

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:

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

ВОЙТИ ➤

Рисунок 1 – Форма поиска закона

Вторая страница – результат поиска:

Законопроект №274621-7

О бюджете Фонда социального страхования Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов

Профильный комитет: Комитет Государственной Думы по бюджету и налогам

НА ГЛАВНУЮ

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:

! Заполните одно выбранное поле!

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

ВОЙТИ >

Рисунок 3 – Отправка пустой формы

! Заполните только одно выбранное поле!

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

ВОЙТИ >

Рисунок 4 – Отправка полностью заполненной формы

Найдём закон по его номеру:

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

274621-7

Профильный комитет

ВОЙТИ >

Рисунок 5 – Поиск закона по его номеру

Законопроект № 274621-7

О бюджете Фонда социального страхования Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов

Профильный комитет: Комитет Государственной Думы по бюджету и налогам

НА ГЛАВНУЮ

Рисунок 6 – Найденный закон

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

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

qwerty'; SELECT * from law;--

Профильный комитет

ВОЙТИ ➤

Рисунок 7 – Попытка проведения SQL-инъекции

Законопроект № 947436-7 О внесении изменений в Федеральный закон "О недрах" в части отнесения полезных ископаемых к общераспространенным полезным ископаемым Профильный комитет: Комитет Государственной Думы по природным ресурсам
Законопроект № 31990-6 О государственном оборонном заказе Профильный комитет: Комитет Государственной Думы по обороне
Законопроект № 274620-7 О бюджете Федерального фонда обязательного медицинского страхования на 2018 год и на плановый период 2019 и 2020 годов Профильный комитет: Комитет Государственной Думы по бюджету и налогам
Законопроект № 274618-7 О федеральном бюджете на 2018 год и на плановый период 2019 и 2020 годов Профильный комитет: Комитет Государственной Думы по бюджету и налогам
Законопроект № 274619-7 О бюджете Пенсионного фонда Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов Профильный комитет: Комитет Государственной Думы по бюджету и налогам
Законопроект № 366426-7 О внесении изменений в статьи 12 и 25 Федерального закона "Об основах социального обслуживания граждан в Российской Федерации" Профильный комитет: Комитет Государственной Думы по труду

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;--*

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

qwerty'; DROP TABLE law;--

Профильный комитет

ВОЙТИ >

Рисунок 9 – Попытка проведения SQL-инъекции

[42P01] ERROR: relation "public.law" does not exist
Позиция: 17

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:

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

Комитет Государственной Думы по бюджету и налогам

ВОЙТИ >

Рисунок 11 – Поиск закона по профильному комитету

<p>Законопроект № 274620-7</p> <p>О бюджете Федерального фонда обязательного медицинского страхования на 2018 год и на плановый период 2019 и 2020 годов</p> <p>Профильный комитет: Комитет Государственной Думы по бюджету и налогам</p>
<p>Законопроект № 274618-7</p> <p>О федеральном бюджете на 2018 год и на плановый период 2019 и 2020 годов</p> <p>Профильный комитет: Комитет Государственной Думы по бюджету и налогам</p>
<p>Законопроект № 274619-7</p> <p>О бюджете Пенсионного фонда Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов</p> <p>Профильный комитет: Комитет Государственной Думы по бюджету и налогам</p>
<p>Законопроект № 274621-7</p> <p>О бюджете Фонда социального страхования Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов</p> <p>Профильный комитет: Комитет Государственной Думы по бюджету и налогам</p>
<p>Законопроект № 274622-7</p> <p>О страховых тарифах на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний на 2018 год и на плановый период 2019 и 2020 годов</p> <p>Профильный комитет: Комитет Государственной Думы по бюджету и налогам</p>

НА ГЛАВНУЮ

Рисунок 12 – Найденные законы

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

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

qwerty'; SELECT * from law;--|

ВОЙТИ >

Рисунок 13 – Попытка проведения SQL-инъекции

НА ГЛАВНУЮ

Рисунок 14 – Неудача SQL-инъекции

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

Поиск законопроекта по полю (первое поле с возможностью SQL-инъекции, второе - без)

Номер законопроекта

Профильный комитет

Evil'; DROP TABLE law;--|

ВОЙТИ >

Рисунок 15 – Попытка проведения SQL-инъекции

В результате данной SQL-инъекции таблица law не удалась – 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.