

# Онлайн образование

otus.ru



Проверить, идет ли запись

**Меня хорошо видно  
&& слышно?**



Тема вебинара

# Динамический SQL



**Коробков Виктор**

Консультант команды технологического обеспечения ООО «ИТ ИКС5 Технологии»

Telegram: @Korobkov\_Viktor



# Правила вебинара



Активно  
участвуем



Off-topic обсуждаем  
в Telegram



Задаем вопрос  
в чат или голосом



Вопросы вижу в чате,  
могу ответить не сразу

## Условные обозначения



Индивидуально



Время, необходимое  
на активность



Пишем в чат



Говорим голосом



Документ



Ответьте себе или  
задайте вопрос

# Маршрут вебинара

Понятие динамического SQL

EXEC

SQL Injections

sp\_executesql

Kitchen sink

Рефлексия

# Цели вебинара

## После занятия вы сможете

1. Создавать запросы с динамическим SQL
2. Объяснять разницу между `exec` и `sp_executesql`
3. Понимать угрозу SQL инъекций
4. Представлять, что такое Kitchen sink



# 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, выполняется 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-ver17>


# Что такое SQL Injections ???

## SQL Injection.

User-Id:

Password:

`select * from Users where user_id= 'srinivas'  
and password = 'mypassword'`



User-Id:

Password:

`select * from Users where user_id= ' OR 1= 1; /*'  
and password = '*/--'`



# 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-ver17>

# 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  
любими  
условиями одним  
запросом



# Домашнее задание

Пишем динамический PIVOT по заданию из занятия "Операторы CROSS APPLY, PIVOT, UNPIVOT".

Требуется написать запрос, который в результате своего выполнения формирует сводку по количеству покупок в разрезе клиентов и месяцев.

В строках должны быть месяцы (дата начала месяца), в столбцах - клиенты.

Нужно написать запрос, который будет генерировать результаты для всех клиентов. Имя клиента указывать полностью из поля CustomerName.



# Рефлексия

# Рефлексия



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**