Работа с sql-инъекциями

Для выполнения работы был создан проект с двумя страницами: первая страница содержит форму поиска законопроекта, вторая страница показывает информацию о законопроекте.

Дизайн первой страницы

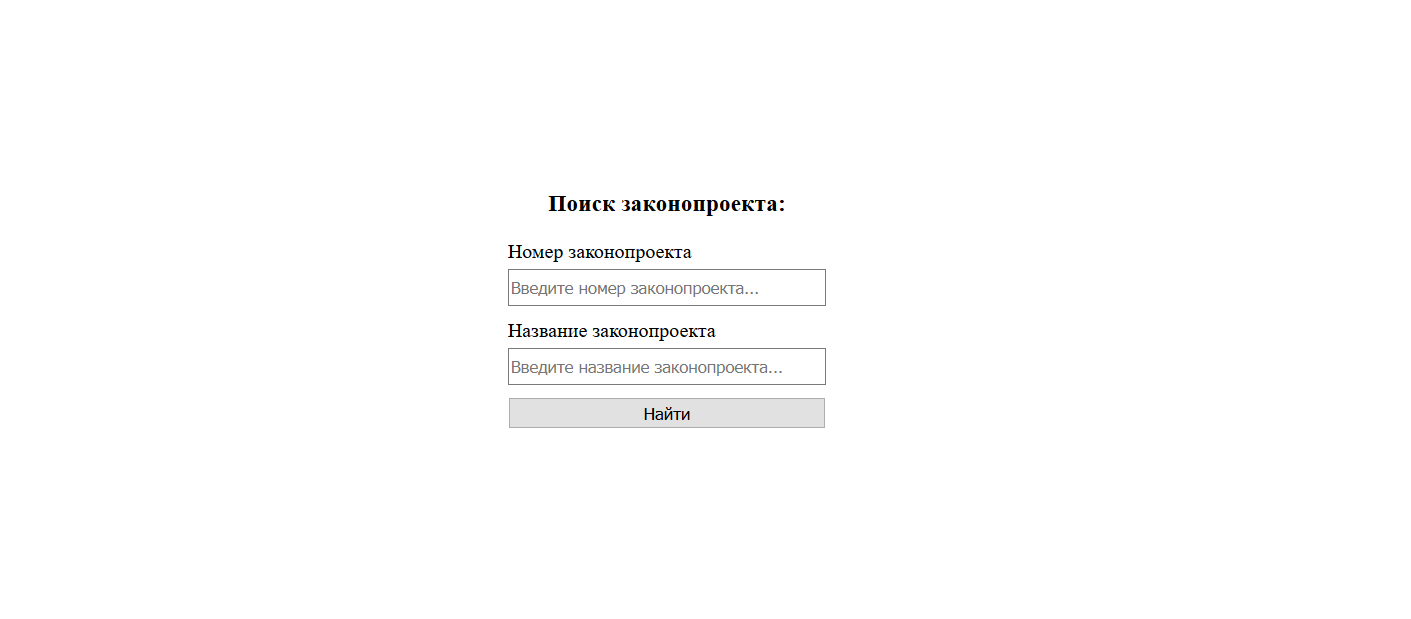


Рисунок – 1. Дизайн главной страницы

Дизайн второй страницы

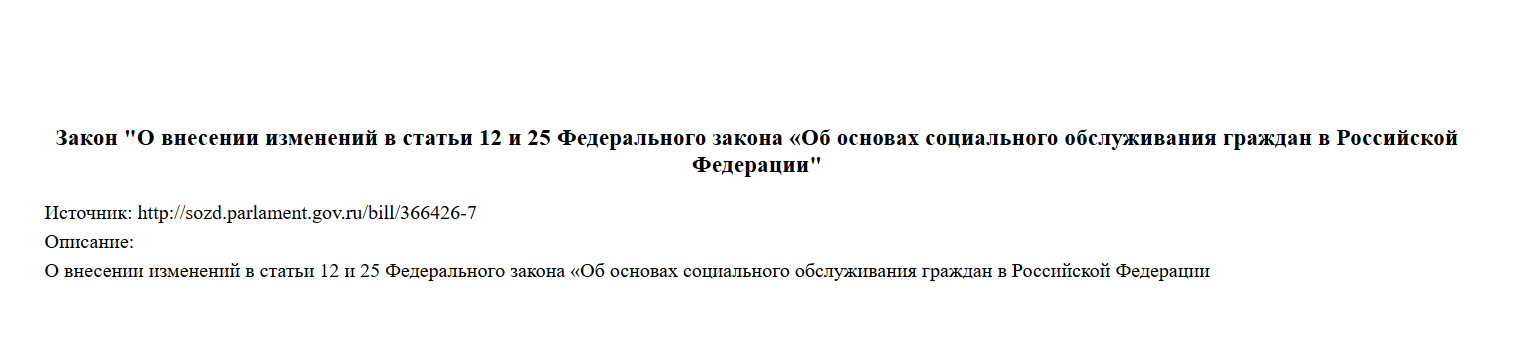


Рисунок – 2. Дизайн второй страницы

Примеры sql-инъекции

1. Попробуем в поле номер законопроекта ввести 366426-7

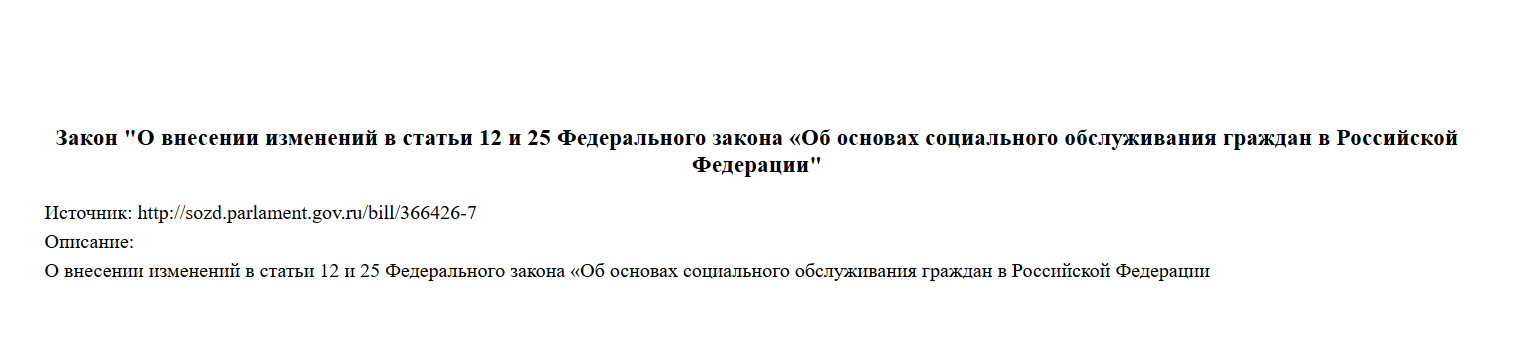


Рисунок – 3. Правильный вывод информации о законе

1. Попробуем в поле номер законопроекта ввести 366426-7 OR 1=1

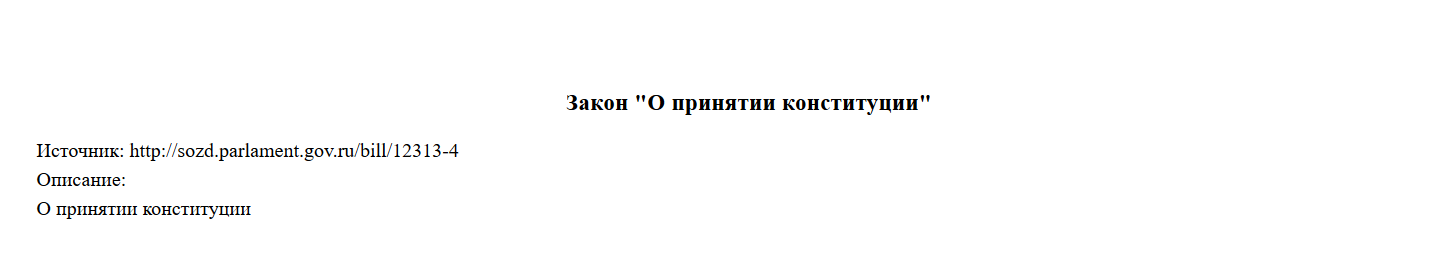


Рисунок – 4. Неверный вывод информации о законе

Так как данное поле не защищено от sql-инъекций, то при записи в поле номер законопроекта строчки 366426-7 OR 1=1 мы получили запись, которая имеет совсем другой номер законопроекта.

1. Проверим как защищено поле “название законопроекта”. Введем сначала правильные данные и посмотрим результат.

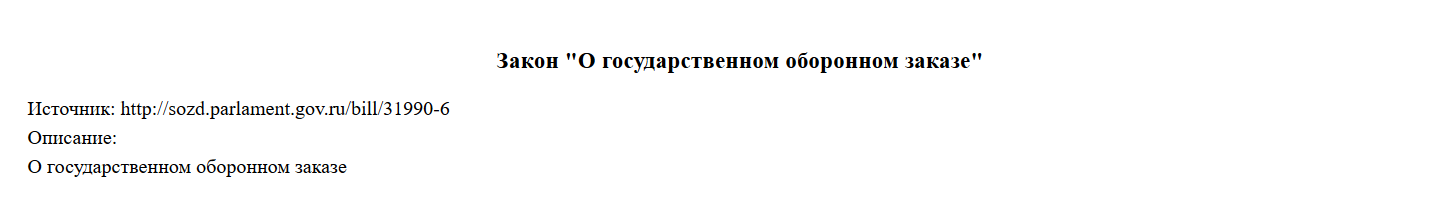


Рисунок – 5. Пример вывода при правильном вводе

1. Введем неверные данные в поле “название законопроекта”. Введем в поле значение " or ""="

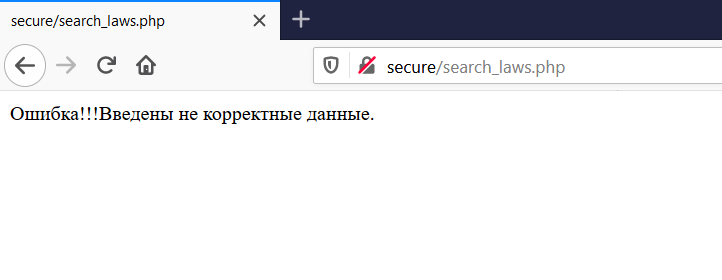


Рисунок – 6. Результат выполнения

Так как для создания запроса к бд мы используем PDO, то данный запрос не был выполнен и на выход мы получаем пустую переменную $law.

1. Проверка sql-инъекции на основе пакетных операторов. Запишем в поле “название законопроекта” строку “О государственном оборонном заказе; DROP TABLE laws”.

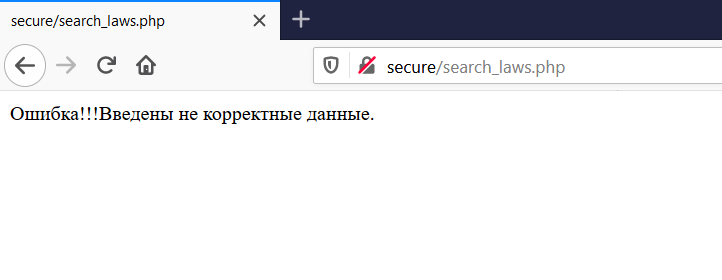


Рисунок – 7. Результат выполнения