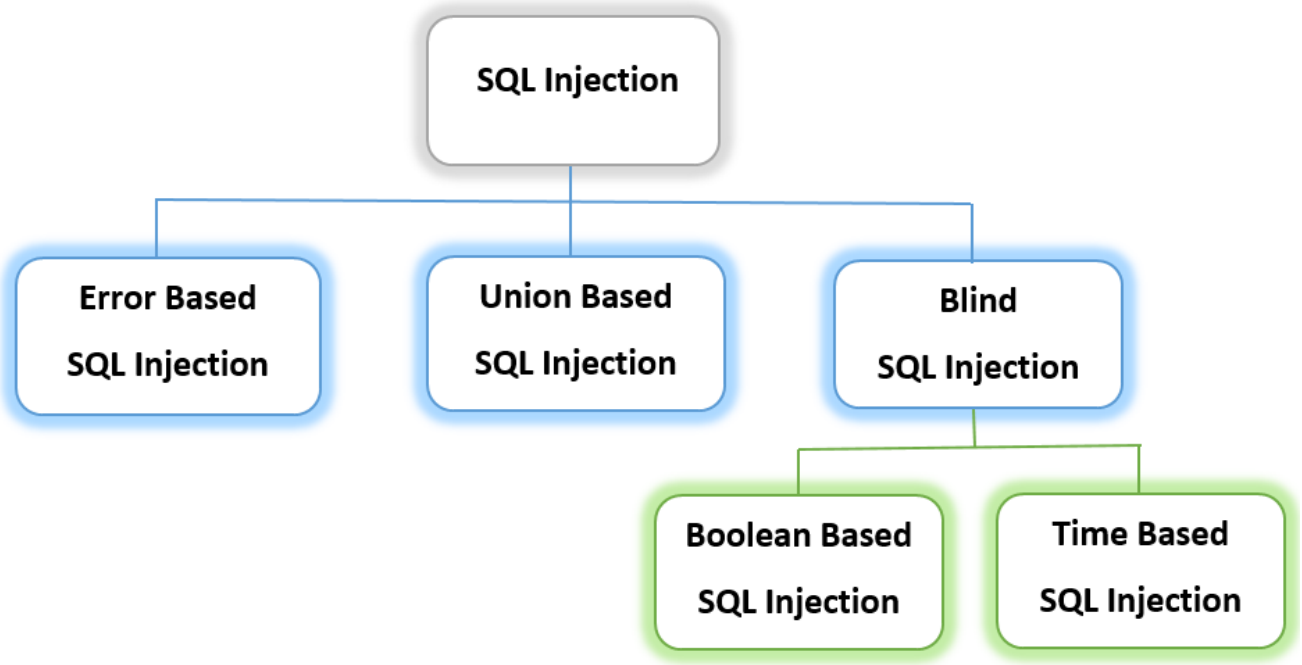
Типы SQL-инъекций (SQLi)

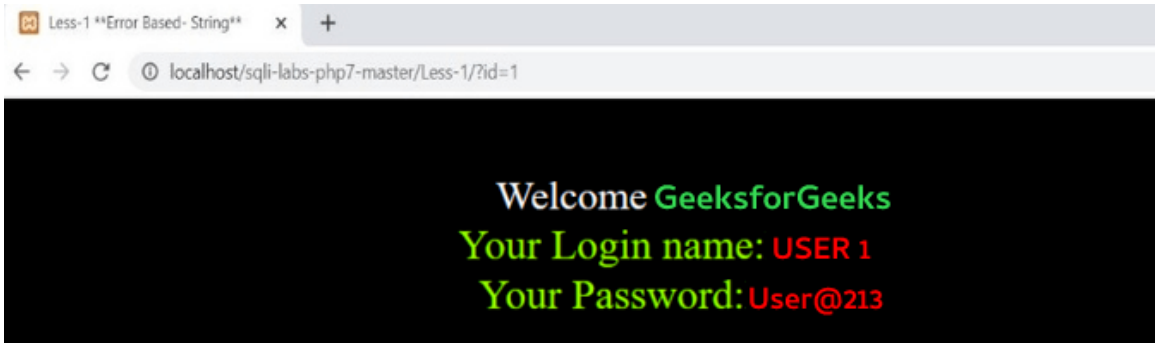
V вишалкумар98765432

SQL-инъекция - это атака, в которой используется вредоносный SQL-код для манипулирования внутренними базами данных с целью получения информации, которая не предназначалась для показа. Данные могут включать конфиденциальные корпоративные данные, списки пользователей или конфиденциальные данные потребителя. В этой статье приведены типы SQL-инъекций с их примерами. SQL Injections-LABS (платформа для изучения SQL-инъекций), демонстрирующая, как вы можете выполнять каждый тип SQL-инъекций.

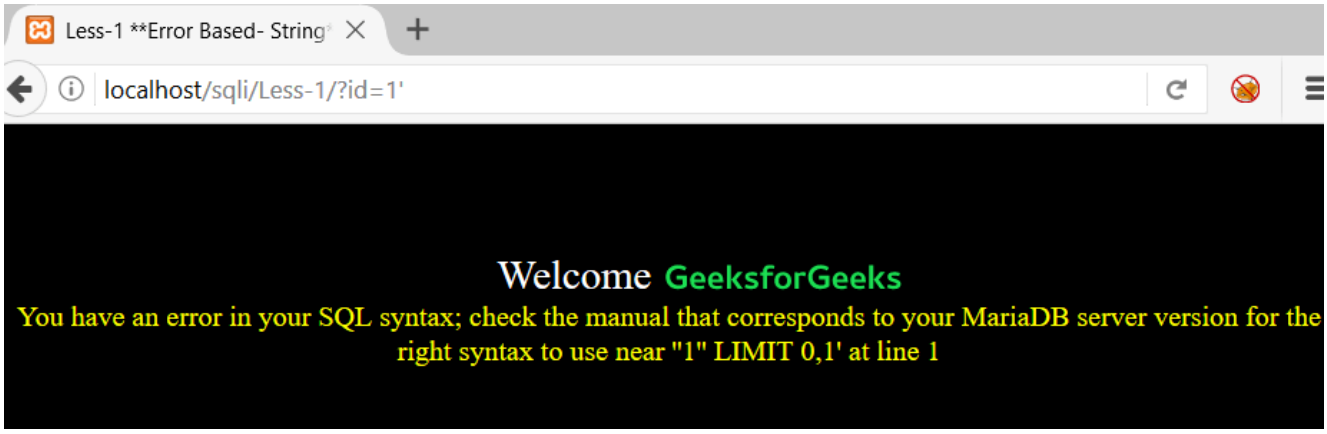


1. SQL-инъекции на основе ошибок:

SQL-инъекции на основе ошибок получают информацию о структуре базы данных из сообщений об ошибках, выдаваемых сервером базы данных. В редких случаях злоумышленник может перечислить всю базу данных, используя только SQL-инъекцию на



Но если мы введем **?id=1'**, это выдаст ошибку.



Теперь эта ошибка поможет нам определить местонахождение внутреннего запроса.

Если мы удалим первую и последнюю кавычки из **"1" LIMIT 0,1'**, то она станет **'1" LIMIT 0,1**.

1' - это наши входные данные, и одинарная кавычка после этого ввода указывает, что наши входные данные заключены в одинарные кавычки. Это означает, что запрос, который был выполнен обратно в базе данных, был следующим:

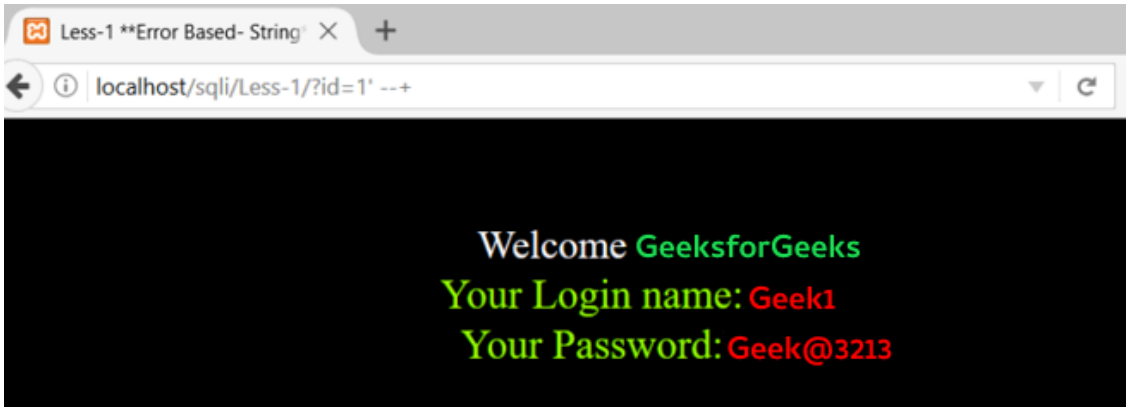
что синтаксически неверно. Теперь мы исправим этот запрос, указав входные данные **?id=1' –+**.

–+ закомментирует все, что последует за этим. Итак, наш внутренний запрос будет:

Запрос:

```
select * from table_name where id='1' --+'
```

и снова мы получаем имя пользователя и пароль.



Теперь мы можем вставить запрос между **цитатой** и **-+** для извлечения данных из базы данных.

2. SQL-инъекции на основе объединения:

SQL-инъекции на основе объединения используют оператор UNION SQL для объединения результатов двух или более запросов SELECT в единый результат, который впоследствии возвращается как часть HTTP-ответа.

Запрос:

```
SELECT EMP_ID, EMP_DOJ FROM EMP
UNION SELECT dept_ID, dept_Name FROM dept;
```

Этот SQL-запрос выдаст единый результирующий набор из двух столбцов, включающий значения из столбцов EMP EMP_ID и EMP_DOJ, а также столбцов dept dept_ID и dept_Name.

Для функционирования запроса ОБЪЕДИНЕНИЯ должны быть выполнены две важные потребности:

- Каждый запрос должен возвращать одинаковое количество столбцов.
- Типы данных должны быть одинаковыми, т.Е. они не изменяются после выполнения