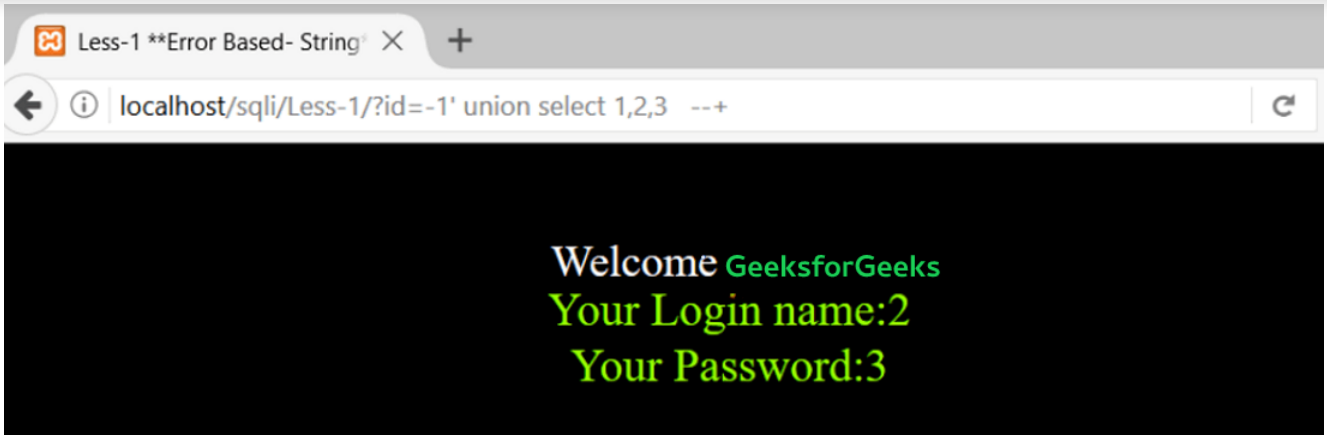
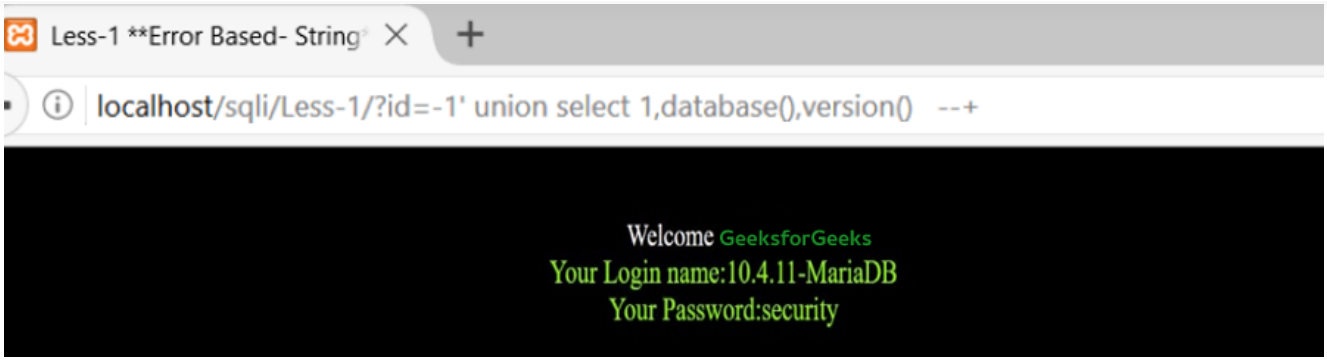


Это демонстрирует, что мы получаем значения из столбцов 2 и 3 в качестве выходных данных. В результате мы можем использовать эти два столбца для извлечения информации о базе данных и из нее.

Запрос:

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

Это предоставит базу данных, которую мы используем в данный момент, а также текущую



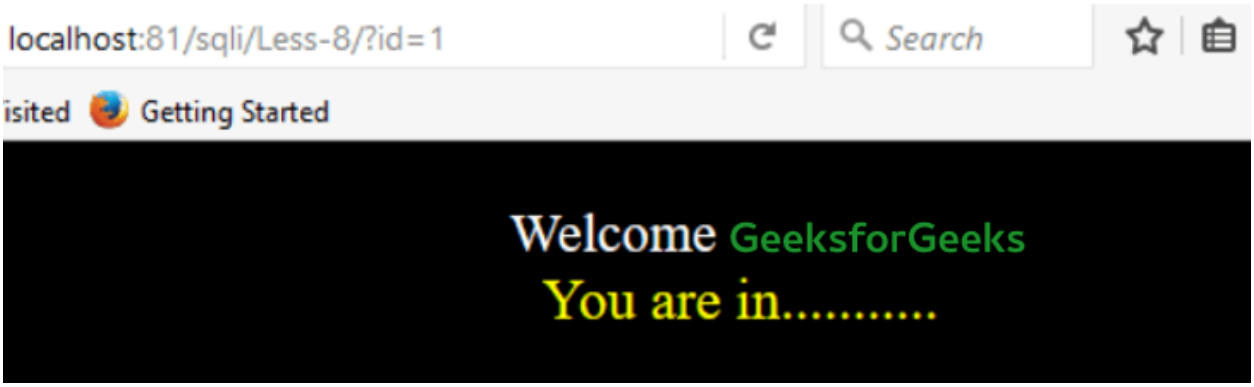
3. Слепые SQL-инъекции на основе логических значений:

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.

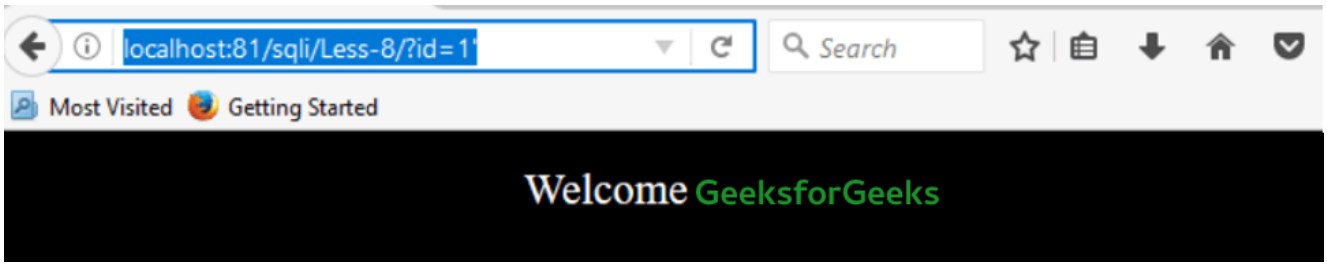
Пример:

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

На веб-странице желтым шрифтом будет выведено “вы находитесь в”, как показано на рисунке.



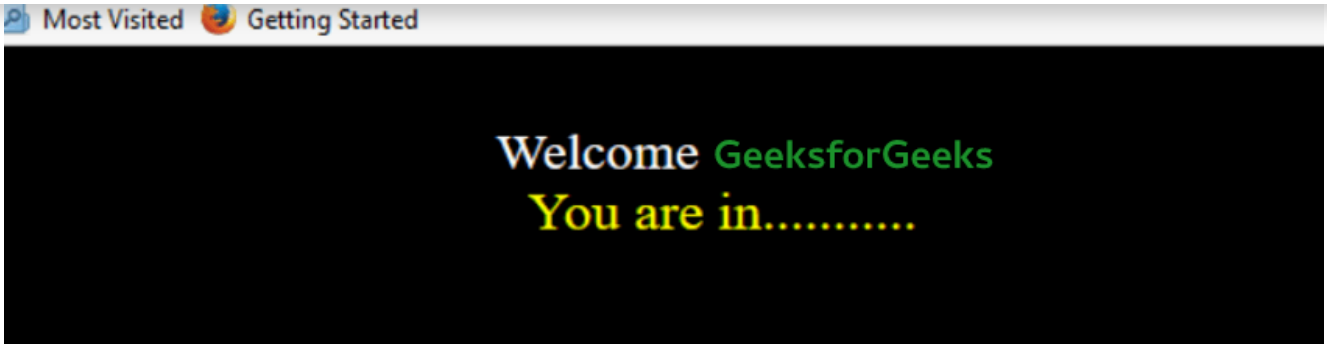
Когда злоумышленник пытается использовать **запятую (‘) ?id=1’**, чтобы прервать этот запрос, он не сможет найти уведомление об ошибке, используя также какой-либо другой метод. Более того, если злоумышленник попытается ввести неверный запрос, как показано на рисунке, желтый текст исчезнет.



Затем злоумышленник использует слепую SQL-инъекцию, чтобы убедиться, что запрос на внедрение возвращает результат true или false.

```
?id=1' AND 1=1 --+
```

Теперь база данных проверяет, равно ли 1 для заданного условия. Если запрос является допустимым, он возвращает значение TRUE; как видно на скриншоте, у нас есть текст желтого цвета “вы находитесь в”, указывающий, что наш запрос действителен.

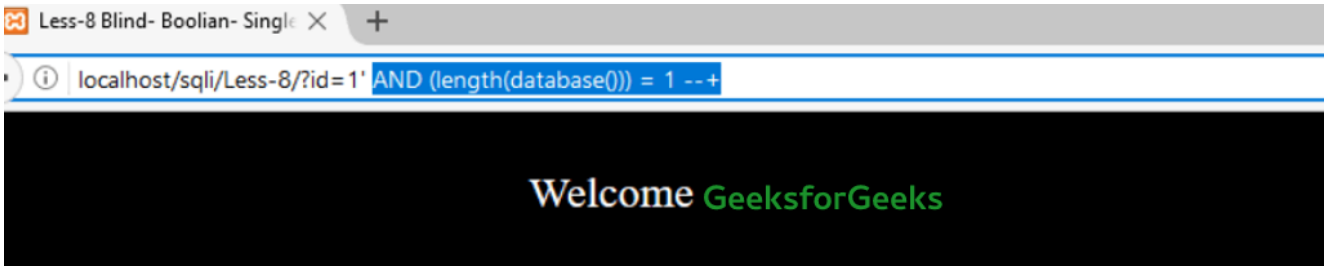


В результате это подтверждает, что веб-приложение уязвимо для слепой SQL-инъекции. Мы получим информацию базы данных, используя условия true и false.

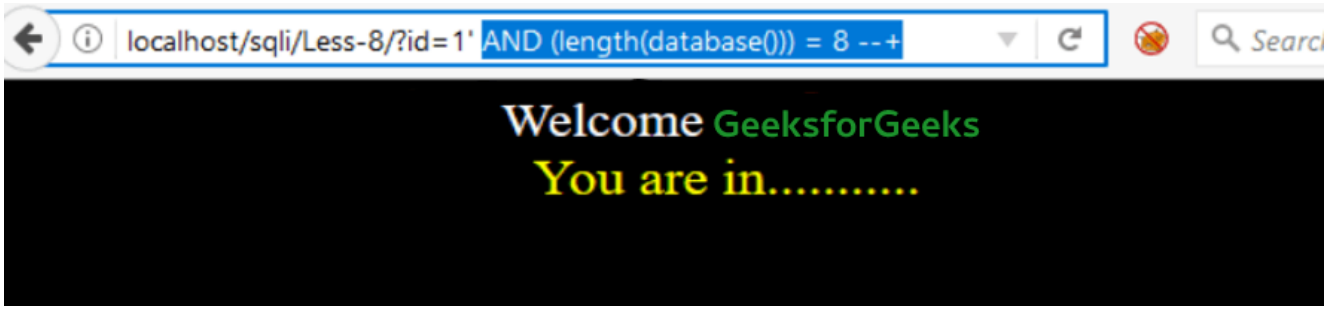
Теперь мы введем следующий запрос, который задаст вопрос, равна ли длина строки базы данных 1, и он ответит возвращением TRUE или FALSE через текст “вы находитесь внутри”.

```
?id=1' AND (length(database())) = 1 --+
```

Как вы можете видеть на изображении, текст снова исчезает, указывая, что он вернул FALSE для ответа "НЕТ", длина строки базы данных не равна 1.



Когда мы проверяем длину строки, равную 8, возвращается yes, и снова отображается желтый текст “вы находитесь в”.



4. Слепые SQL-инъекции на основе времени:

В зависимости от результата ответ HTTP будет либо отложен, либо возвращен немедленно. Даже если данные из базы данных не возвращаются, злоумышленник может определить, возвращала ли используемая полезная нагрузка значение true или false. Поскольку злоумышленник должен перечислять базу данных посимвольно, эта атака часто протекает медленно (особенно на больших базах данных).

```
And SLEEP(10) if sleep then Vulnerable
OR SLEEP(10) if sleep then vulnerable
```

Последнее обновление : 08 августа 2022 г.

Похожие чтения


Как защититься от атак SQL-инъекций?


Что такое атаки с объединением SQL-инъекций?

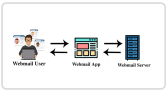

Разница между XSS и SQL-инъекцией

Шпаргалка по SQL-инъекциям


Каковы недостатки внедрения?

Что такое CSV-инъекция?

Как выполняется атака с использованием строки подключения?


Что такое внедрение заголовка SMTP?


Внедрение XPath


Внедрение SMTP

Предыдущая страница Далее

Статья, подготовленная :

V

вишалкумар98765432

вишалкумар98765432

Подписаться

Голосуйте за сложность