МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»  
Институт радиоэлектроники и информационных технологий (ИРИТ-РТФ)

**ОБНАРУЖЕНИЕ И ИСПРАВЛЕНИЕ SQL INJECTION  
  
Отчет по лабораторной работе**по дисциплине «Разработка безопасных веб-приложений»

Преподаватель Мирвода С.Г.

Студенты Кетель В.В.

Пестов М.А.

дата подпись

Группа РИ – 571227

Код и наименование направления подготовки (специальности):   
10.05.02 Информационная безопасность телекоммуникационных систем

Екатеринбург 2021

1. **Войти на сайт и увидеть список книг и авторов**

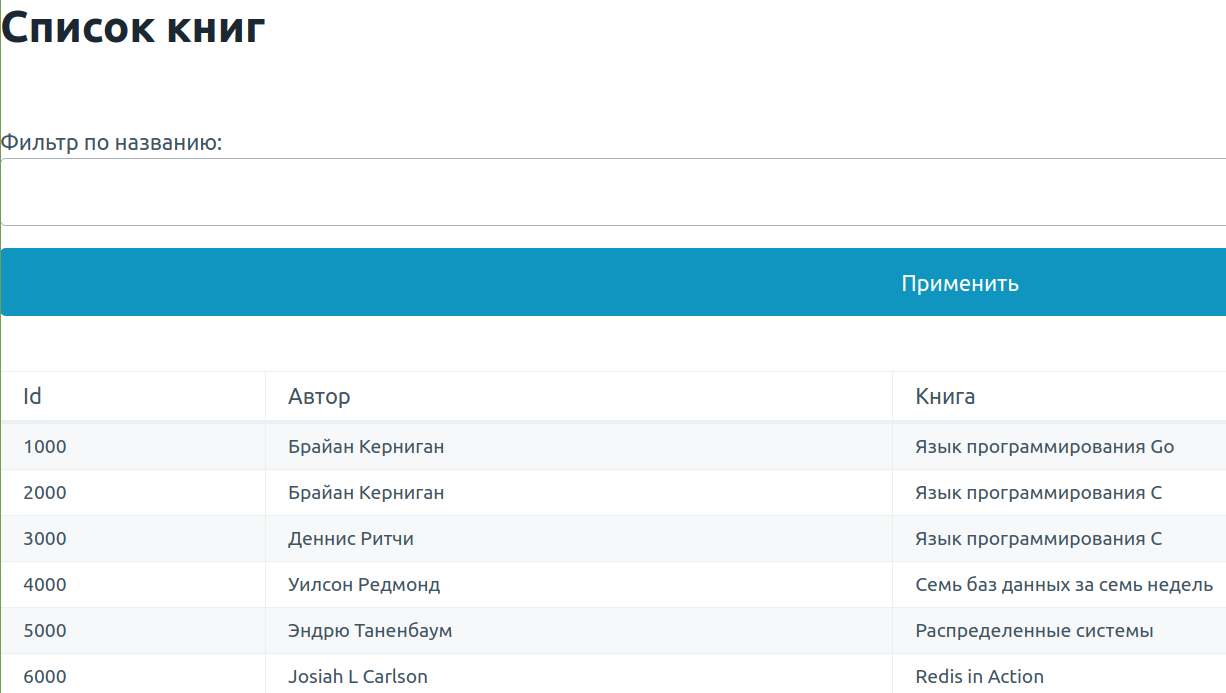


Рисунок 1 – Список книг, доступный после авторизации. Авторизация выполнена под пользователем «admin», пароль «12345»

1. **Обнаружить SQL инъекцию**

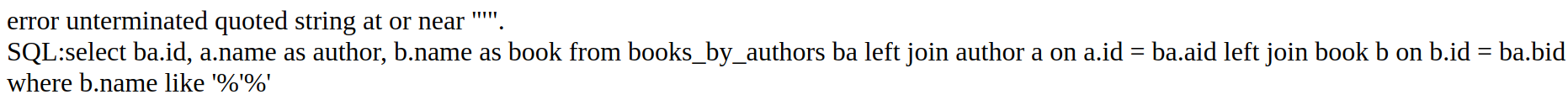


Рисунок 2 – Ввод одинарной кавычки приводит к ошибке синтаксиса SQL запроса в БД. При этом в выводе ошибки можем наблюдать структуру запроса

1. **Обход установленного фильтра, Получение данных из другой таблицы, Похищение пароля пользователя**

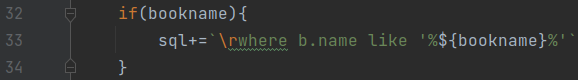


Рисунок 3 – Уязвимость находится в данном месте. Фильтр можно легко обойти, указав при вводе, например, «Язык%'--».

Воспользуемся этой уязвимостью для получения данных из другой таблицы с целью похищения пароля пользователя. Для этого введем в поле фильтра книг:

' union all select ba.id, users.name, users.pass from users, books\_by\_authors ba where ba.id = 1000--

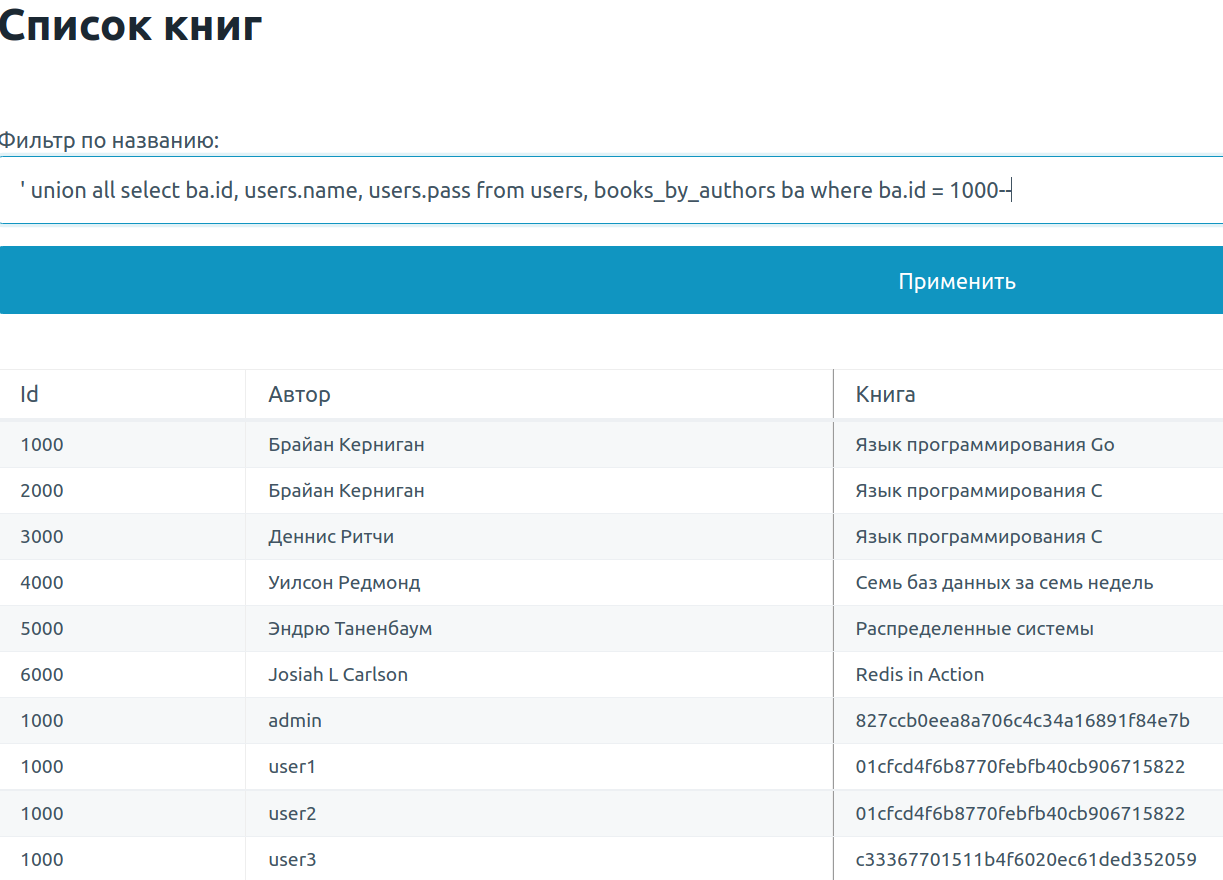


Рисунок 4 – Успешное обращение к посторонней таблице users с целью кражи паролей пользователей. Таким образом, были скомпрометированы пароли пользователей admin и user1-3

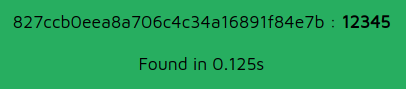


Рисунок 5 – Выполнено декодирование хеша md5 → искомый пароль от пользователя admin - 12345

1. **Исправление уязвимости**

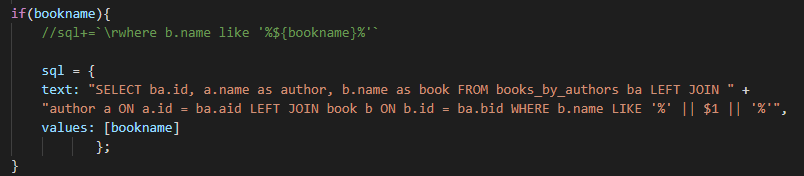


Рисунок 6 – Уязвимость исправлена. Сверху закомментировано — уязвимое место, а снизу заменено на исправленный вариант

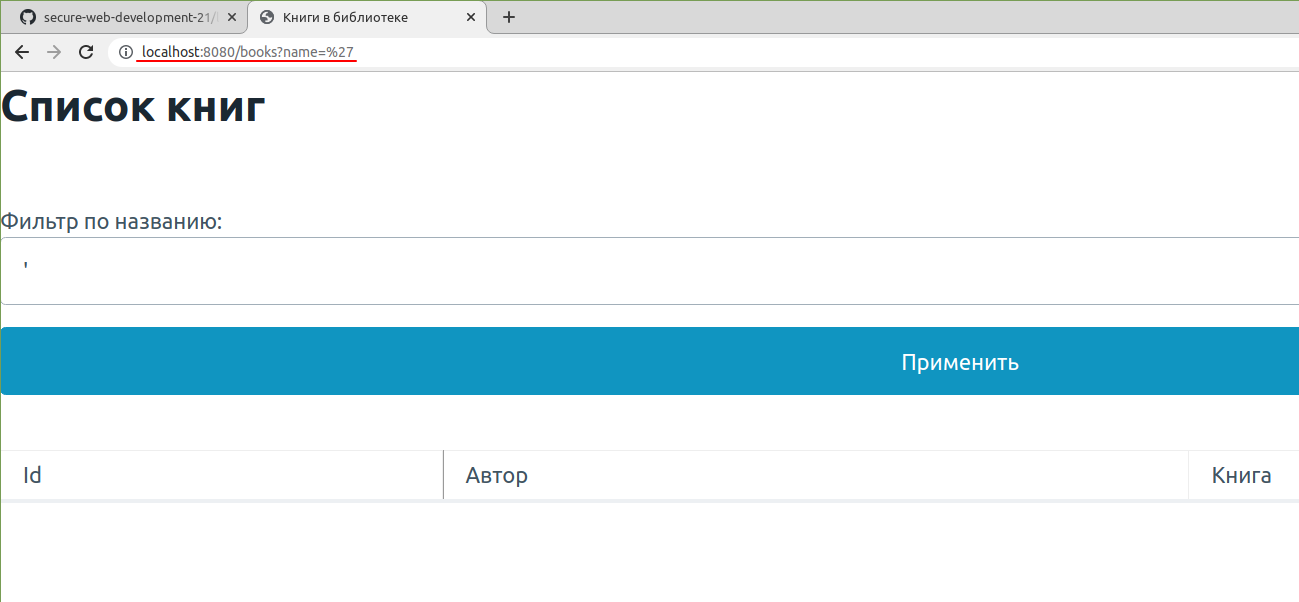


Рисунок 7 – При внесенный исправлениях ввод кавычки в поле не нарушает структуру запроса SQL

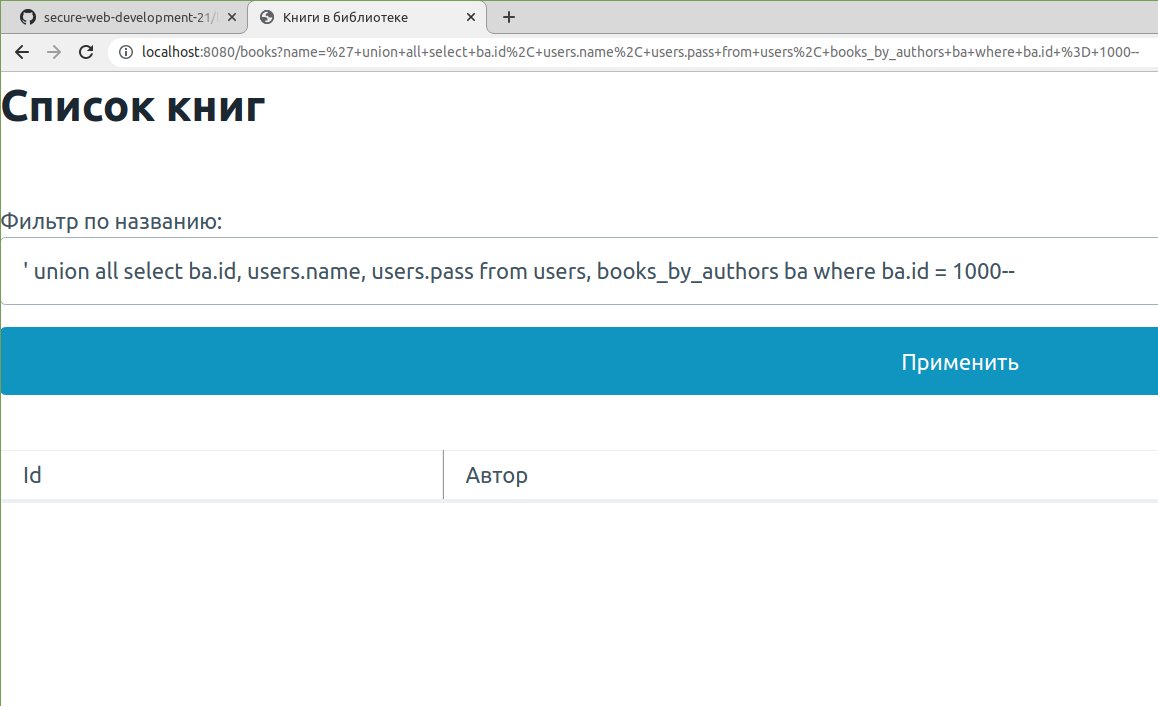


Рисунок 8 – Ранее используемый запрос на компрометацию паролей пользователей не работает. Уязвимость SQL Injection успешно исправлена