Гр. 522403 Яцкевич Фёдор

Отчет на тему

**Тестирование на SQL инъекции**

Суть SQL инъекции состоит в том, что при изменении параметра SQL запроса на определенный текст, представляющий собой часть SQL запроса, результат выполнения запроса изменится.

Пример SQL инъекции:

Есть запрос поиска пользователя из базы по ID, принимающий ID в качестве параметра:

SELECT \*

FROM users

WHERE

Id = ‘?’;

Ожидается, что параметр является целым числом. Но что если вместо этого параметр будет следующая строка?

1‘; DELETE FROM users;

В таком случае итоговый запрос будет следующий:

SELECT \*

FROM users

WHERE

Id = ‘1‘; DELETE FROM users;’;

Вместо одного запроса было выполнено два. В лучшем результатом данного запроса будет ошибка. В худшем – сотрутся все данные из таблицы users.

Суть использования SQL инъекций состоит в том, что пользователь, пользующийся веб сервисом, взаимодействующим с базой данных, может изменить параметр http запроса или данные cookie, с определенной целью. Например, удаление данных веб сервиса, получение данных, недоступных простому пользователю.

Тестировать сервис на SQL инъекции не имеет смысла на стороне клиента, т.к. хакер может вручную заполнить параметр запроса или данные cookie SQL инъекцией (через консоль браузера).

Таким образом приходим к тому что сервис необходимо тестировать с момента прихода запроса на сервер, т.к. тестовые данные нужно занести в параметр запроса.