ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

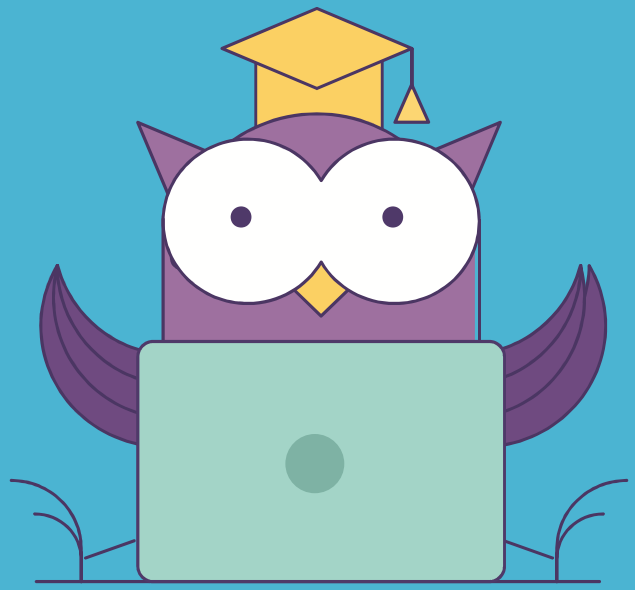
Динамический SQL

Курс «Разработчик MS SQL Server»

Занятие № 12

Кристина Кучерова

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо
Ставьте - если есть проблемы

Цель вебинара

По окончании вебинара вы сможете:

- Воспользуемся переменными и IF..Then..Else
- Писать запросы с динамическим SQL
- Объяснять что такое Ad Hoc запросы
- Объяснить разницу между EXEC и sp_executesql

Маршрут вебинара

IF THEN ELSE

Динамический SQL

Exec

Sp_executesql

Выводы

Что было на прошлом занятии?

OTUS

- Как храняться xml, json
- Зачем xml хранить тип xml, почему не просто varchar?
- Как результаты запроса преобразовать в xml, json?
- Как выбрать отдельные поля, элементы из json, xml?

Объявление переменной DECLARE

- @Имя переменной
- Назначение типа данных
- Присваивание значения NULL

Присваивание значений

```
DECLARE @var = 1
```

```
SET @var = 1
```

```
SELECT @var = 1
```

IF .. THEN .. ELSE

IF условие

    То что выполнится, если условие True

ELSE

    То что выполнится если условие FALSE

Зачему нужен динамический SQL?

OTUS

1. Вам нужно сделать выборку из разных таблиц, 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)

Как выглядит Динамический SQL?

На самом деле это просто строка.

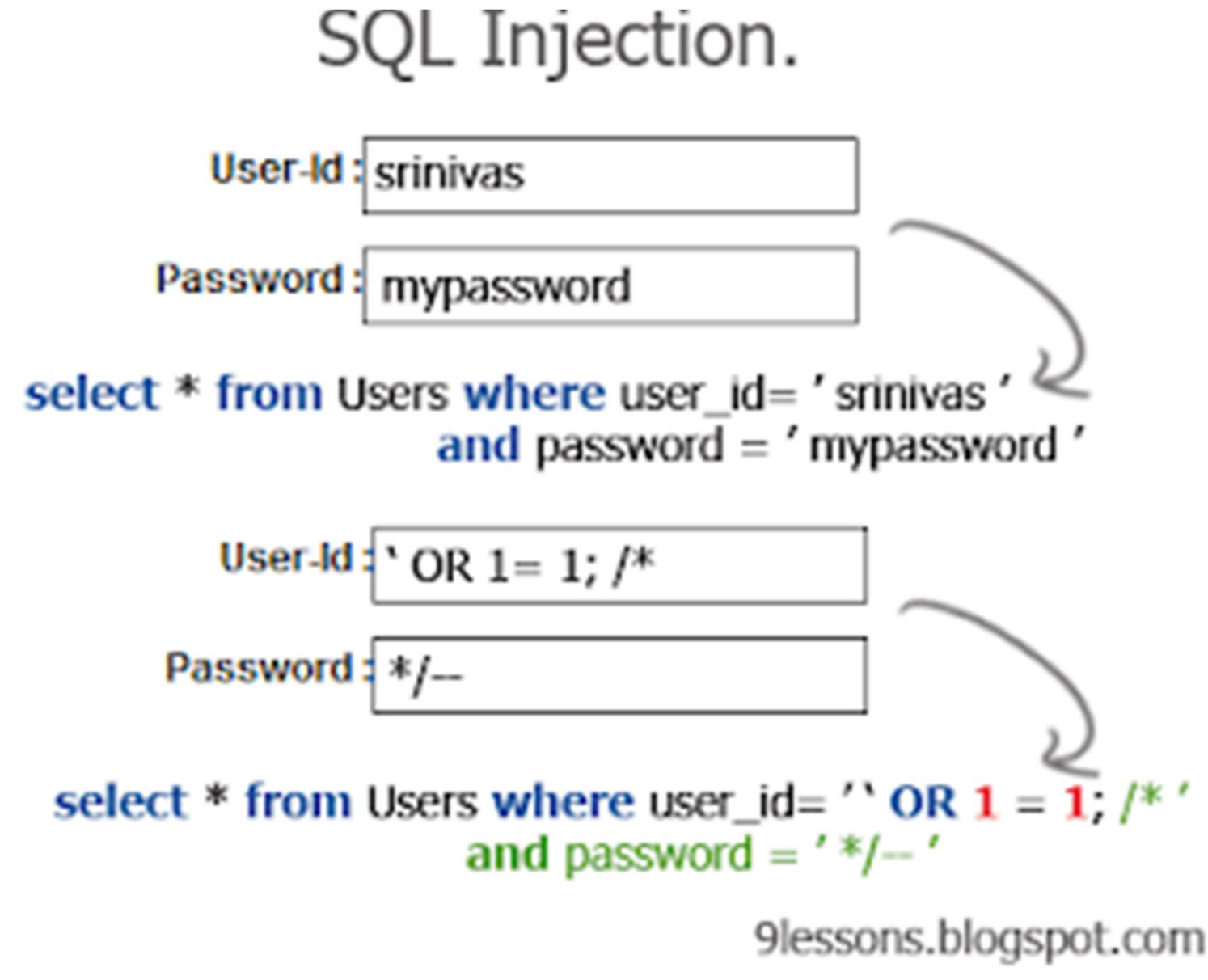
Просто SQL внутри строки

Exec

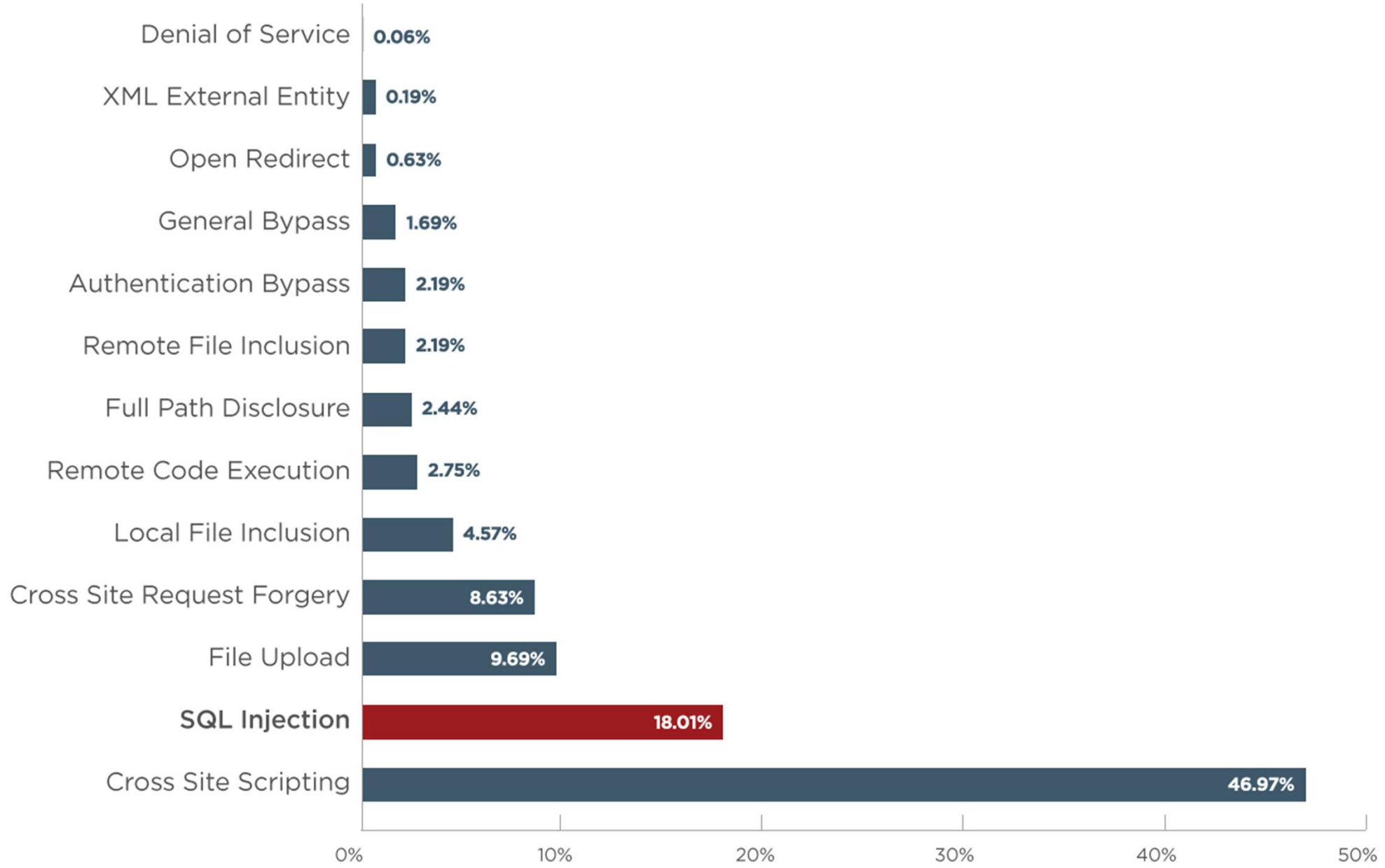
Или

Sp_executesql

Включение SQL кода в текстовые поля формы и получение информации о БД



Vulnerabilities by Type



Wordfence™

wordfence.com/learn

Защита от SQL Injections

OTUS

- Не собирайте запрос конкатенируя параметры – ни в БД ни в приложении.
- Используйте параметры
- Ограничивайте права пользователя, которого использует приложение

Kitchen sink процедуры

OTUS

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

Merge join

OTUS

Используется, когда оба набора имеют индекс

Может использовать tempdb если в первом наборе много дубликатов

Лучший вариант для больших наборов данных

Рефлексия

О чем мы говорили сегодня?

- Что такое динамический SQL?
- В чем его минусы и плюсы?
- Какие 2 оператора есть для динамического SQL?
- Как уберечься от SQL injections?

Рефлексия

Напишите, пожалуйста, свое впечатление о вебинаре.

- Отметьте 3 пункта, которые вам запомнились с вебинара.
- Что вы будете применять в работе из сегодняшнего вебинара?

Заполните, пожалуйста, опрос в ЛК о занятии

Спасибо
за внимание!
До встречи в Slack и на вебинаре