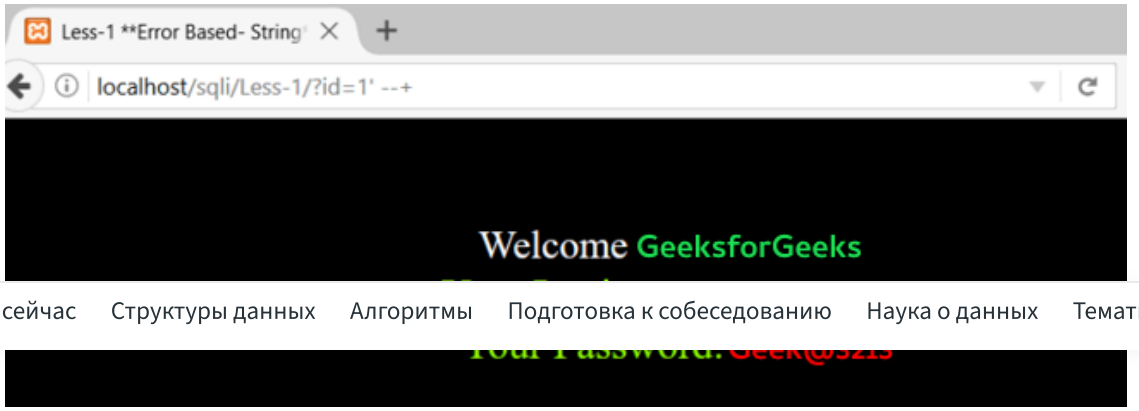
что синтаксически неверно. Теперь мы исправим этот запрос, указав входные данные **?id=1' –+**.

–+ 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

индекс столбца до тех пор, пока не будет обнаружена ошибка.

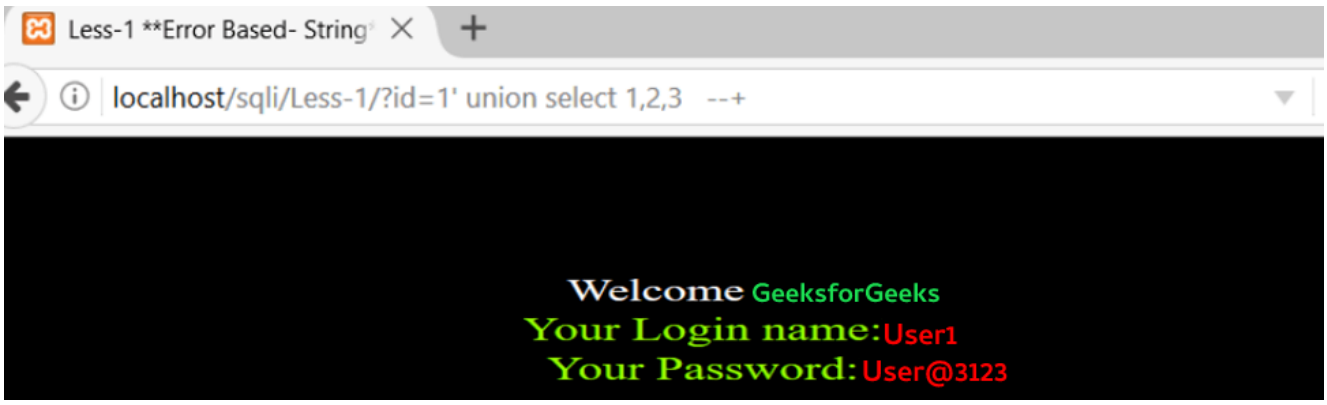
```
?id=1' order by 1 --+      no error
?id=1' order by 2 --+      no error
?id=1' order by 3 --+      no error
?id=1' order by 4 --+      we get error
```

Это демонстрирует, что в запросе отсутствует четвертый столбец. Итак, теперь мы знаем, что запрос в серверной части содержит три столбца.

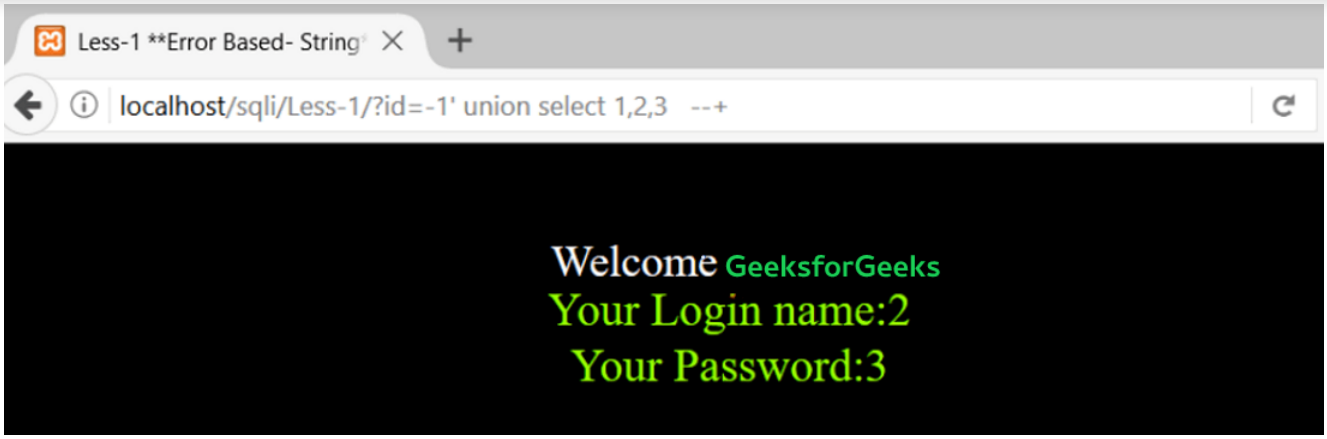
Теперь мы будем использовать оператор UNION, чтобы объединить два запроса и иметь возможность обнаруживать уязвимые столбцы.

Запрос:

```
id=1‘ UNION SELECT 1,2,3 --+
```



Проблемы нет, но мы получаем результирующий набор первого запроса; чтобы получить результат второго запроса select на экране, мы должны сделать результирующий набор первого запроса ПУСТЫМ. Это может быть достигнуто путем предоставления идентификатора, который не существует (отрицательный идентификатор).

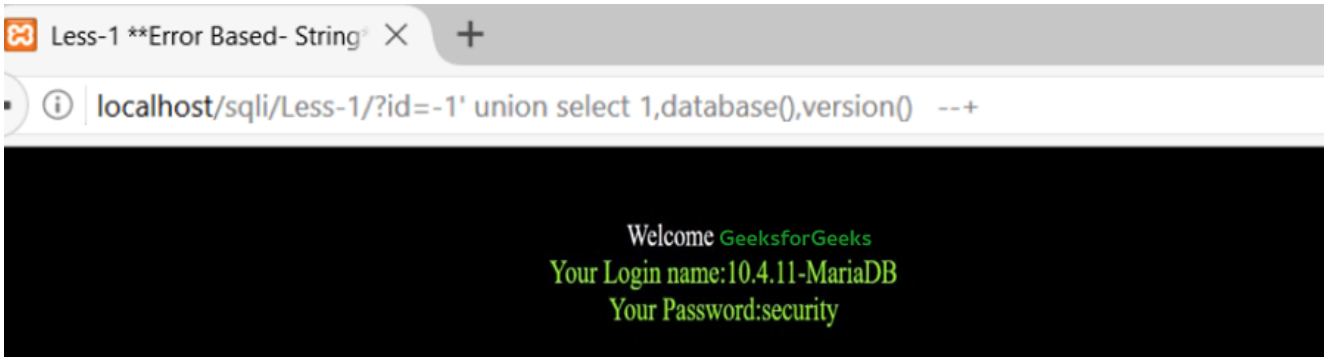


Это демонстрирует, что мы получаем значения из столбцов 2 и 3 в качестве выходных данных. В результате мы можем использовать эти два столбца для извлечения информации о базе данных и из нее.

Запрос:

```
?id=-1‘ UNION SELECT 1,version(),database() --+
```

Это предоставит базу данных, которую мы используем в данный момент, а также текущую версию базы данных, используемой в серверной части.



3. Слепые SQL-инъекции на основе логических значений:

SQL-инъекция на основе логических значений работает путем отправки SQL запроса в базу данных и принуждения приложения выдавать различный ответ в зависимости от того, возвращает запрос TRUE или FALSE.

Пример:

В лабораториях SQL-инъекций, если мы введем **?id=1** в URL браузера, запрос, который