Лабораторная №3

SQL injection

Цель работы:

Получить представление об SQL инъекциях.

Задача 1.

Разработать веб-приложение, содержащее одну страницу с полями ввода логина и пароля, а также кнопкой их отправки. Сервер должен хранить в некоторой базе данных (например, SQLite) таблицу с тремя колонками: логинами, пароль и секрет пользователя (например, число). При вводе корректного логина и пароля сервер должен вернуть на страницу секрет.

Login	Password	Secret
root	VLS*jsvds09dv	875423
user1	Bjkay8A(jl	698346
user2	Nsvpo97px11#	927492
…	…	…

Необходимо продемонстрировать эксплуатацию SQL-инъекции в одном из полей ввода. Результатом инъекции должен быть вывод всех секретов из таблицы. Для того, чтобы инъекция могла быть осуществлена, необходимо формировать строку запроса вручную, например:

```
symbol = 'RHAT'
c.execute("SELECT * FROM stocks WHERE symbol = '%s'" % symbol)
```

Также необходимо продемонстрировать безопасное выполнение запроса, не подверженное инъекции (для этого можно сделать отдельную кнопку). Безопасный запрос должен производиться при помощи параметризованного запроса, например:

```
t = ('RHAT',)
c.execute('SELECT * FROM stocks WHERE symbol=?', t)
print c.fetchone()
```