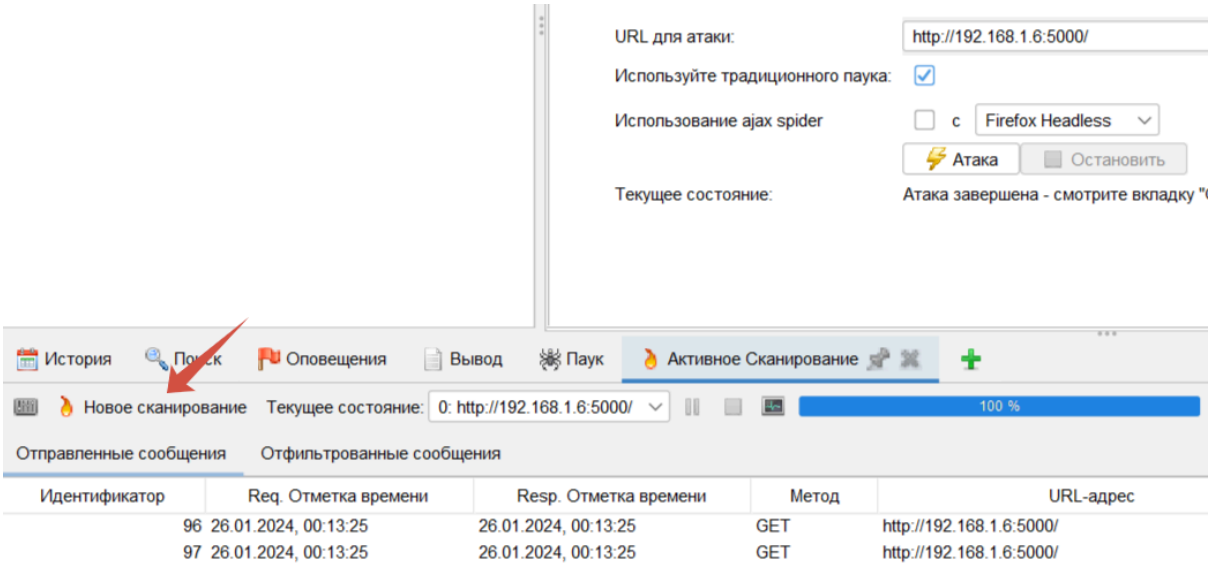
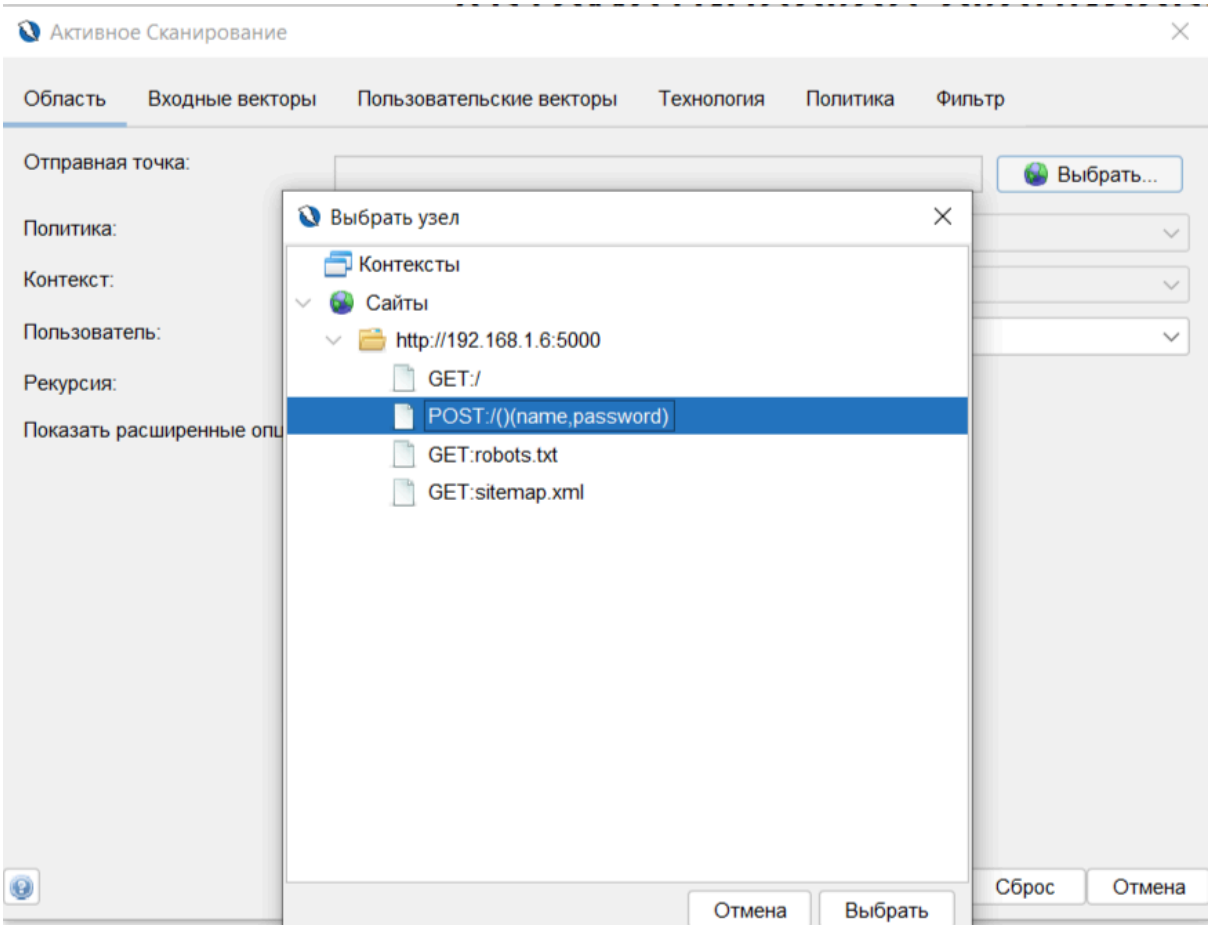
sql-injection-exploit.pdf

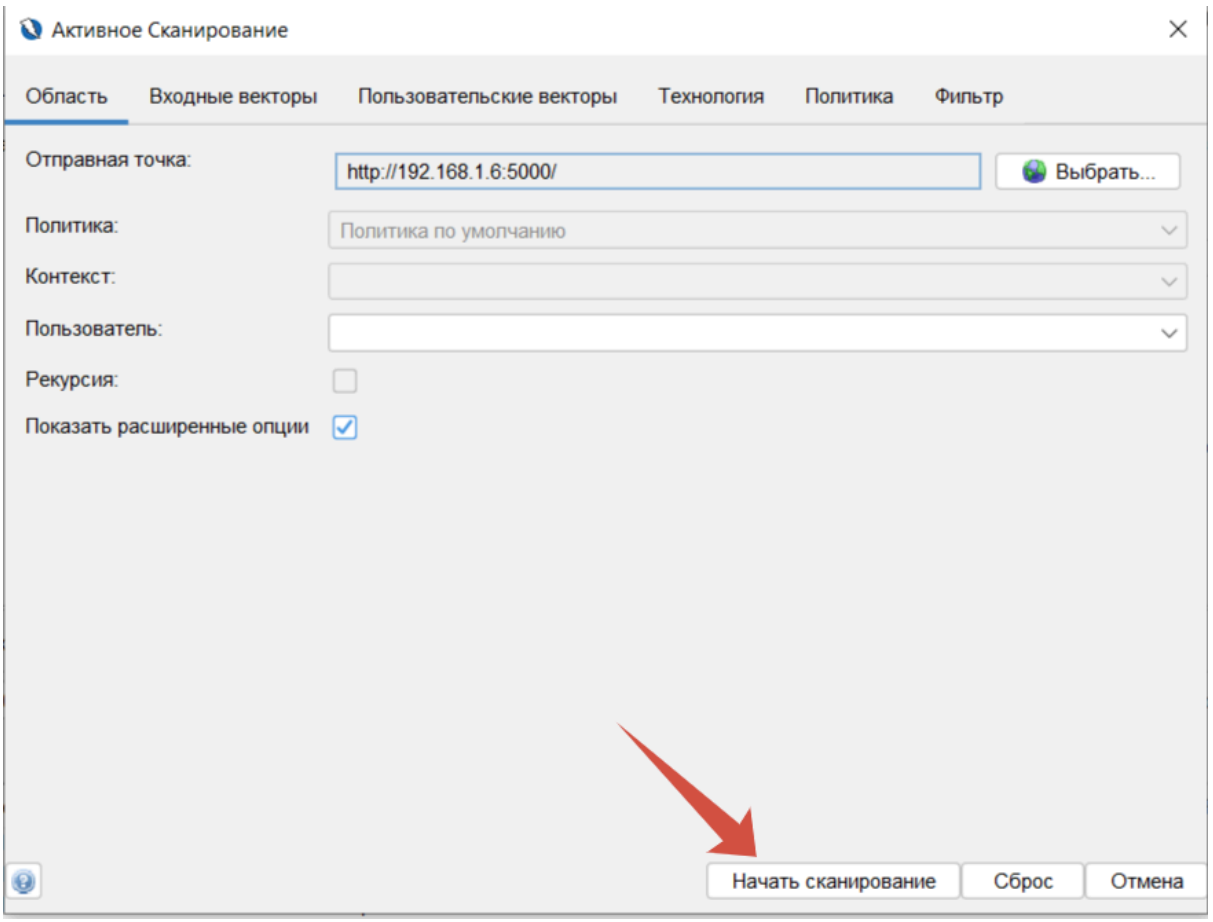
Итак, после запуска атаки на сайт, может случиться, что вы не обнаружите уязвимость sql-injection. Можно подождать, пока ZAP сам запустит активное сканирование, но можно не ждать и запустить его самим. Давайте сделаем это.



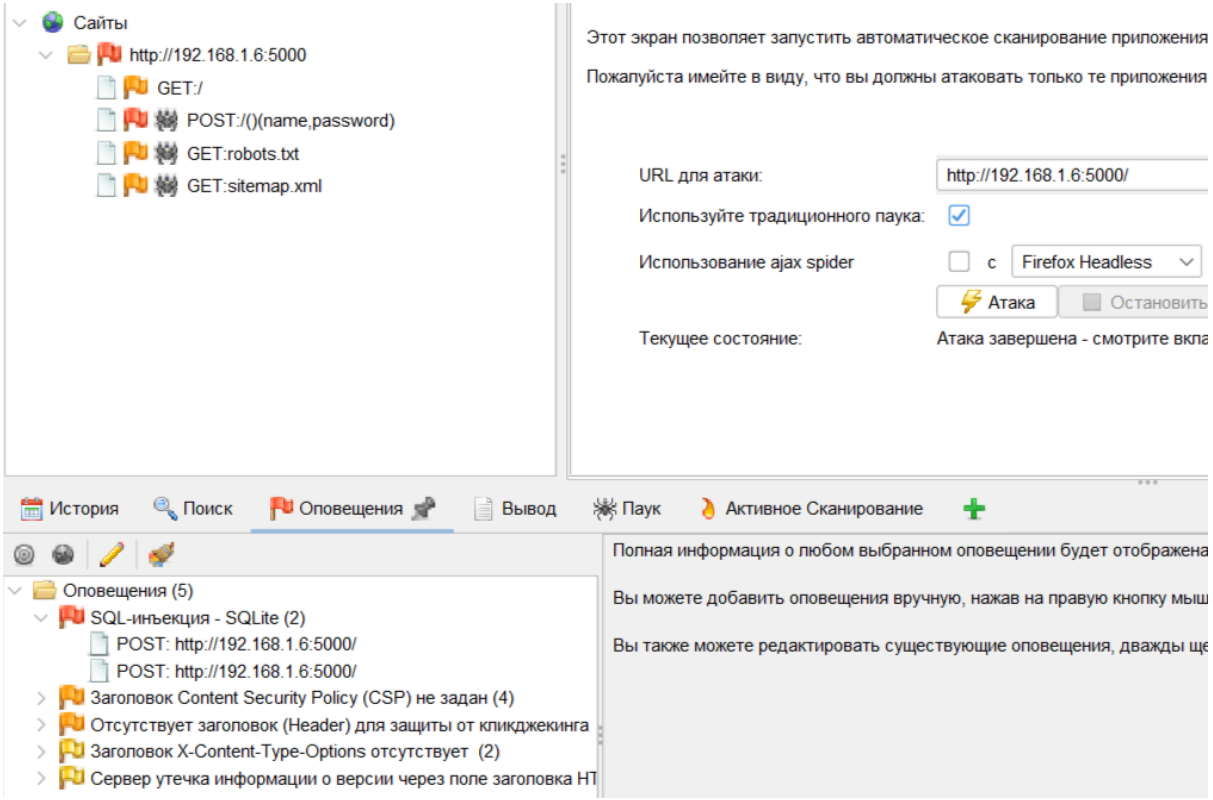
Прожмите кнопку на «Новое сканирование».
Далее выберите узел и метод POST. **Важно:** сайт не появится если не выполнить атаку.



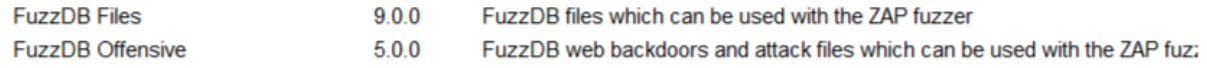
Все остальные настройки можно оставить как есть. Дальше нажмите «Начать сканирование» и сканирование запустится.



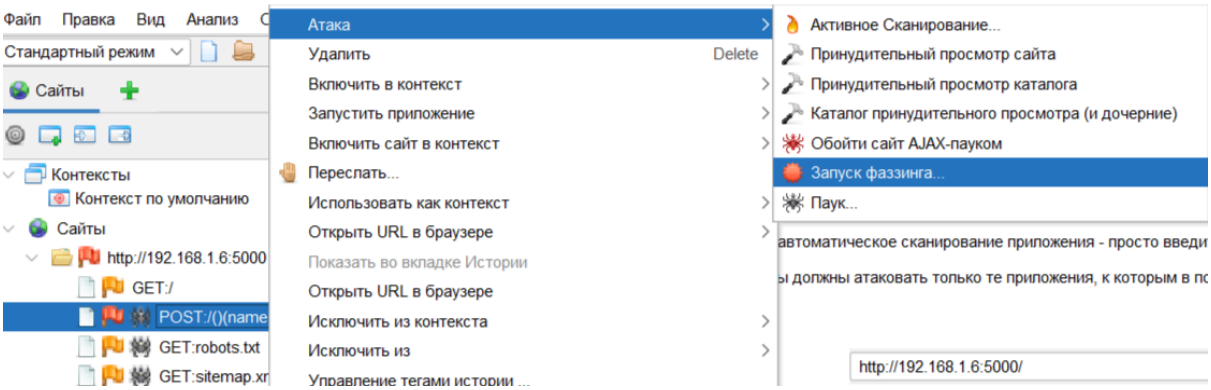
После этого появится обнаруженная уязвимость SQL-injection.



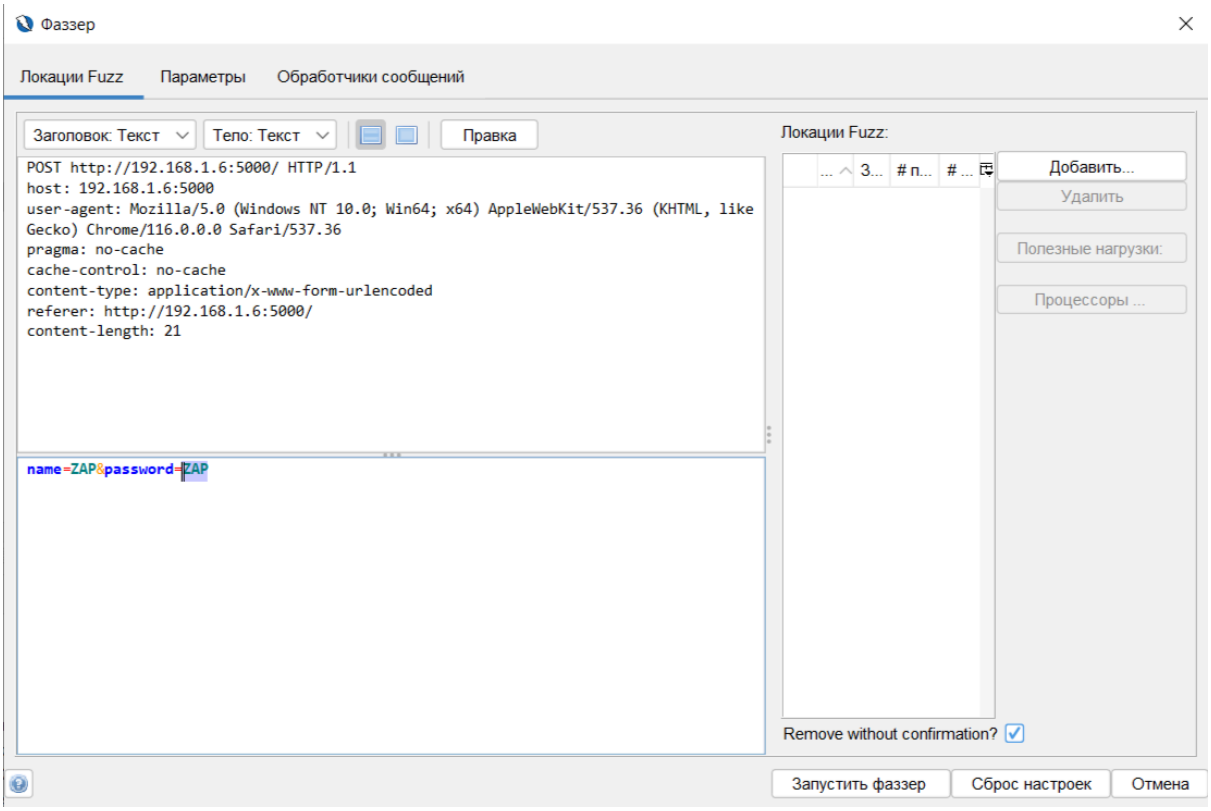
Итак, полдела сделано. Дальше нужно установить 2 новых плагина.
Найдите кнопку с дополнениями и перейдите на вкладку «Рынок дополнений». Затем установите их ***«FuzzDB Files»*** и ***«FuzzDB Offensive»***



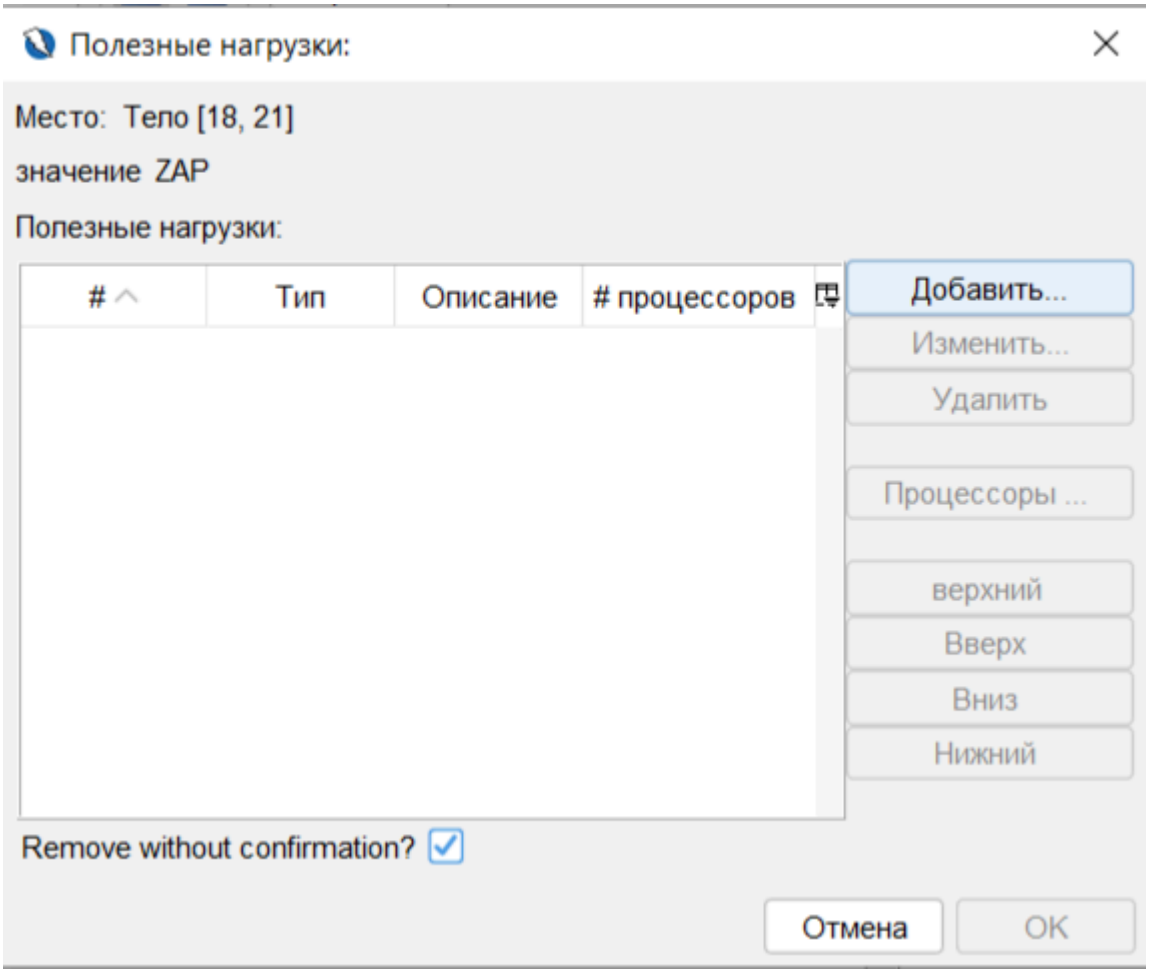
Последний шаг – раскрытие чувствительной информации.
Правой кнопкой мыши кликните на POST запрос на нашем сайте, далее «Атака», затем «Запуск фаззинга».



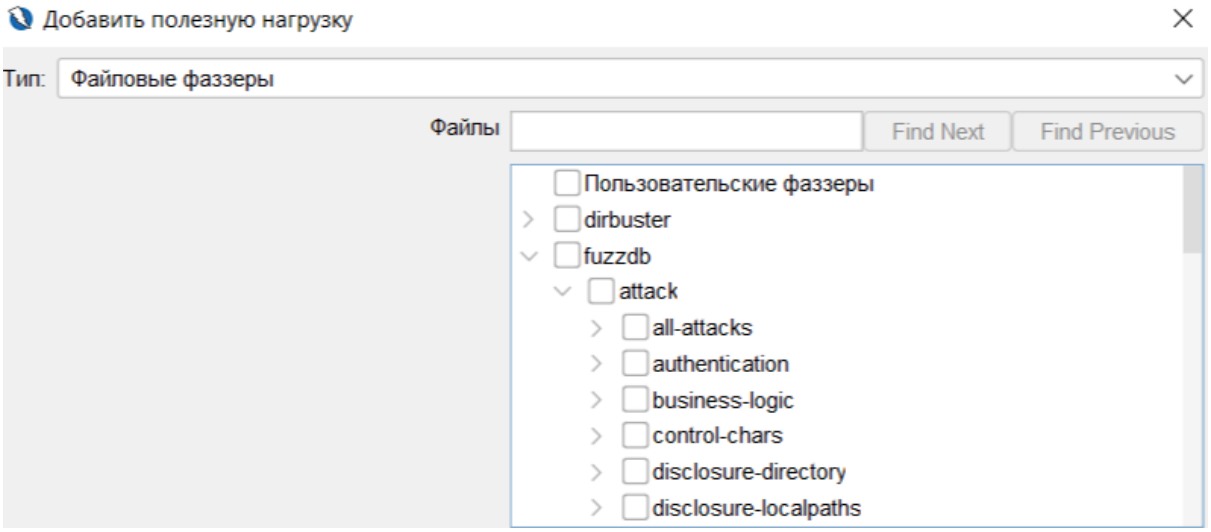
Вы увидите такое окно (как на скриншоте ниже). Выделите нужное поле – **password** – в теле запроса. После этого станет активна кнопка «добавить» в колонке «Локации Fuzz». Нажмите на неё.



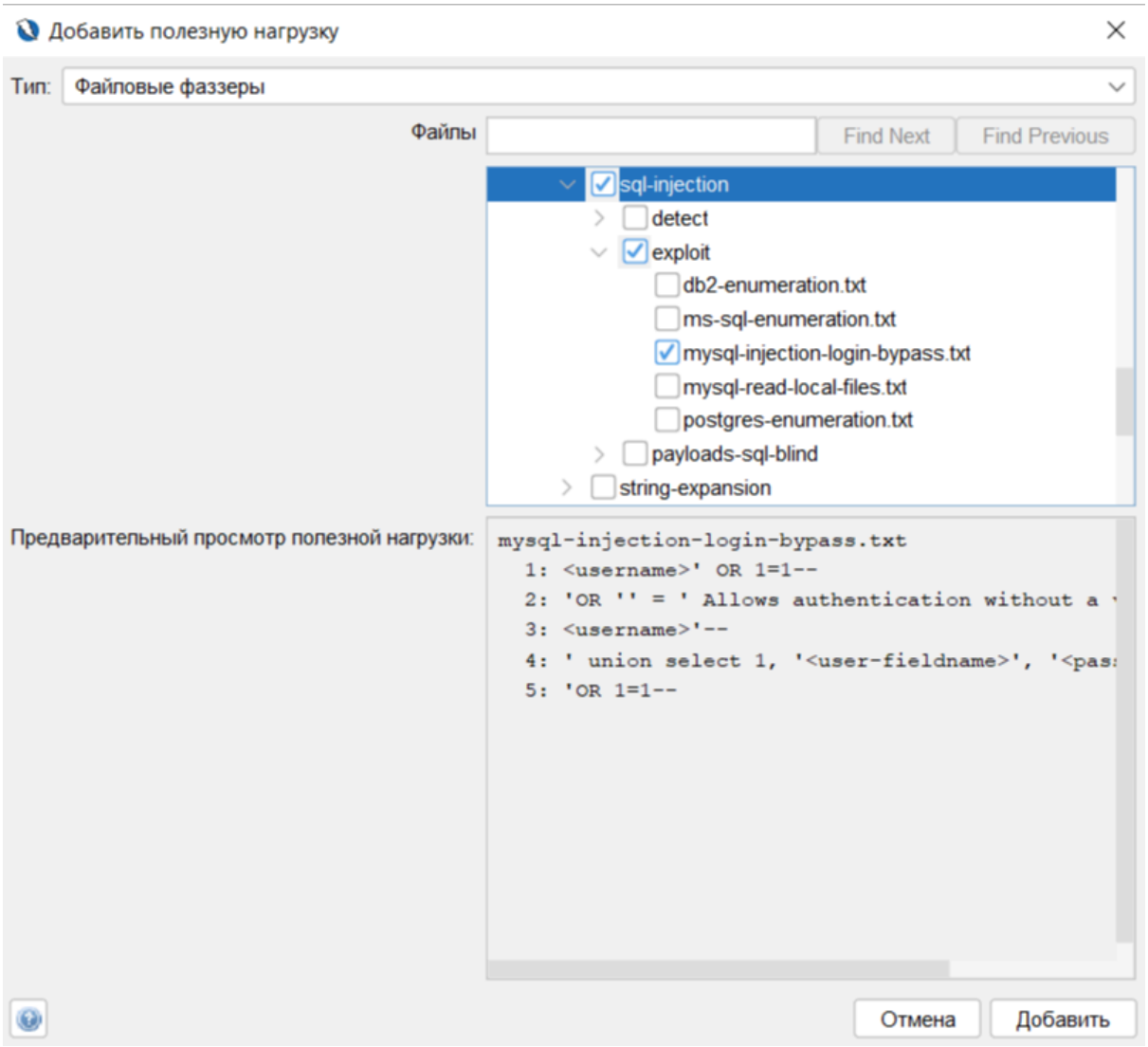
Затем снова нажмите «добавить».



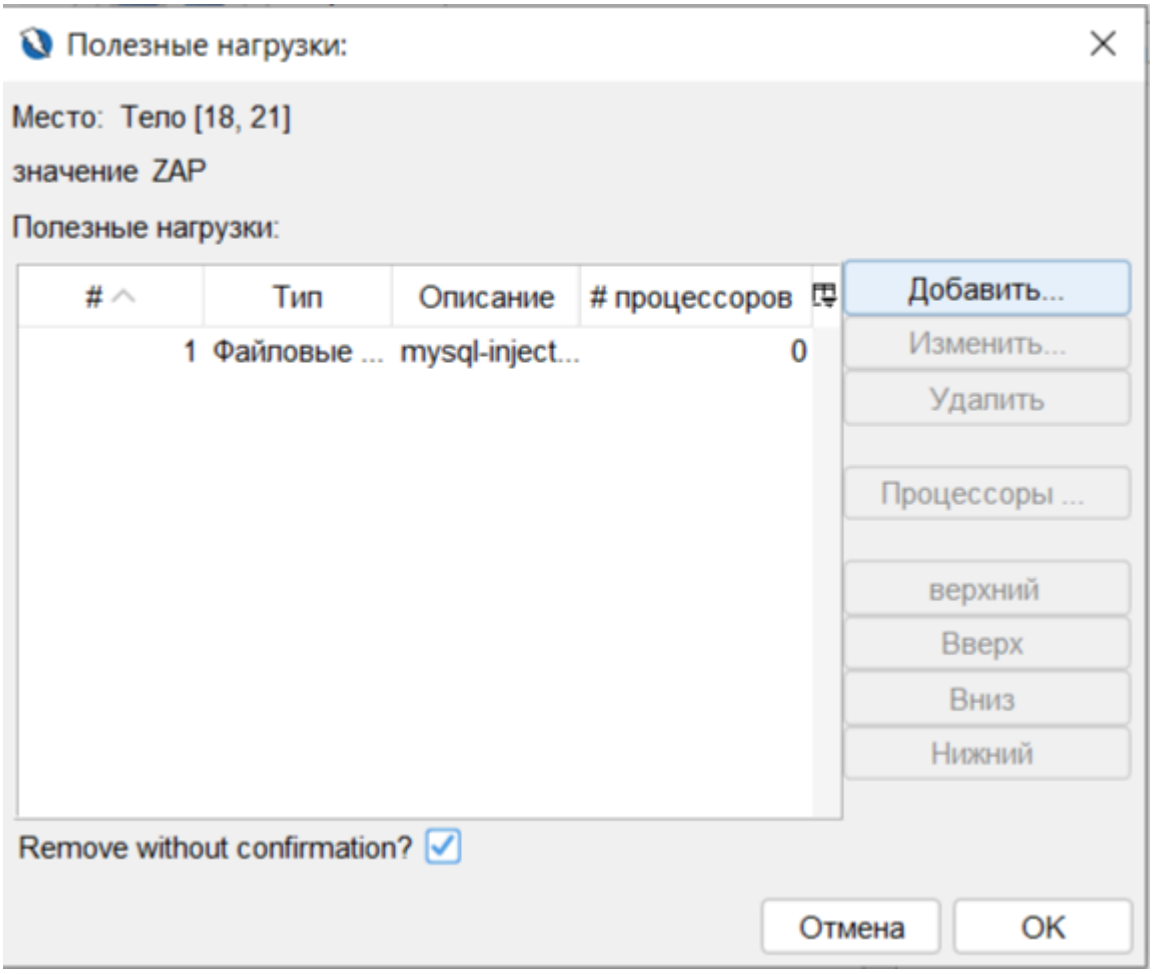
Далее выберите из списка тип фаззера «Файловые фаззеры», затем в колонке справа раскройте fuzzdb->attack->sql-injection->exploit.



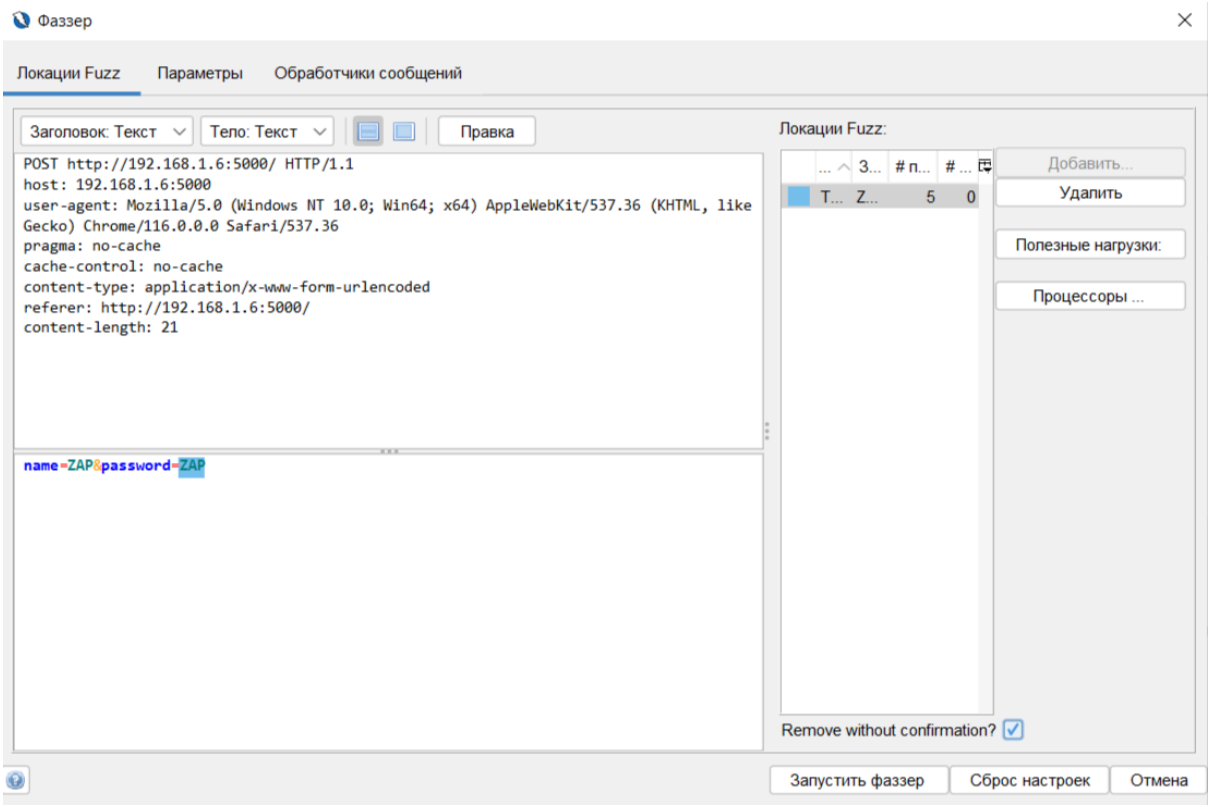
Выберите **mysql-injection-login-bypass** и нажмите «добавить».



Далее нажмите «ок».


Полезные нагрузки:
Место: Тело [18, 21]
значение ZAP
Полезные нагрузки:
^
Тип
Описание
процессоров
1
Файловые ...
mysql-inject...
0
Добавить...
Изменить...
Удалить
Процессоры ...
верхний
Вверх
Вниз
Нижний
Remove without confirmation?
Отмена
OK

И наконец-то запустите фаззер – а потом насладитесь его прекрасной работой.



После запуска, переключитесь на вкладку «ответ» и просмотрите каждый сформированный запрос. В одном из ответов мы сможете получить флаг.