personal project#5

Дисциплина: Основы информационной безопасности

Георгес Гедеон

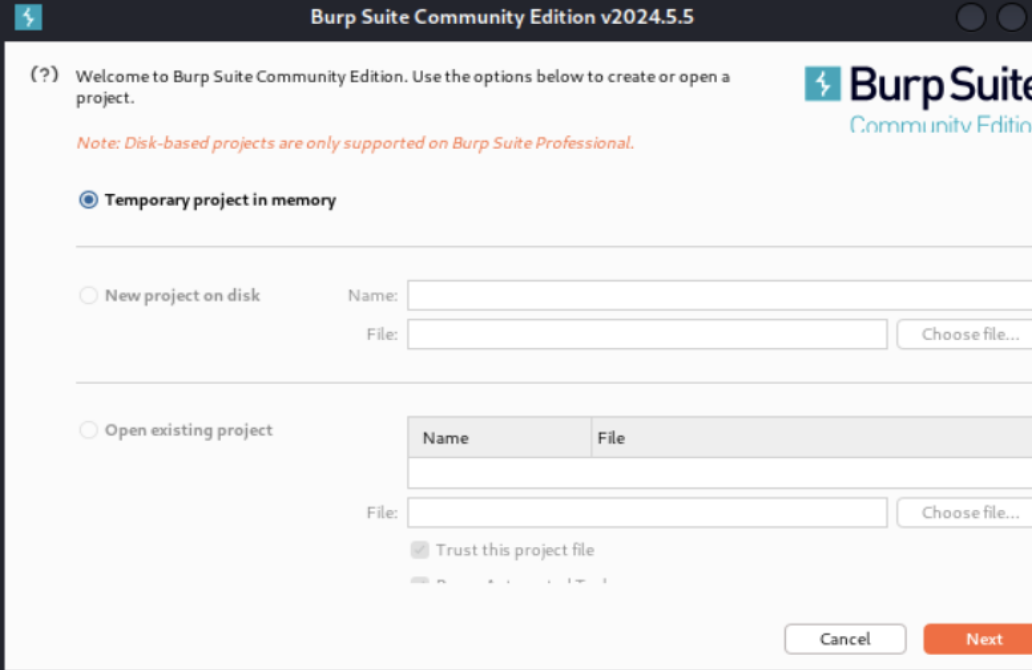
Содержание

## **Цель работы**

Использование Burp Suite.

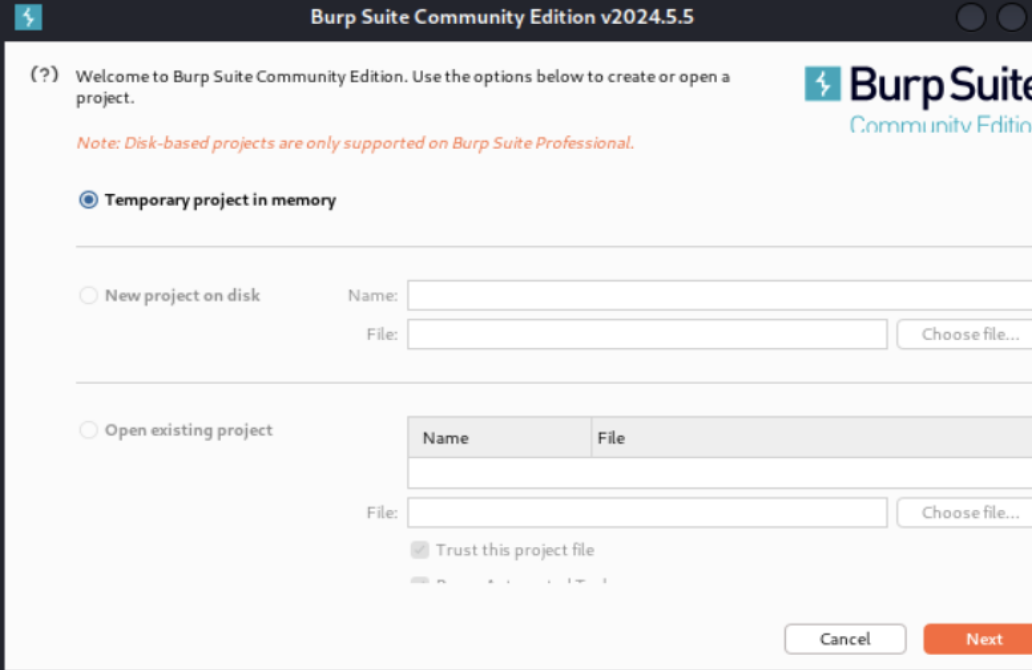
## **Выполнение работы**

Запустим необходимые для работы приложения такие, как Apache.

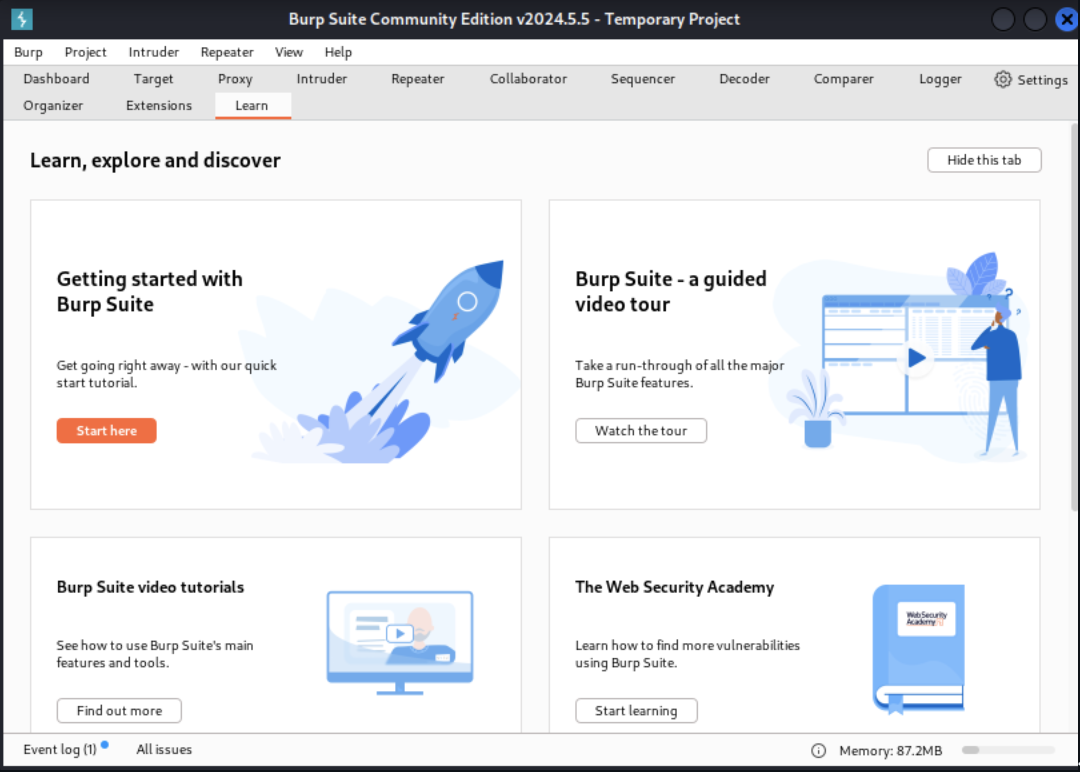


Подготовительный этап

Запускаем Burp Suite через терминал.

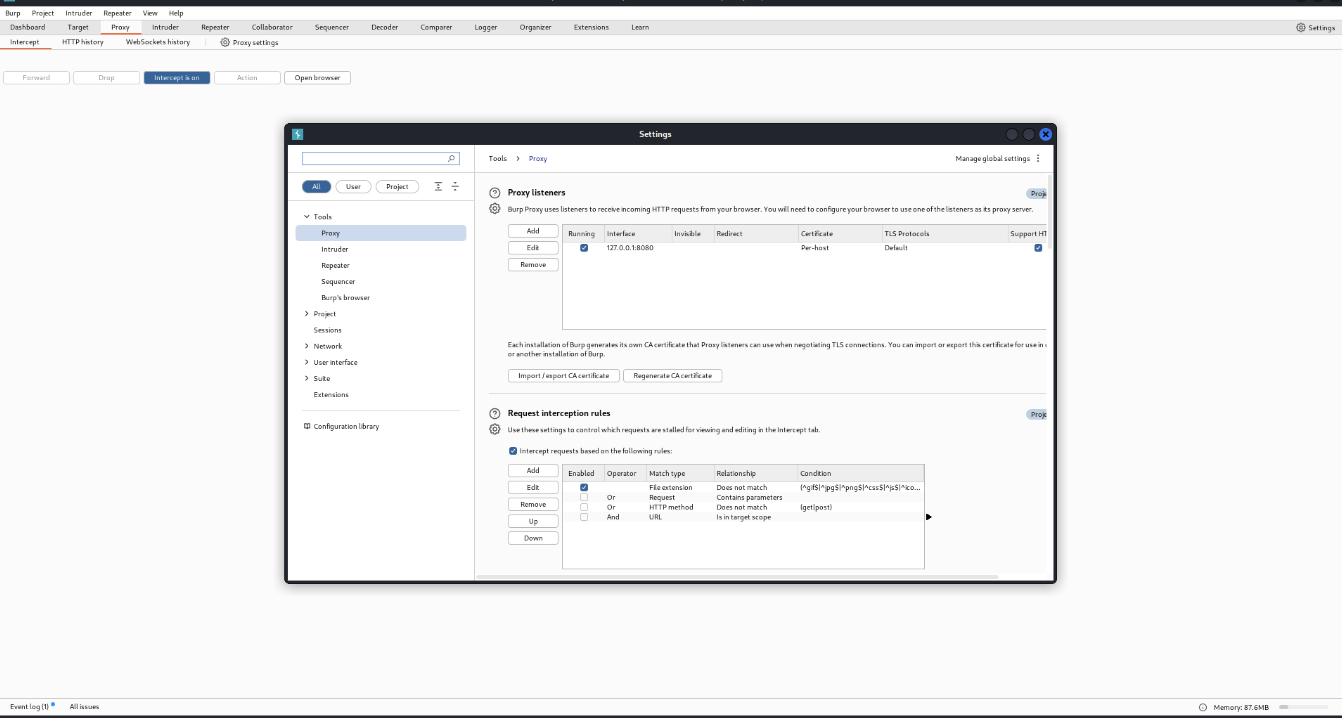


Запуск Burp Suite



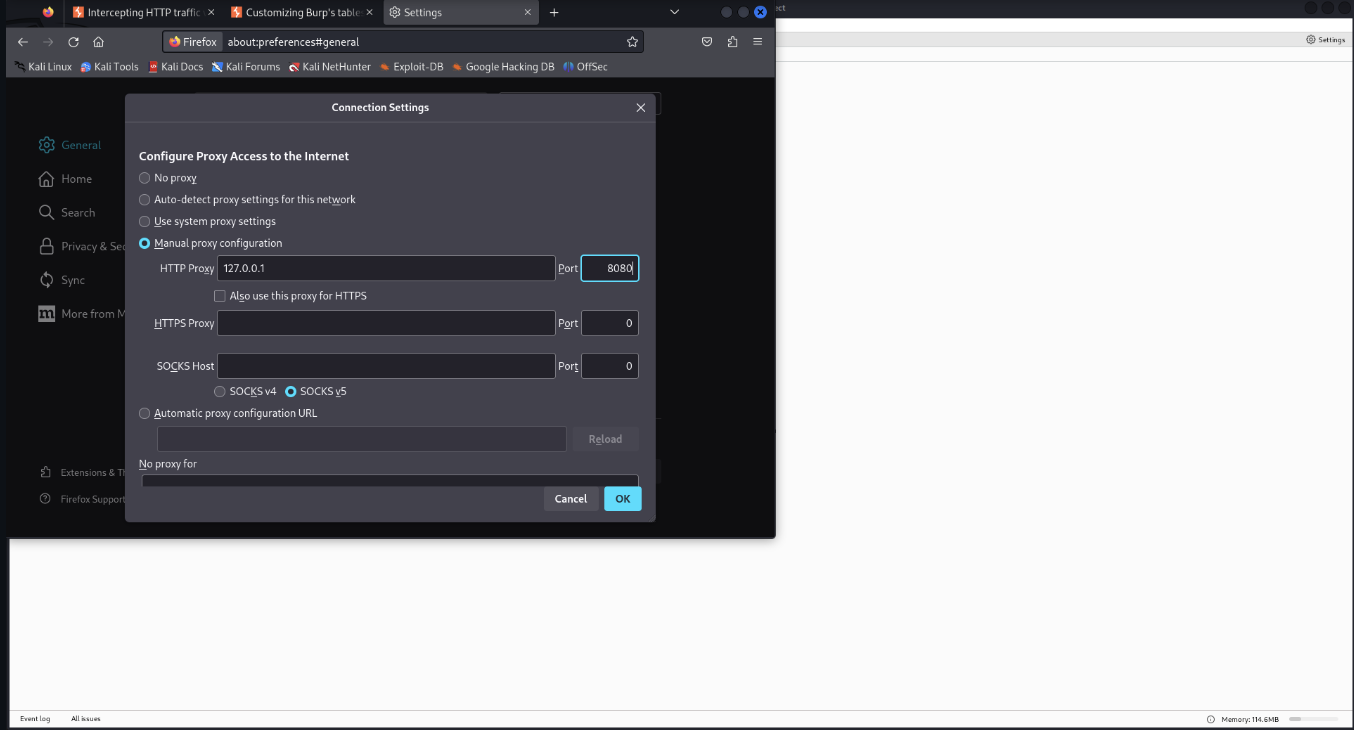
Интерфейс Burp Suite

Во вкладке Proxy убедимся, что Intercept включен.

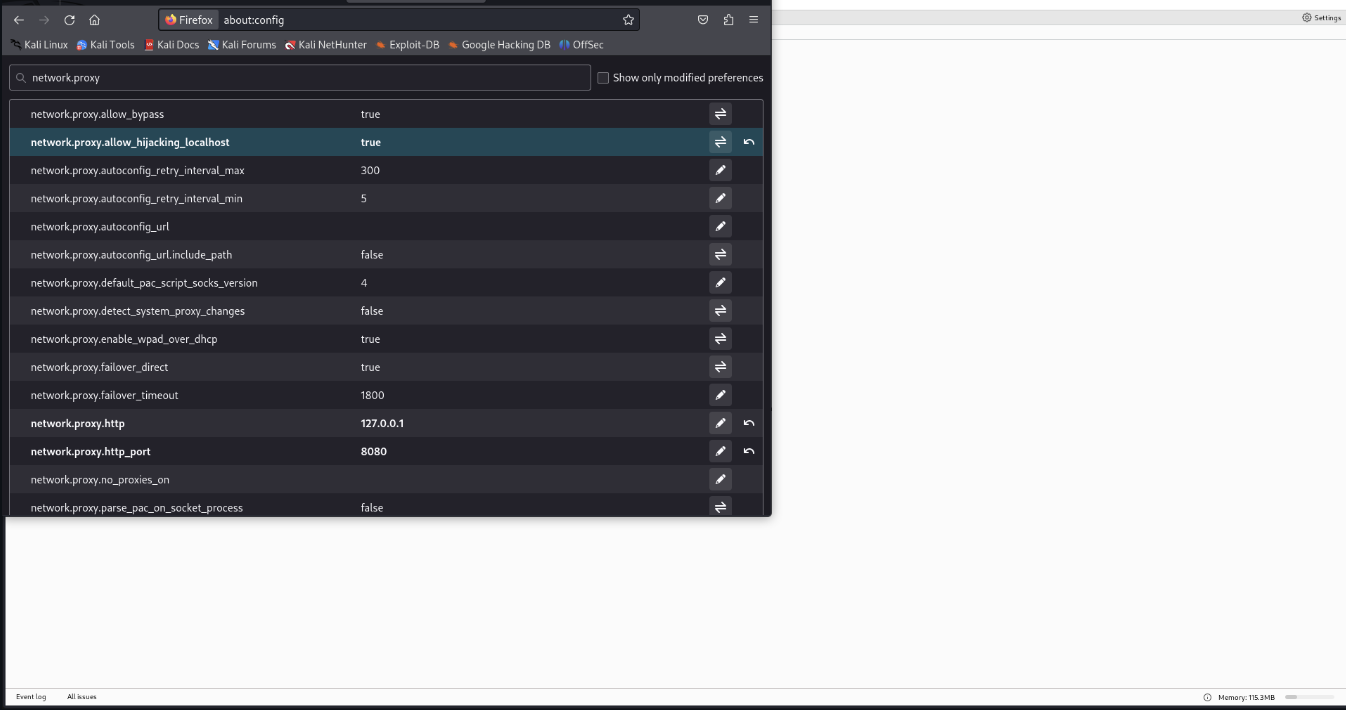


Intercept is on

Далее в настройках браузера Mozilla устанавливаем Proxy на наш localhost 127.0.0.1 и также устанавливаем параметр true на network.proxy.allow\_hijacking\_localhost.

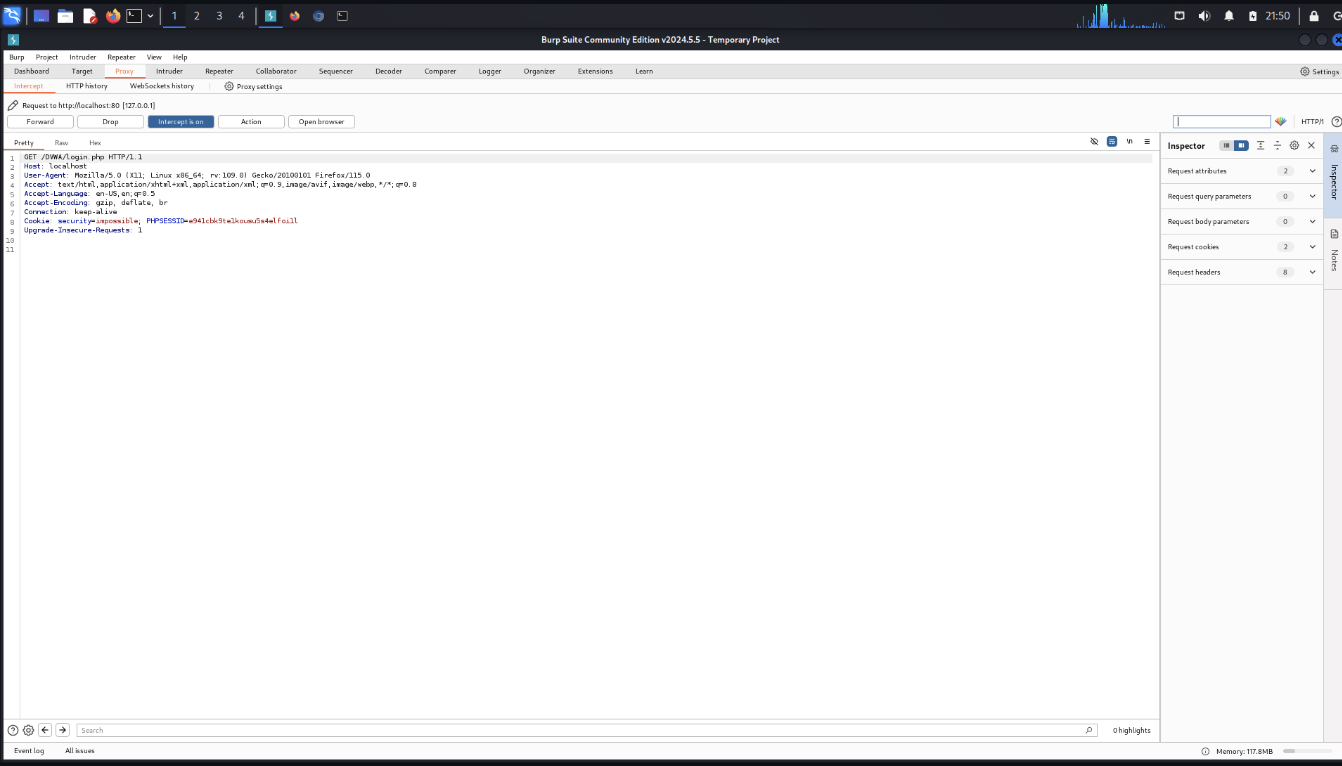


Настройка Proxy



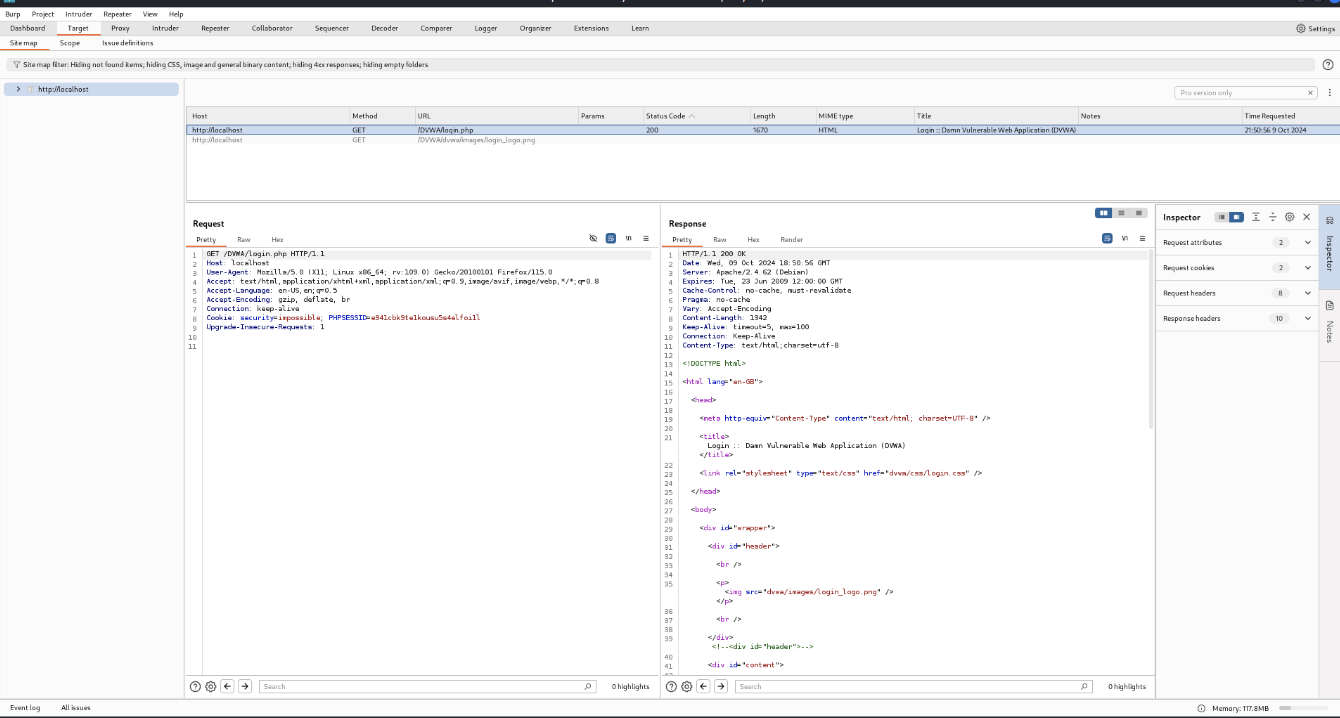
network.proxy.allow\_hijacking\_localhost

Теперь пытаемся зайти на страницу входа DVWA и видим, что наш сигнал был перехвачен Burp Suite.

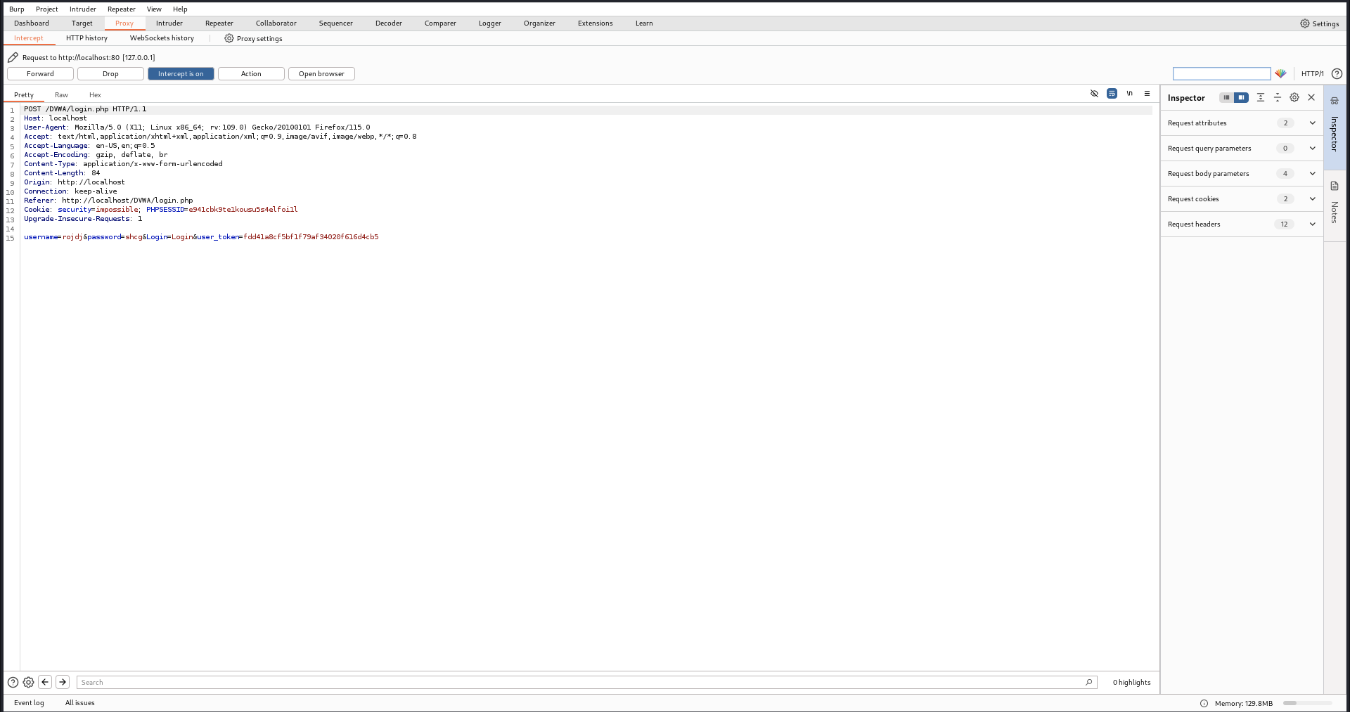


Перехват сигнала

Нажимаем Forward и переходим на вкладку Target, где можно увидеть все истории запросов. Пробуем вести какой-нибудь пароль и логин на странице DVWA и наблюдаем, что запрос был отображен в Burp Suite.

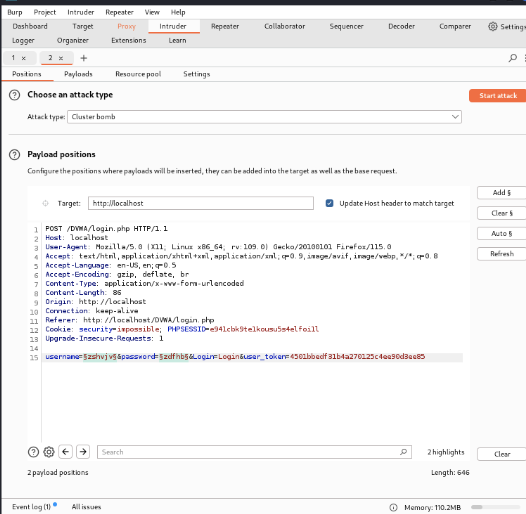


Target



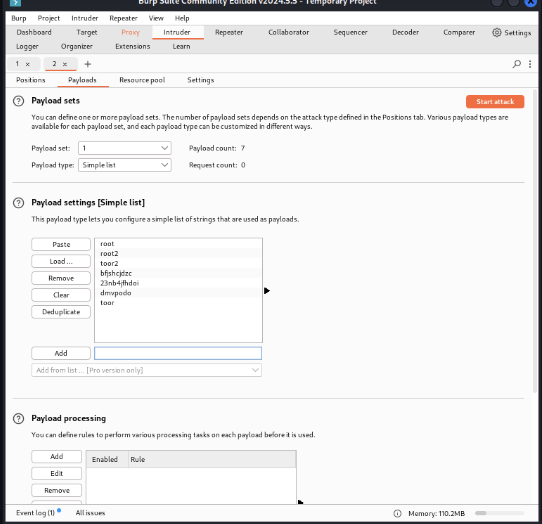
Отслеживание запросов

Находим этот запрос в Target и отправляем во вкладку Intruder, нажав правую кнопку мыши и найдя команду Send to Intruder. Перейдя во вкладку Intruder, изменим тип аттак на Claster Bomb и отметим специальными знаками в запросе те данные, которые хотим подобрать, то есть логин и пароль.

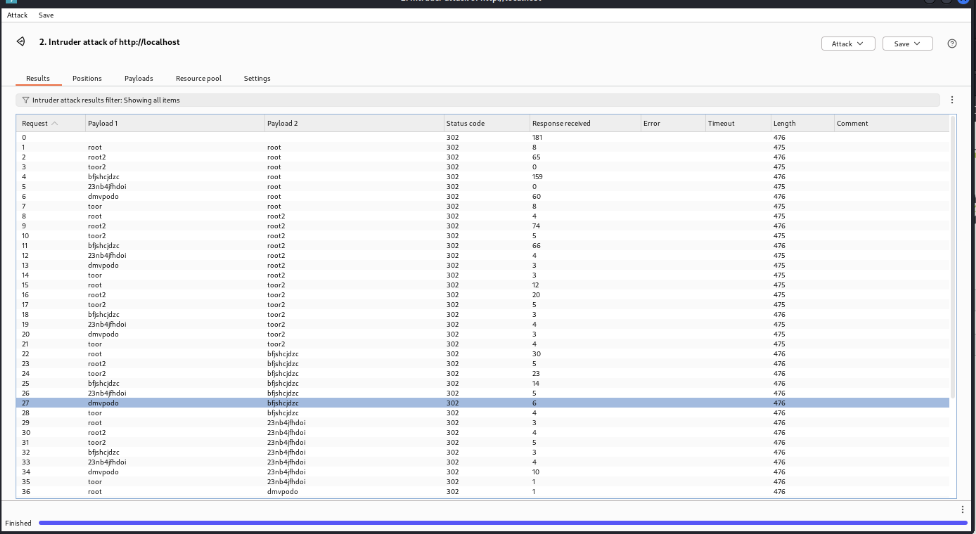


Intruder

В Payloads заполняем случайными данные для подбора логина и пароля.

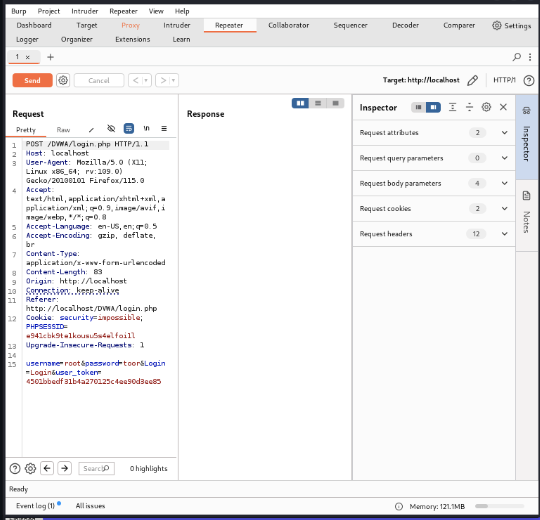


Логин

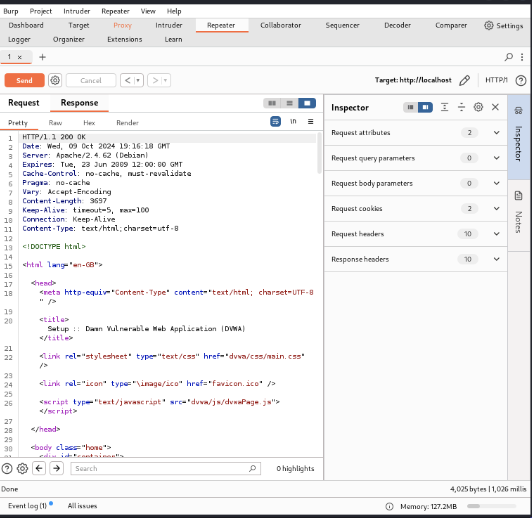


Пароль

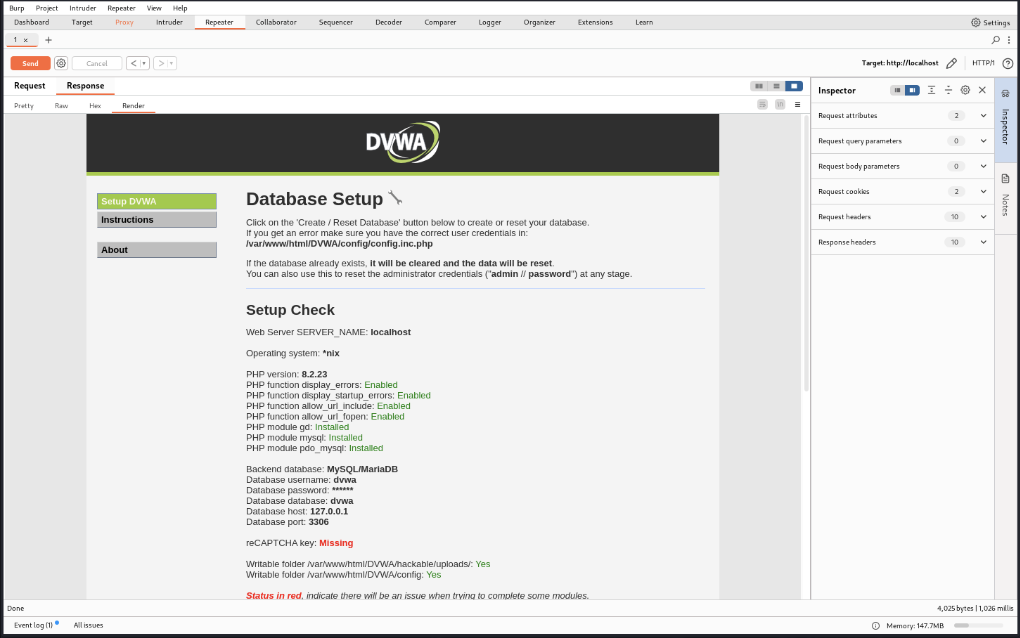
После нажатия кнопки Start Attack программа начинает перебирать всевозможные комбинации для входа. Находим единственно верную комбинацию и отправляем в Repeater для повторной проверки и убеждаемся, что данные подходят .



Подбор пароля



Repeater



Повторная проверка

## Вывод

Мы научились пользоваться Burp Suite.