

Онлайн образование



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



Тема вебинара

Динамический SQL



Дмитрий Тарасов

Разработчик

Об опыте :

С 1995 года опыт работы программистом и администратором различных систем.

Языки программирования:

- Assembler
- C++
- Delphi
- C#

Базы данных:

- MS SQL
- Sybase
- Oracle
- PostgreSQL

Эл. почта: dtarasov@rambler.ru



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

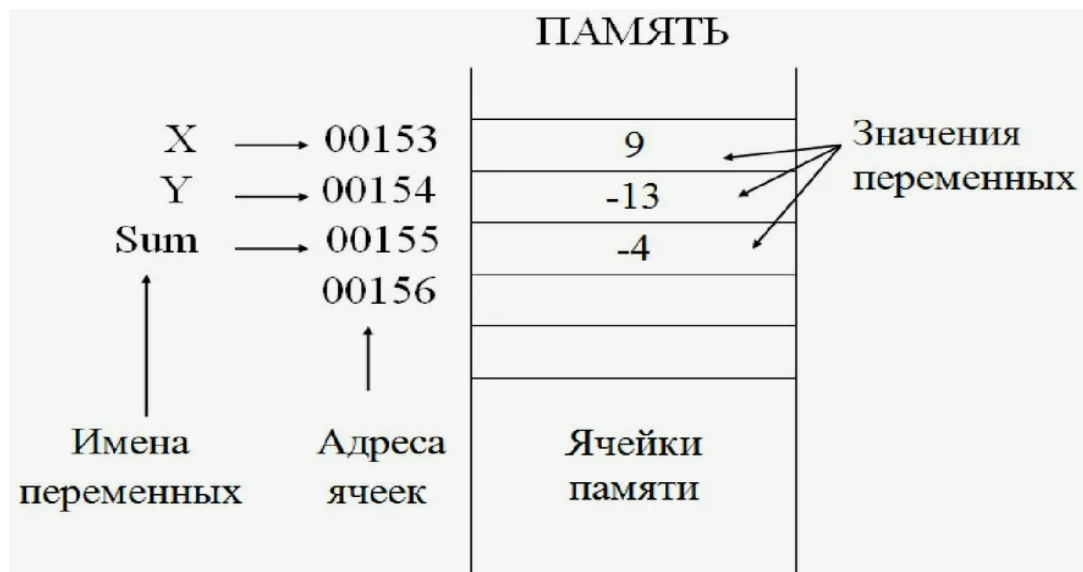


Цели вебинара

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



DECLARE @имя_переменной Тип_данных [= значение];

SET @имя_переменной = значение;

SELECT @имя_переменной = выражение FROM таблица;

Вопросы?



Ставим “+”,
если вопросы есть



Ставим “-”,
если вопросов нет



Динамический SQL

```
declare @str_sql nvarchar(max)
set @str_sql = 'select * from table1'
exec @str_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.

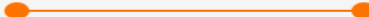
Зачем нужен динамический SQL

Игровые 17 дюймов 15 дюймов Ультрабуки 14 дюймов MacBook Трансформеры Intel i7 Intel i5

Сортировка: сначала недорогие ▾ Группировка: отсутствует ▾

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. ...

Фильтры Очистить

Цена ▾
18 734 — 602 990


Наличие товара ▾
☐ Доступен самовывоз ⁹³¹
☐ Забрать через 5 минут ⁵⁹²
[В конкретном магазине >](#)

Статус товара ▾
☐ Товары по акции ⁷⁶⁴
☐ Доступно в рассрочку ⁷⁴¹
☐ Уцененные товары ⁹

Товары со скидкой ▾
☒ Любой
☐ 5% и больше ²³⁹
☐ 10% и больше ¹¹⁴
☐ 20% и больше ²²

Оценка товара по отзывам ▾
☒ Любой
☐ 4,5 и выше ²⁷⁶
☐ 4 и выше ²⁹⁴
☐ 3,5 и выше ²⁹⁸

EXECute

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

Поддерживает в качестве аргумента конкатенацию строк и/или переменных.

```
declare @str_sql nvarchar(max)
```

```
set @str_sql = 'select * from table1'
```

```
exec @str_sql
```

<https://docs.microsoft.com/ru-ru/sql/t-sql/language-elements/execute-transact-sql?view=sql-server-ver17>

Вопросы?



Ставим “+”,
если вопросы есть

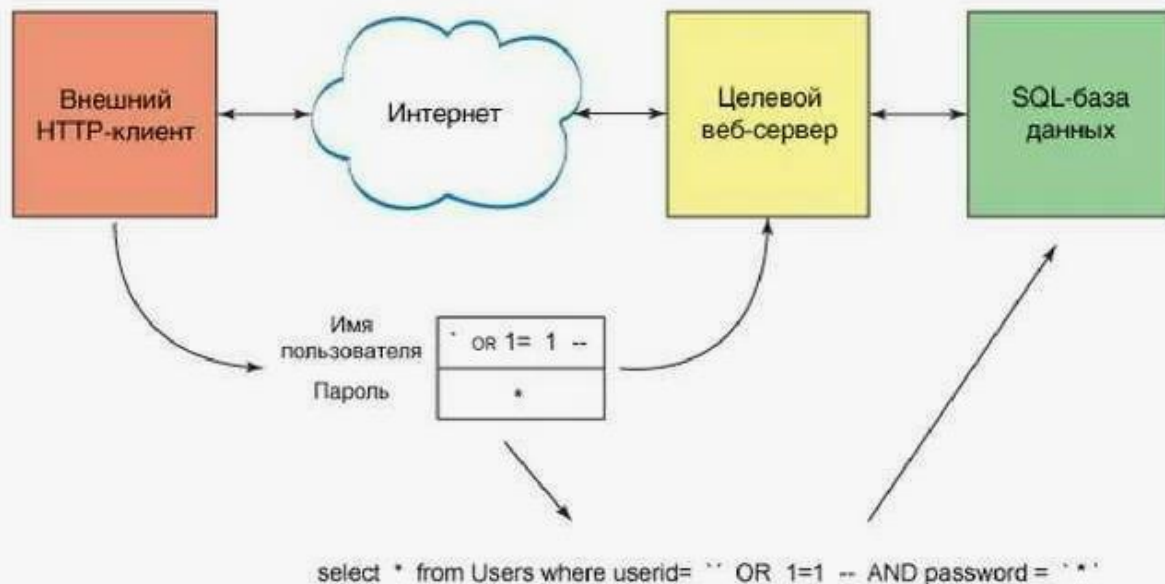


Ставим “—”,
если вопросов нет



SQL инъекция

Внедрение в данные (передаваемые через GET, POST запросы или значения Cookie) произвольного SQL кода.



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.

Вопросы?



Ставим “+”,
если вопросы есть



Ставим “—”,
если вопросов нет



sp_executesql

```
sp_executesql [ @stmt = ] statement  
[  
    { , [ @params = ] N'@parameter_name data_type [ OUT | OUTPUT ][ ,...n ]' }  
    { , [ @param1 = ] 'value1' [ ,...n ] }  
]
```

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>

Вопросы?



Ставим “+”,
если вопросы есть



Ставим “-”,
если вопросов нет



Kitchen sink

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



Вопросы?



Ставим “+”,
если вопросы есть



Ставим “—”,
если вопросов нет

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**