Выполнил: Пархомов А.С., АИ-17

Тема: Безопасность

Ход работы

Для выполнения поставленного задания был создан небольшой двухстраничный проект.

Первая страница – форма поиска закона по его номеру или профильному комитету:

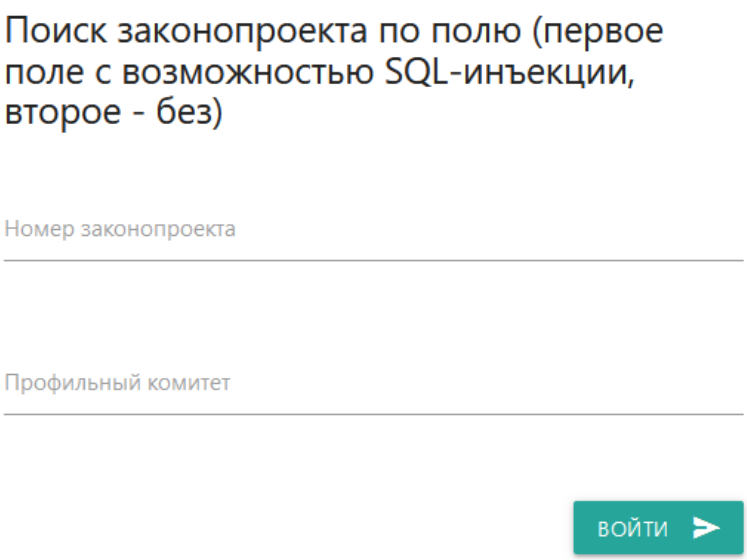

Рисунок 1 – Форма поиска закона

Вторая страница – результат поиска:

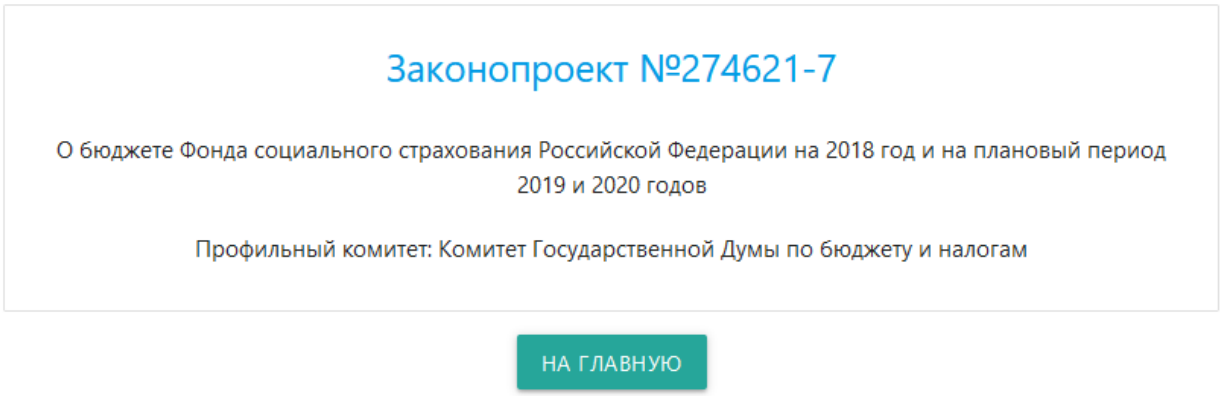

Рисунок 2 – Результат поиска

Для изучения и проведения SQL-инъекций были выбраны два драйвера базы данных PostgreSQL – PgConnect и PDO. При поиске закона по его номеру используется PgConnect, а при поиске по профильному комитету – PDO.

В случае отправки пустой или полностью заполненной формы будут выведены следующие ошибки:

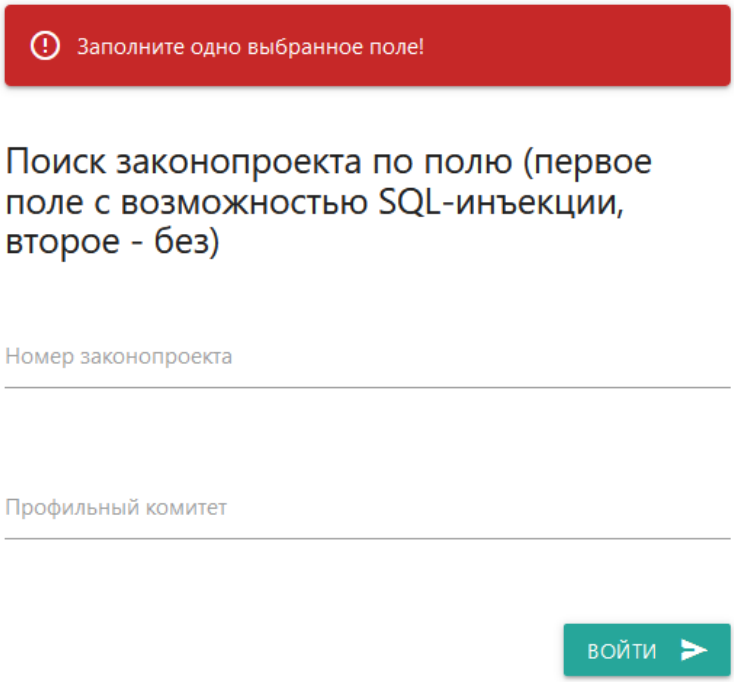

Рисунок 3 – Отправка пустой формы

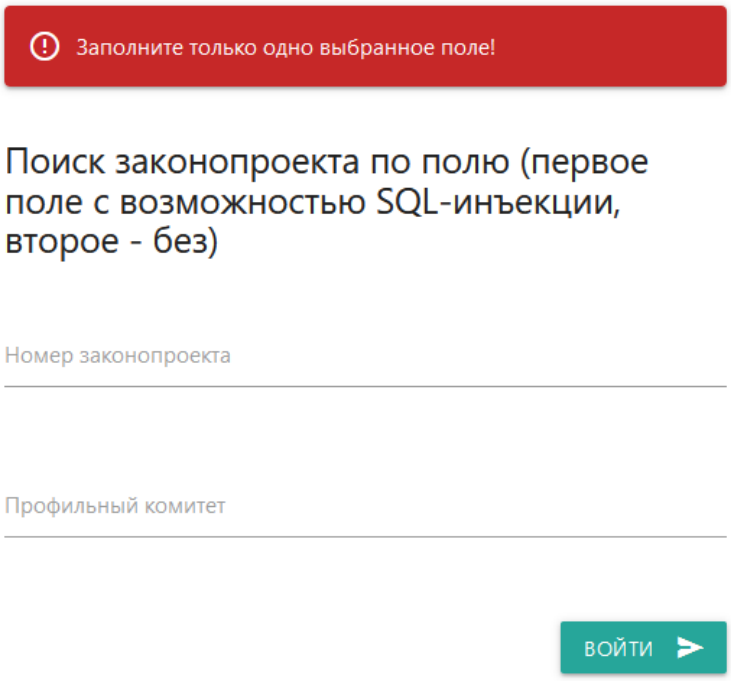

Рисунок 4 – Отправка полностью заполненной формы

Найдём закон по его номеру:

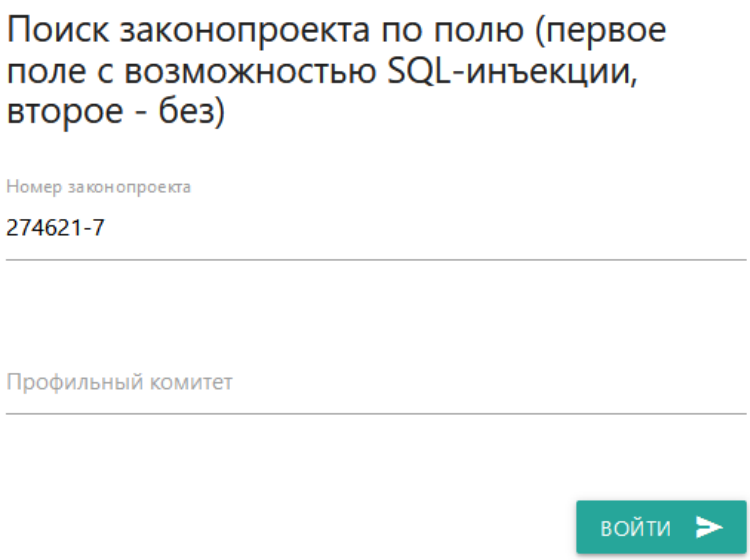

Рисунок 5 – Поиск закона по его номеру

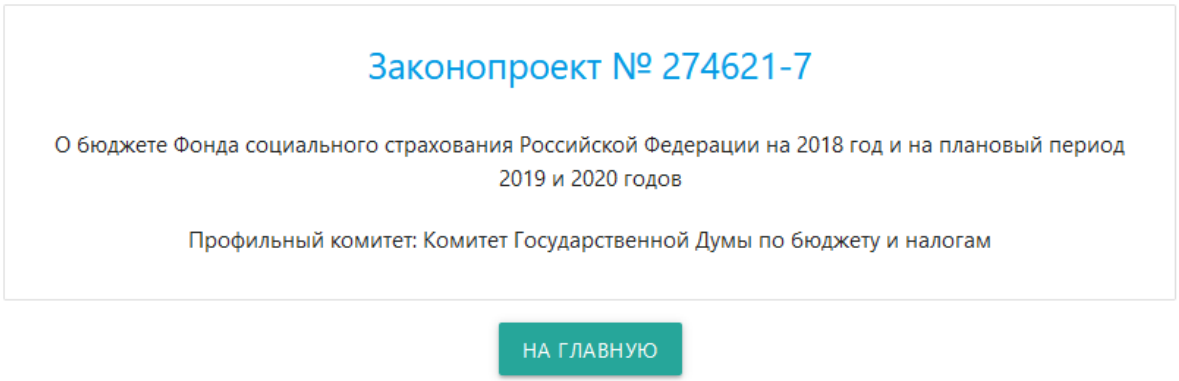

Рисунок 6 – Найденный закон

Как видим из рисунка 6, закон был успешно найден. Теперь попытаемся провести SQL-инъекцию следующего вида: *qwerty'; SELECT * from law;--*

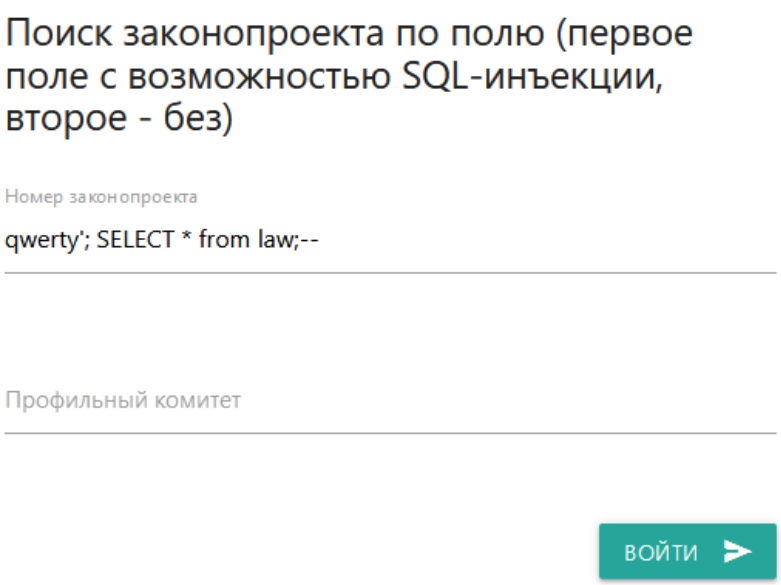

Рисунок 7 – Попытка проведения SQL-инъекции

Рисунок 8 – Успешная SQL-инъекция

Как видим из рисунка 8, SQL-инъекция была успешно проведена – были выведены все записи из таблицы law. Теперь проведём следующую SQL-инъекцию: *qwerty'; DROP TABLE law;--*

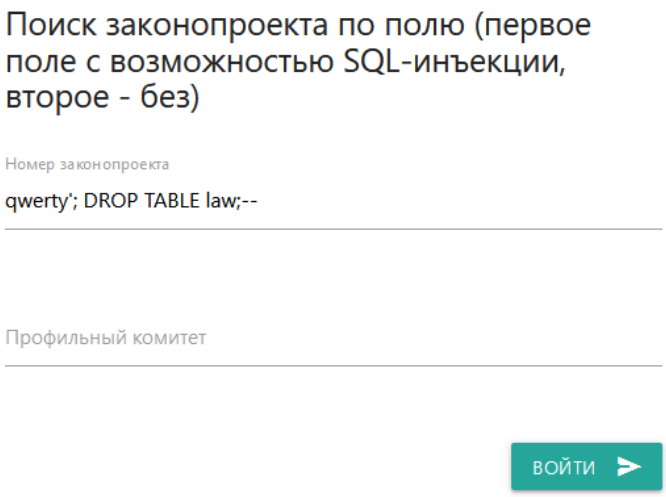

Рисунок 9 – Попытка проведения SQL-инъекции

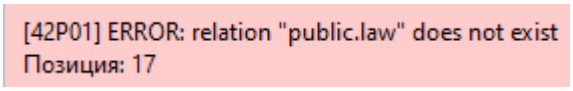

Рисунок 10 – Успешная SQL-инъекция

Как видим из рисунка 10, SQL-инъекция была успешно выполнена и таблица law удалена. Перейдём к работе с PDO.

Найдём закон по профильному комитету:

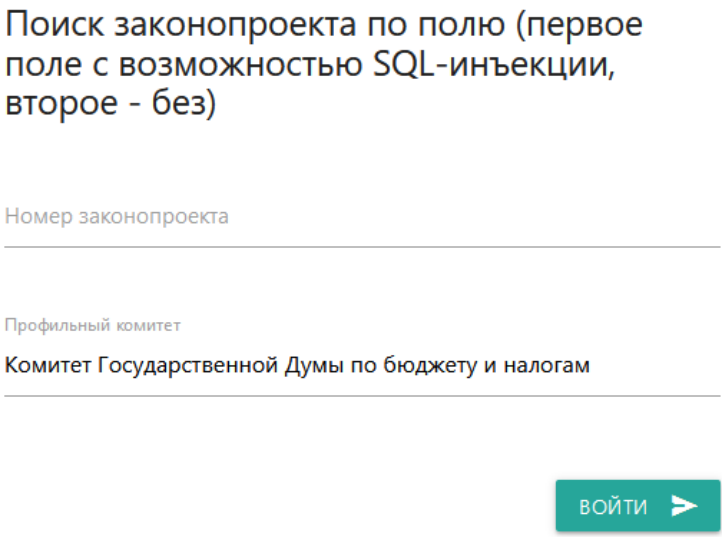

Рисунок 11 – Поиск закона по профильному комитету

Рисунок 12 – Найденные законы

Как видим из рисунка 12, законы были успешно найдены. Теперь попытаемся провести SQL-инъекцию следующего вида: *qwerty'; SELECT * from law;--*

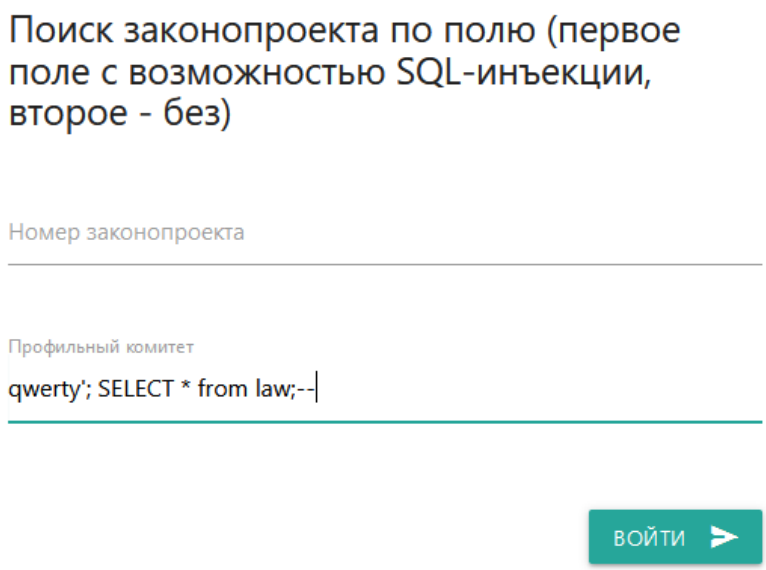

Рисунок 13 – Попытка проведения SQL-инъекции

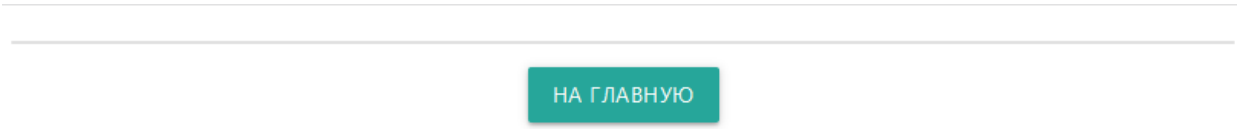

Рисунок 14 – Неудача SQL-инъекции

Как видим из рисунка 14, SQL-инъекция провалилась. Попытаемся провести следующую SQL-инъекцию: *qwerty'; DROP TABLE law;--*

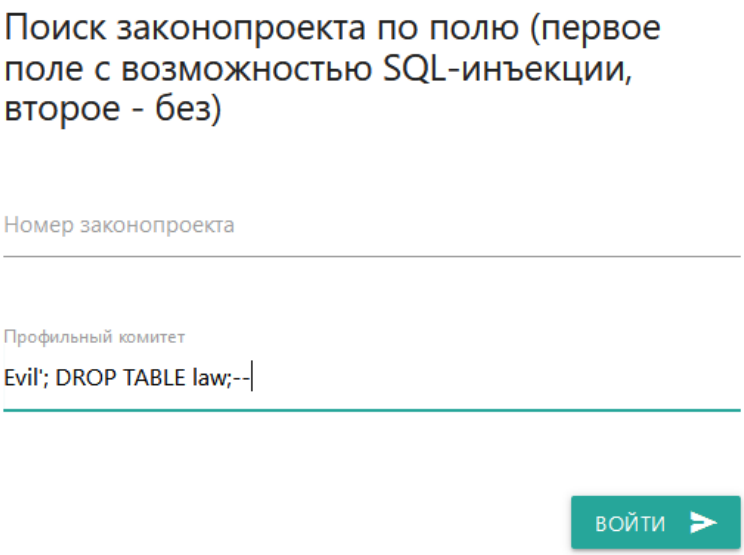

Рисунок 15 – Попытка проведения SQL-инъекции

В результате данной SQL-инъекции таблица law не удалилась – попытка провалилась.

Можно сделать следующий вывод: PDO является более предпочтительным драйвером для работы с базами данных, так как не допускает мультикомандные запросы и с помощью параметров корректно обрабатывает передаваемые данные.