как обычная SQL инструкция операторами exec или sp_executesql.

Зачем нужен динамический SQL

1. Например, нужно сделать выборку из разных таблиц, при этом таблица определяется параметром.
2. В зависимости от условий меняются фильтры в WHERE.
3. Нужны разные поля для вывода.
4. Хотите выполнить SELECT * FROM tbl WHERE x IN (@list)
5. ...

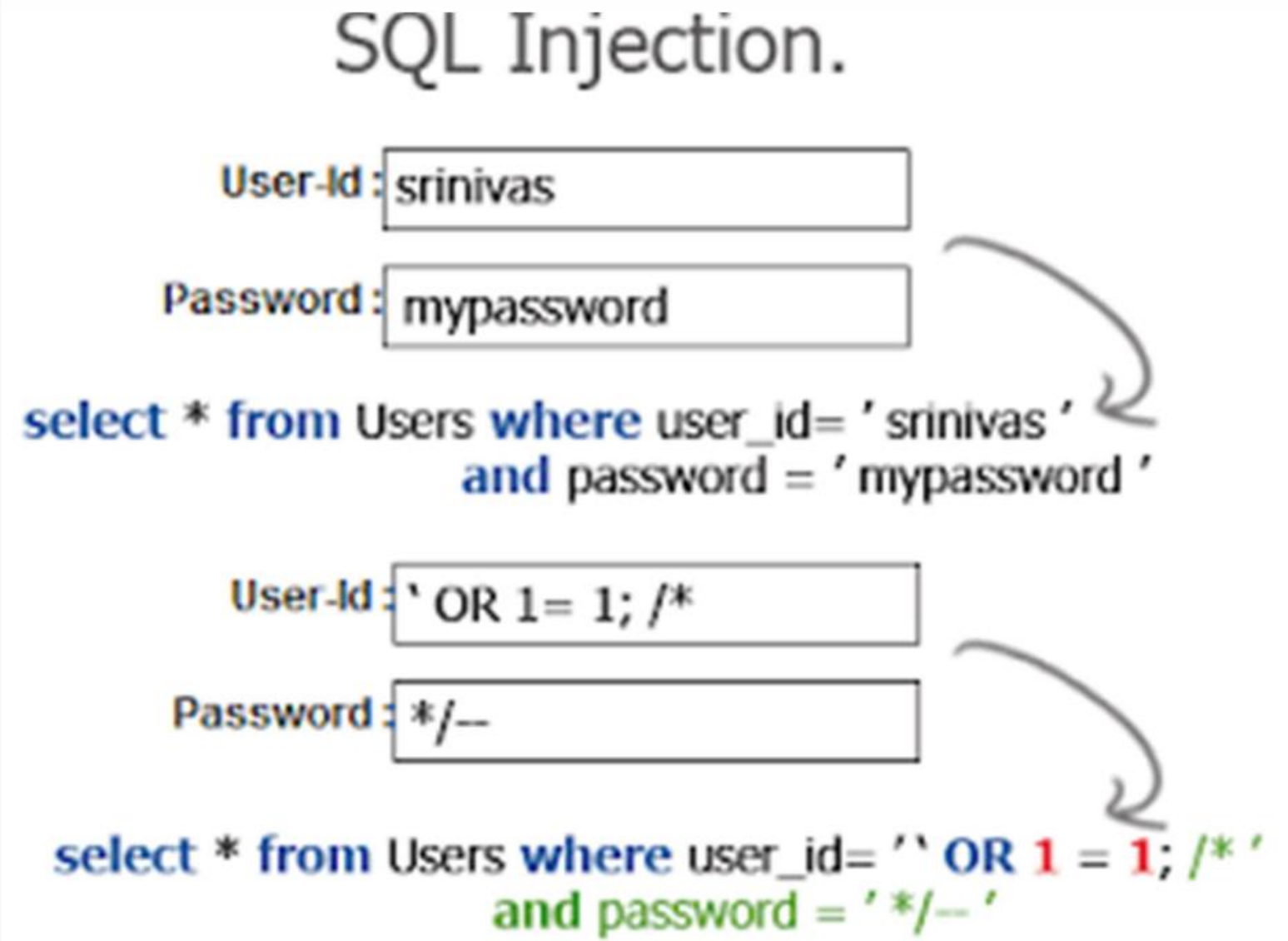
EXECute

Это команда запуска хранимых процедур и SQL инструкций в виде текстовой строки.

Поддерживает в качестве аргумента конкатенацию строк и/или переменных.

https://docs.microsoft.com/ru-ru/sql/t-sql/language-elements/execute-transact-sql?view=sql-server-ver15

Что такое SQL Injections ???



Как избежать SQL Injections ???

1. Не собирайте запрос конкатенируя параметры – ни в БД ни в приложении.
2. Используйте параметры.
3. Ограничивайте права пользователя, который использует приложение.

sp_executesql

Это системная хранимая процедура Microsoft SQL Server, которая выполняет SQL инструкции.

Особенности:

1. НЕ поддерживает в качестве параметров конкатенацию строк.
2. Текст запроса должен быть в формате Unicode NVARCHAR/NCHAR).
3. Имеется возможность передачи параметров в выполняемый скрипт и получение выходных значений.

https://docs.microsoft.com/ru-ru/sql/relational-databases/system-stored-procedures/sp-executesql-transact-sql?view=sql-server-ver15

sp_executesql

Параметры:

1 - текст SQL инструкции;

2 - объявление переменных;

3 - передача значений для переменных.

Kitchen sink

Процедура с кучей параметров (которые могут быть не заданы) для поиска с любыми условиями одним запросом.

Домашнее задание

Динамический PIVOT: по заданию из занятия “Операторы CROSS APPLY, PIVOT, CUBE” требуется написать запрос, который в результате своего выполнения формирует таблицу следующего вида:

	Название клиента
МесяцГод	Количество покупок

Нужно написать запрос, который будет генерировать результаты для всех клиентов.
Имя клиента указывать полностью из CustomerName.
Дата должна иметь формат dd.mm.yyyy например 25.12.2019

Рефлексия

Отметьте 3 пункта, которые вам запомнились с вебинара

1. Динамический SQL: его плюсы и минусы?
2. Какие команды запускают динамический SQL?
3. Как уберечься от SQL Injections?

Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!
Приходите на следующие вебинары

Коробков Виктор Николаевич
email: korviktor01@gmail.com