Отчёт по индивидуальному проекту. Этап №5

*дисциплина: Информационная безопасность*

Морозова Ульяна

Содержание

# 1 Цель работы

Использование Burp Suite.

# 2 Выполнение лабораторной работы

1. Запустим необходимые для работы приложения такие, как Apache (рис. 1).

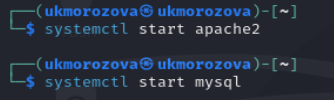


Рис. 1: Подготовительный этап

Запускаем Burp Suite через терминал (рис. 2 - рис. 3).

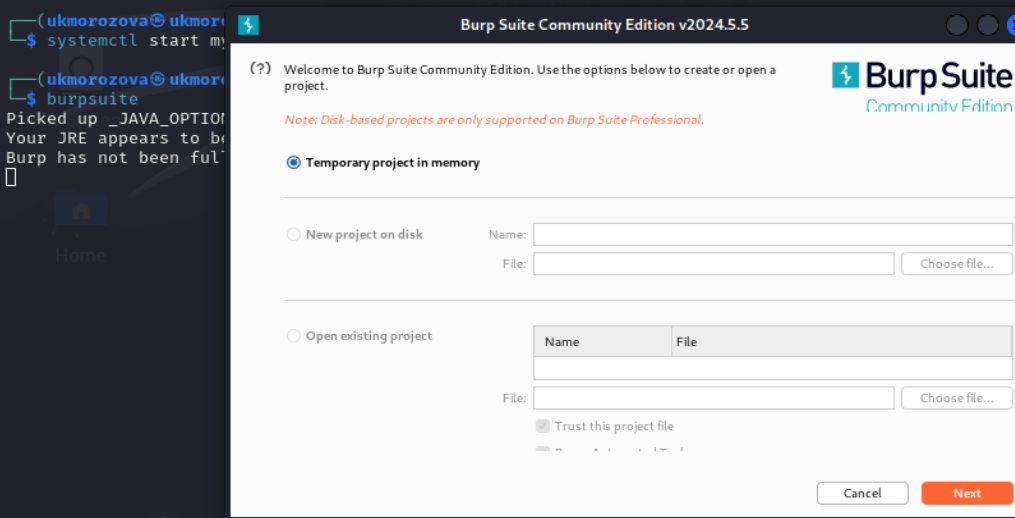


Рис. 2: Запуск Burp Suite

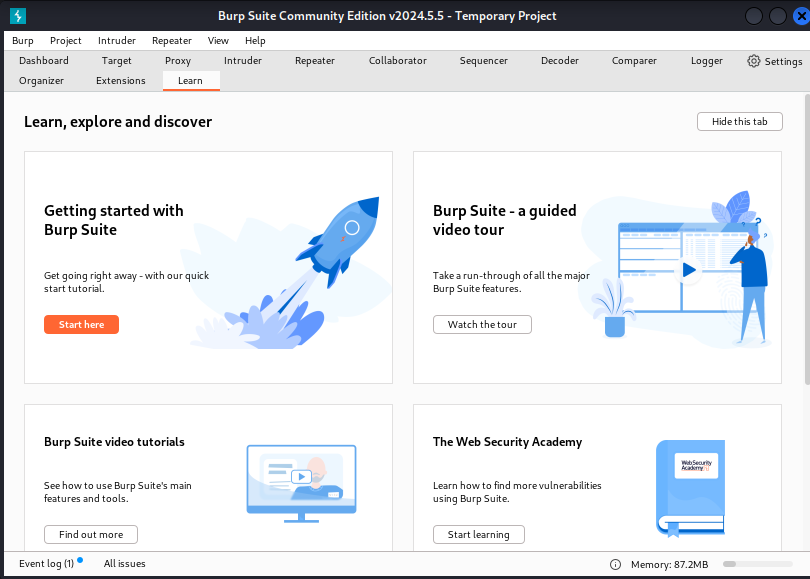


Рис. 3: Интерфейс Burp Suite

1. Во вкладке Proxy убедимся, что Intercept включен (рис. 4).

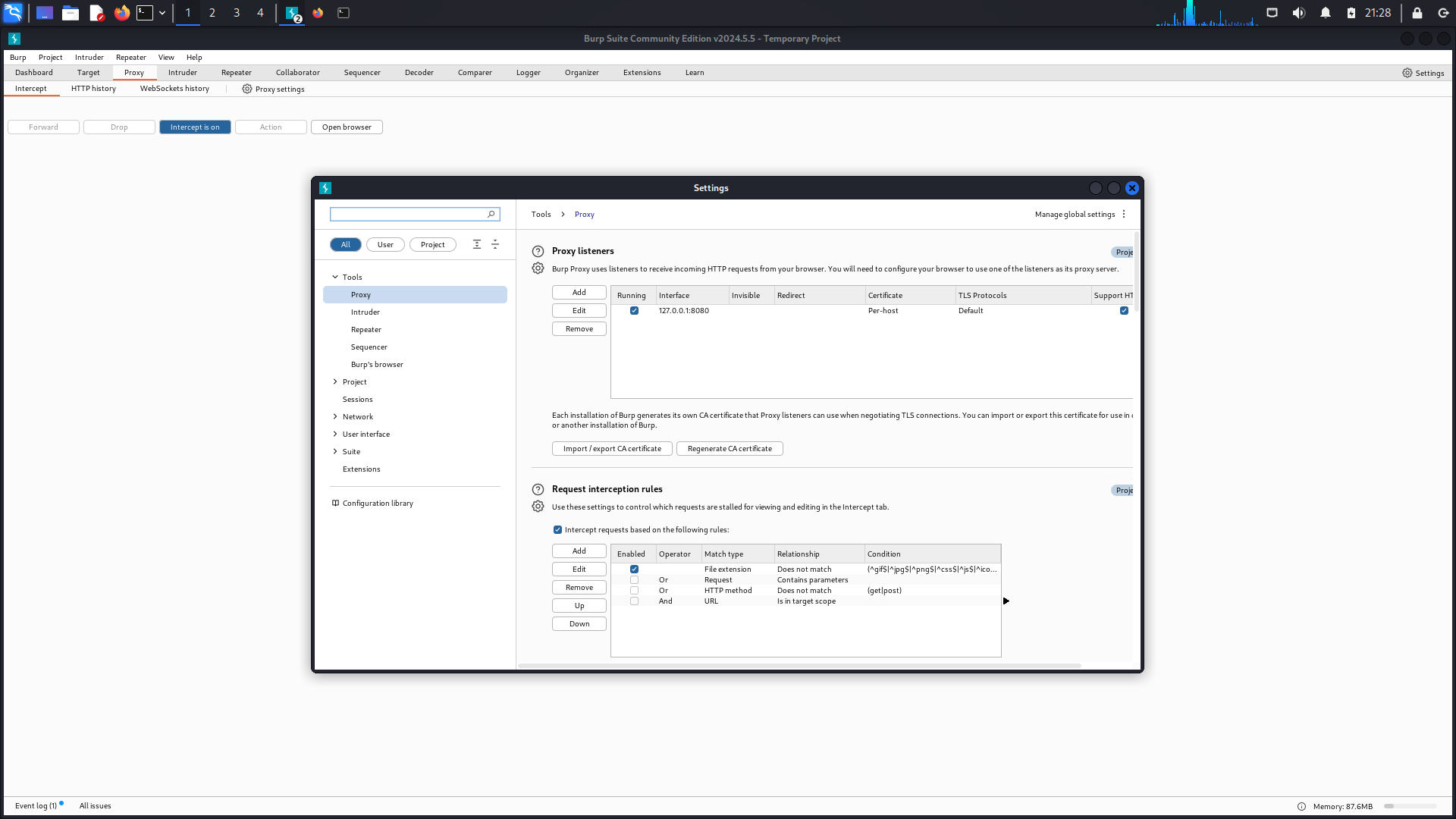


Рис. 4: Intercept is on

Далее в настройках браузера Mozilla устанавливаем Proxy на наш localhost 127.0.0.1 (рис. 5) и также устанавливаем параметр true на network.proxy.allow\_hijacking\_localhost (рис. 6).

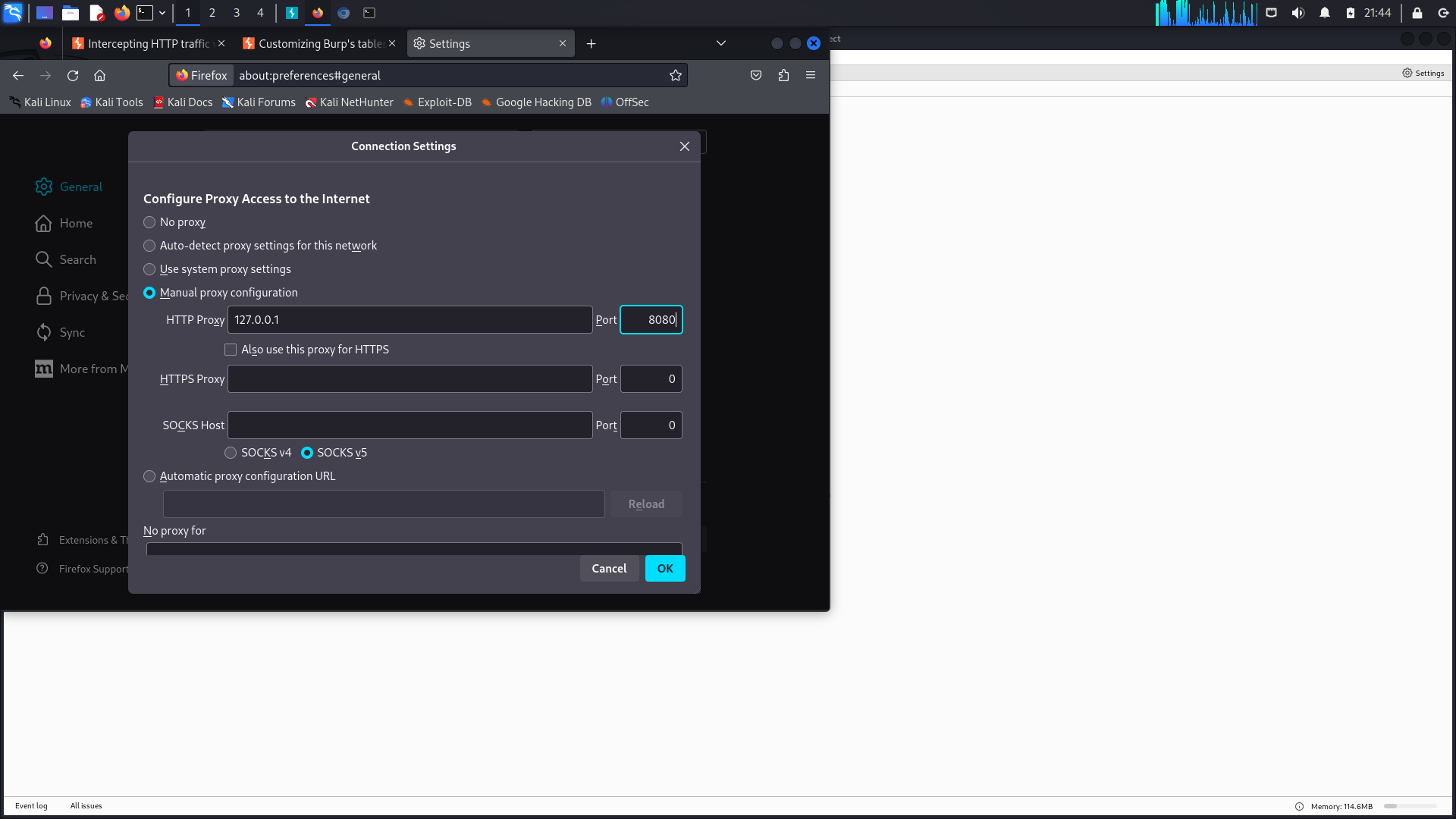


Рис. 5: Настройка Proxy

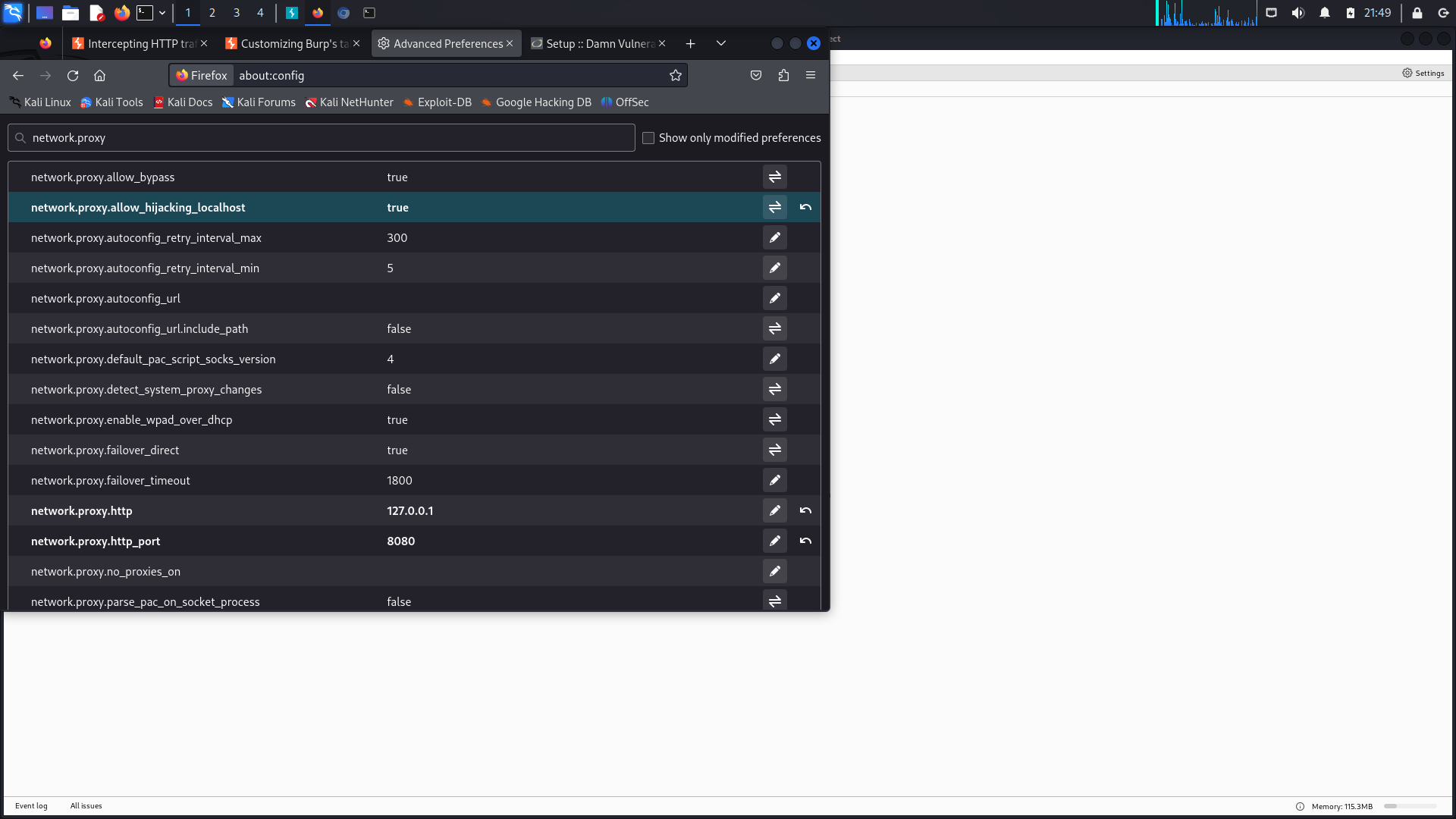


Рис. 6: network.proxy.allow\_hijacking\_localhost

1. Теперь пытаемся зайти на страницу входа DVWA и видим, что наш сигнал был перехвачен Burp Suite (рис. 7).

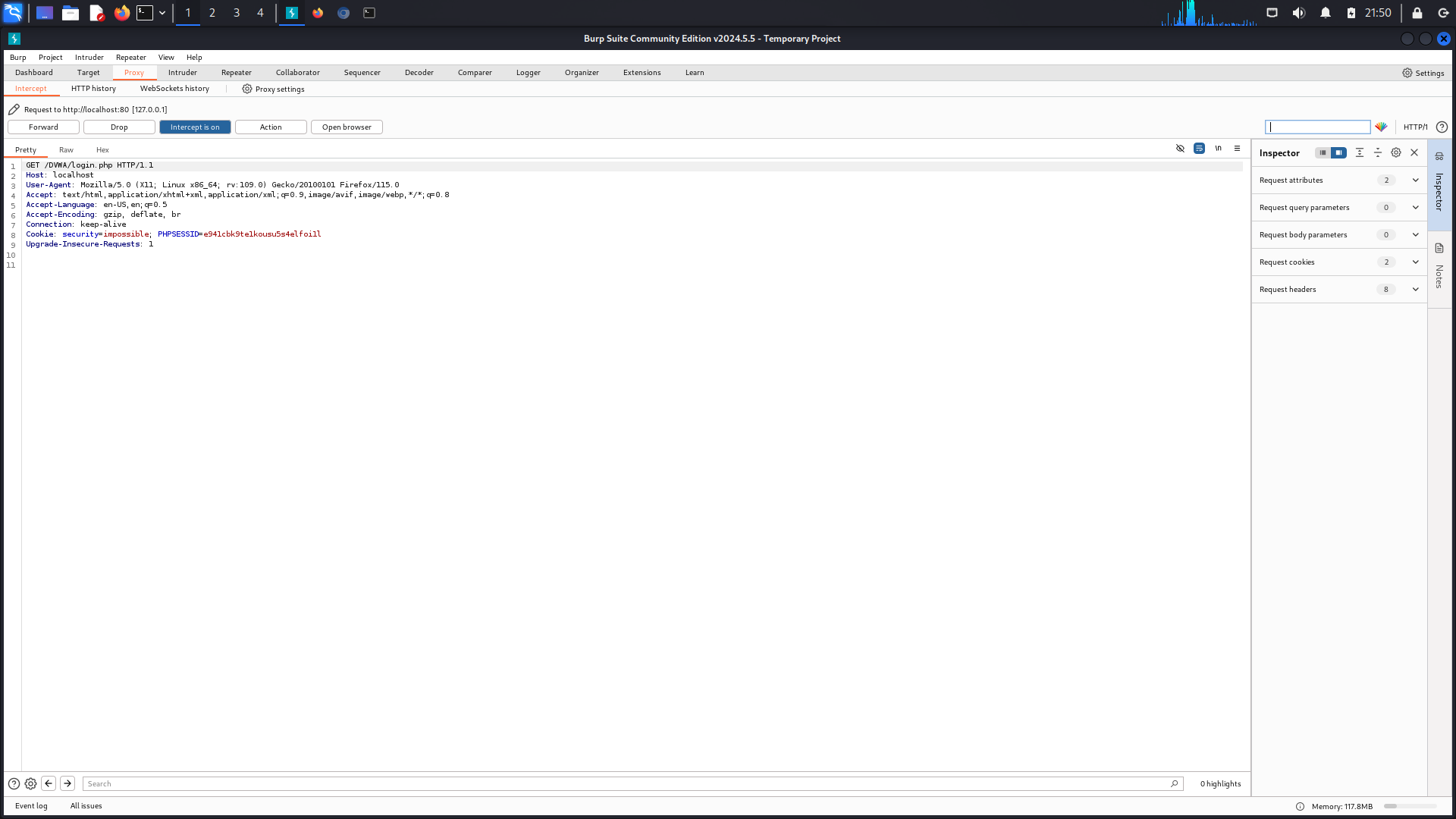


Рис. 7: Перехват сигнала

Нажимаем Forward и переходим на вкладку Target (рис. 8), 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 (рис. 9).

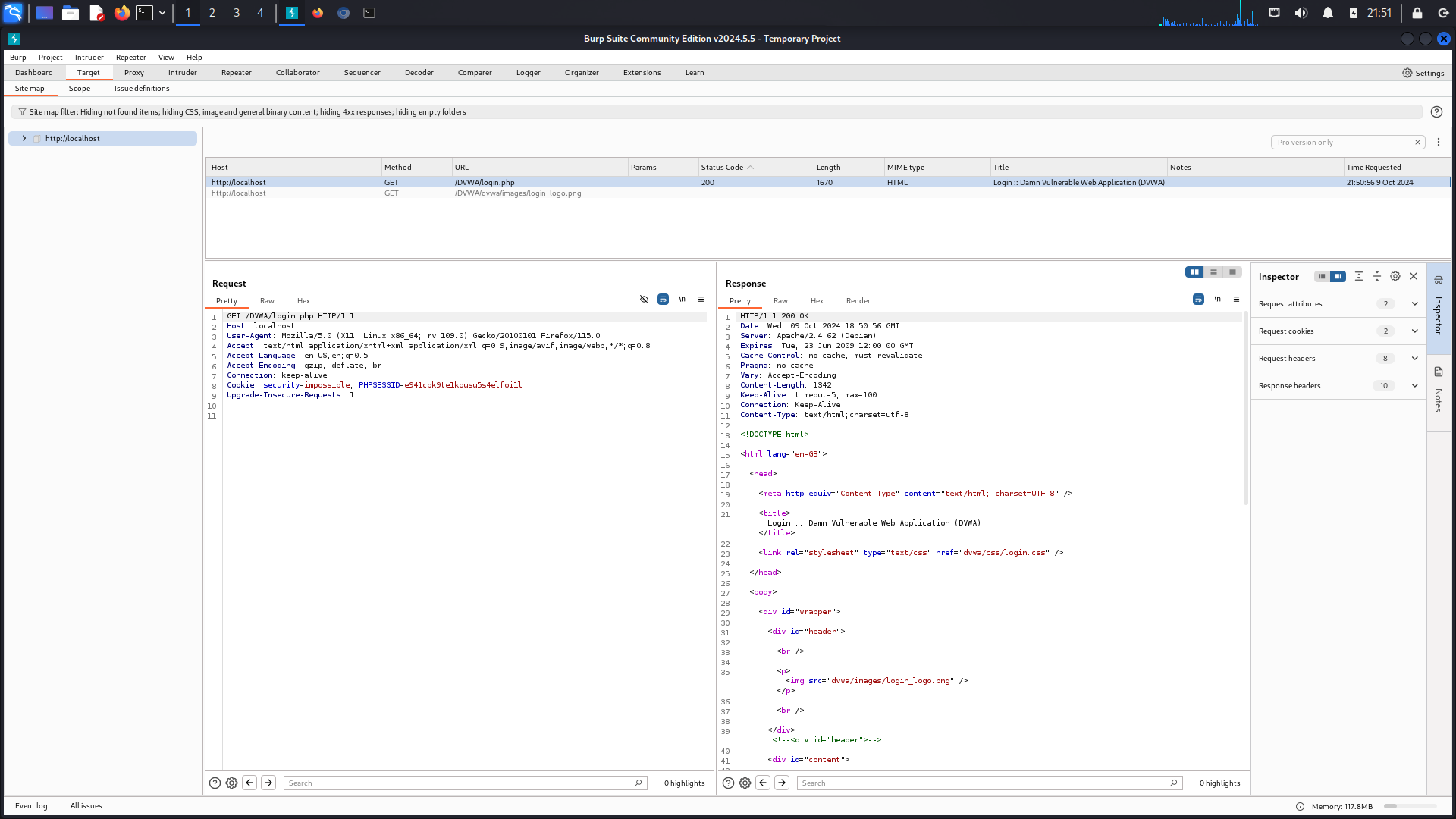


Рис. 8: Target

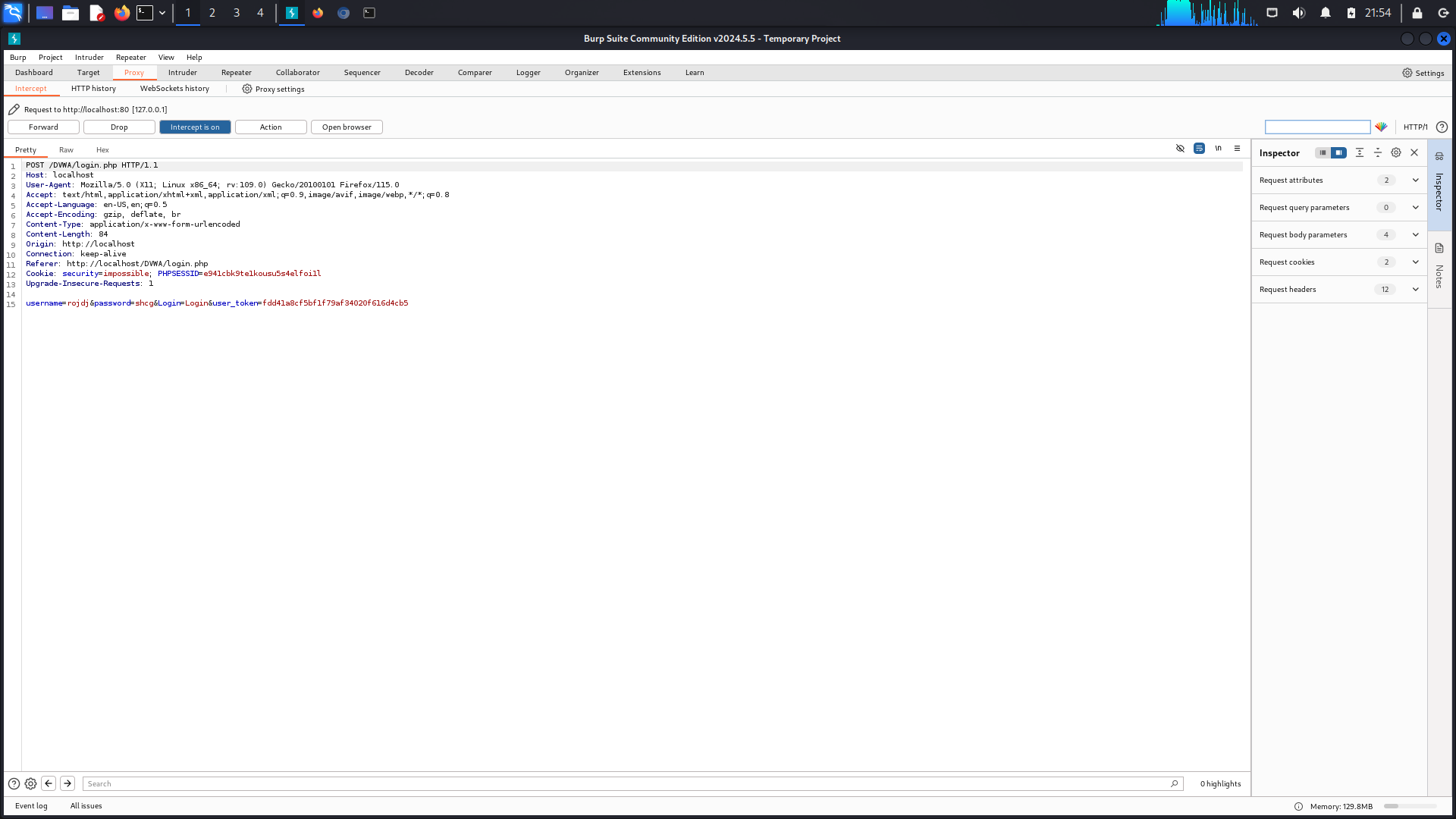


Рис. 9: Отслеживание запросов

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 (рис. 10).

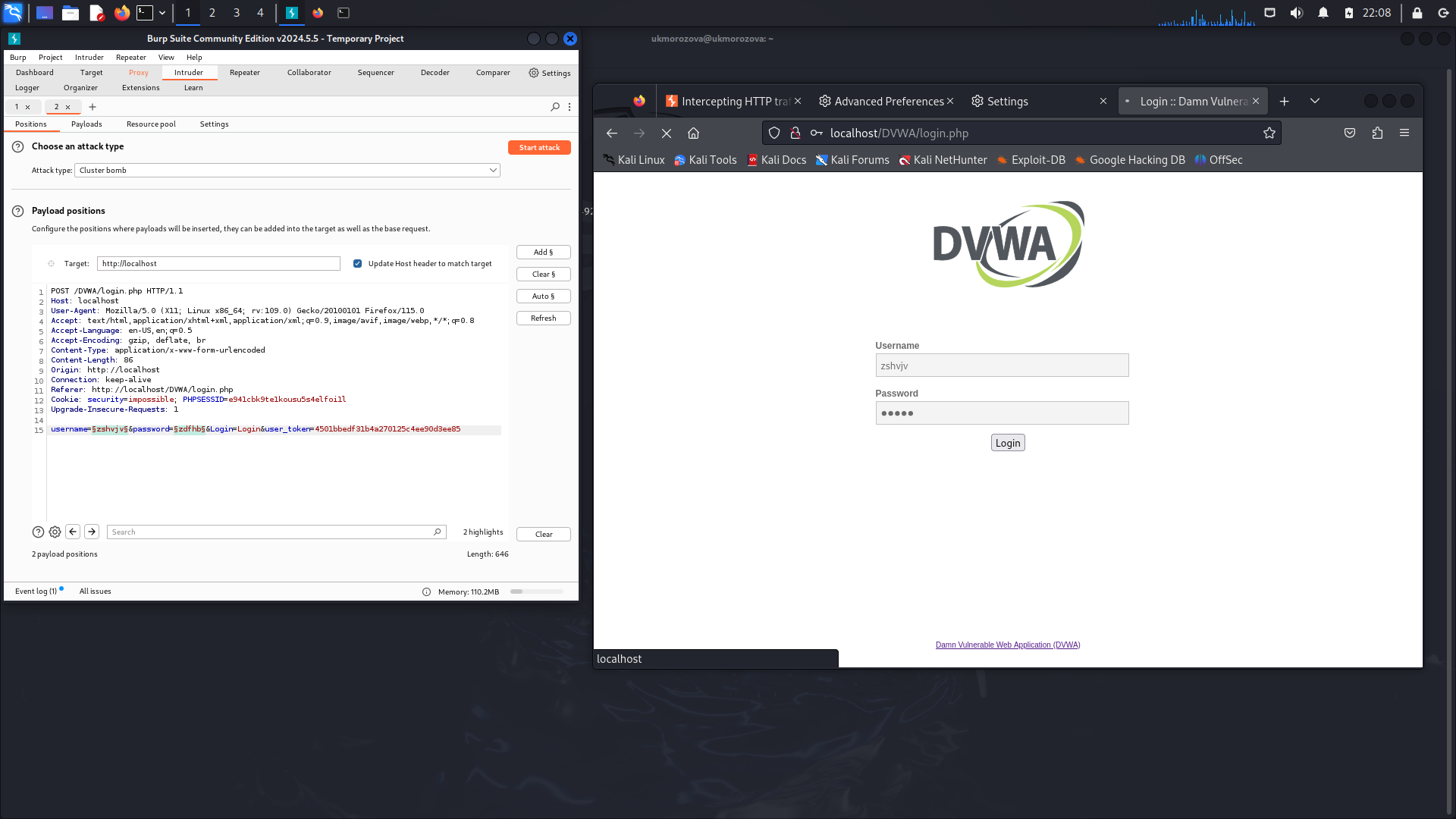


Рис. 10: Intruder

В Payloads заполняем случайными данные для подбора логина и пароля (рис. 11 - рис. 12)

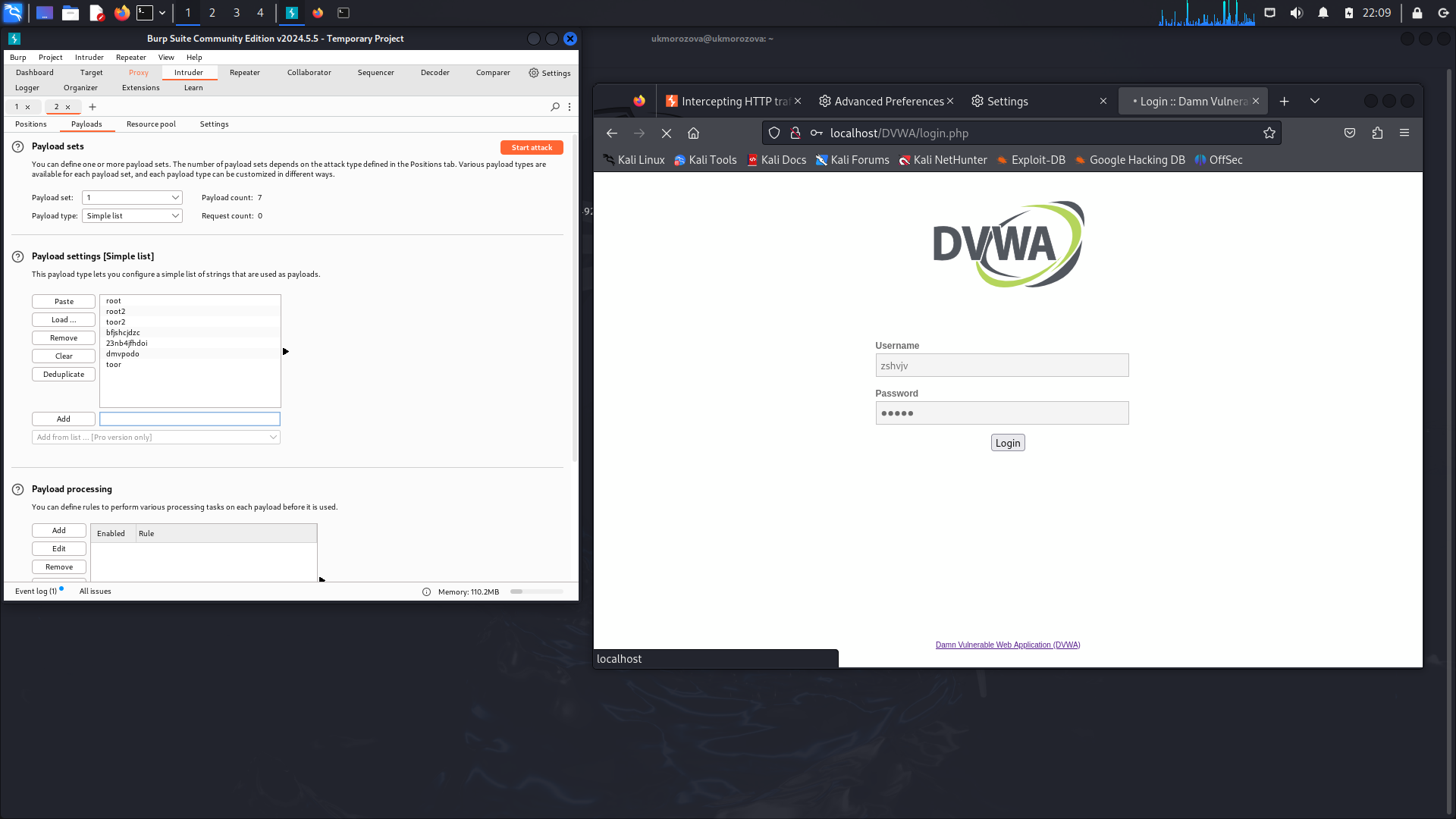


Рис. 11: Логин

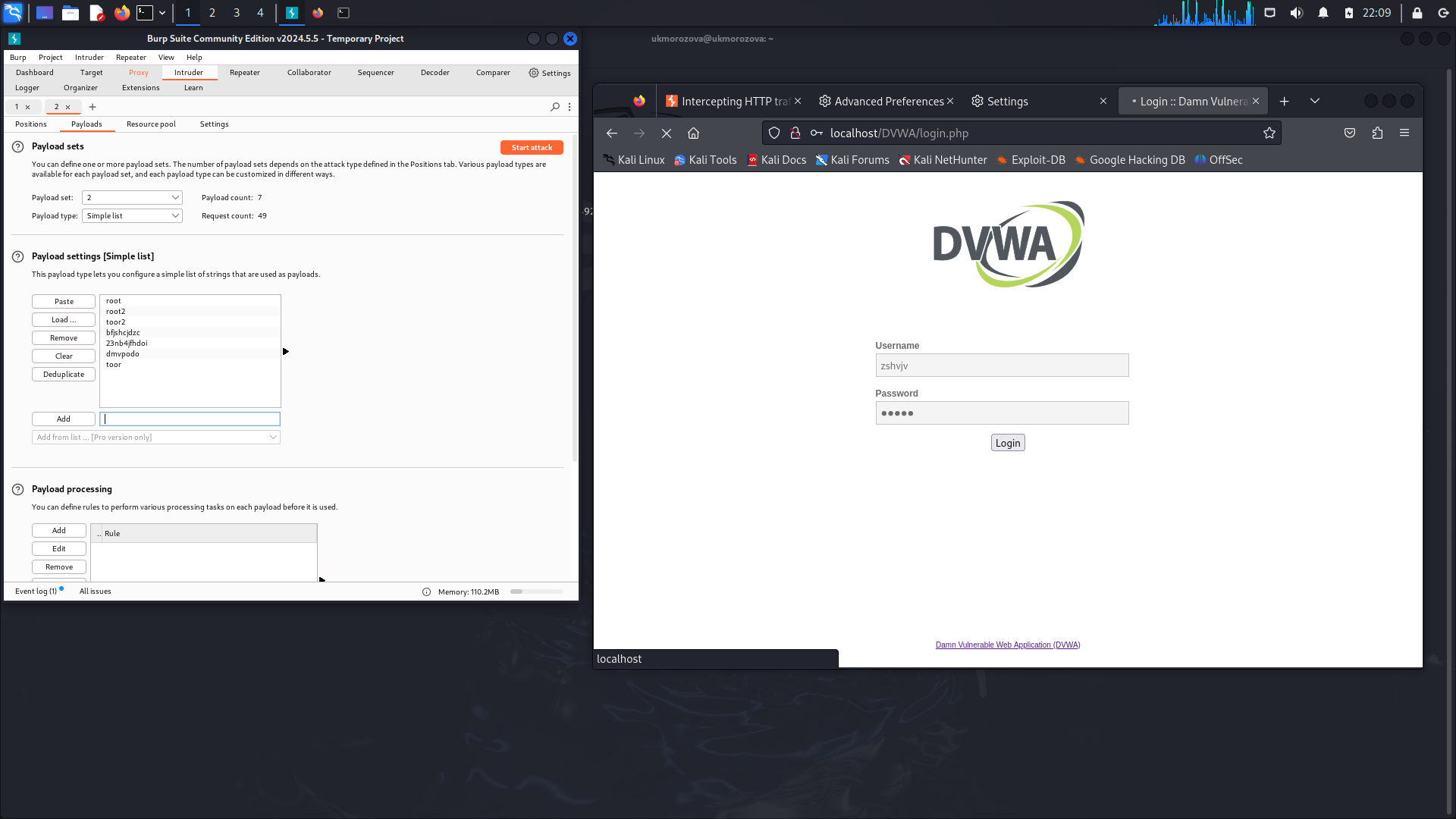


Рис. 12: Пароль

После нажатия кнопки Start Attack программа начинает перебирать всевозможные комбинации для входа (рис. 13). Находим единственно верную комбинацию и отправляем в Repeater (рис. 14) для повторной проверки и убеждаемся, что данные подходят (рис. 15).

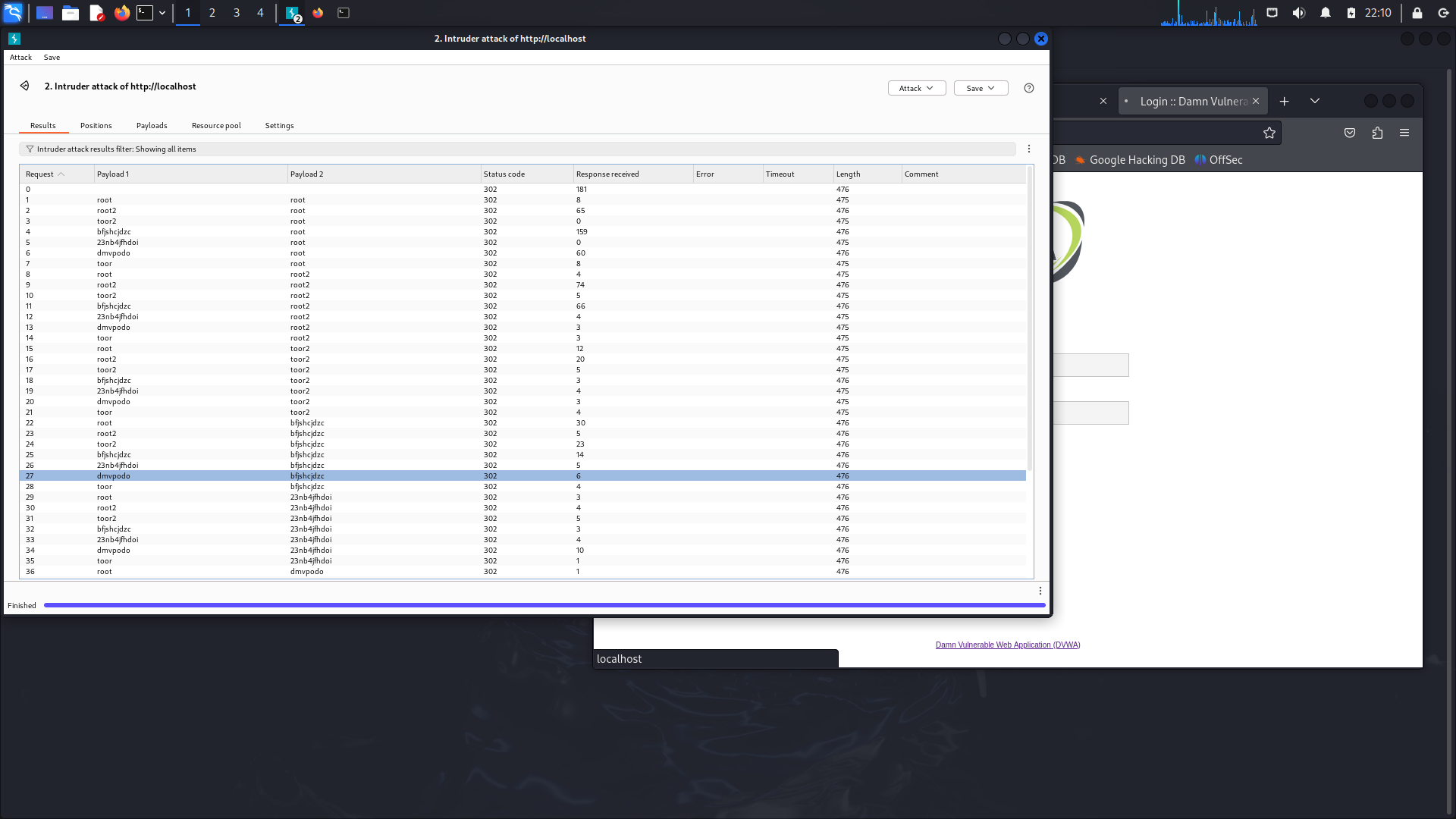


Рис. 13: Подбор пароля

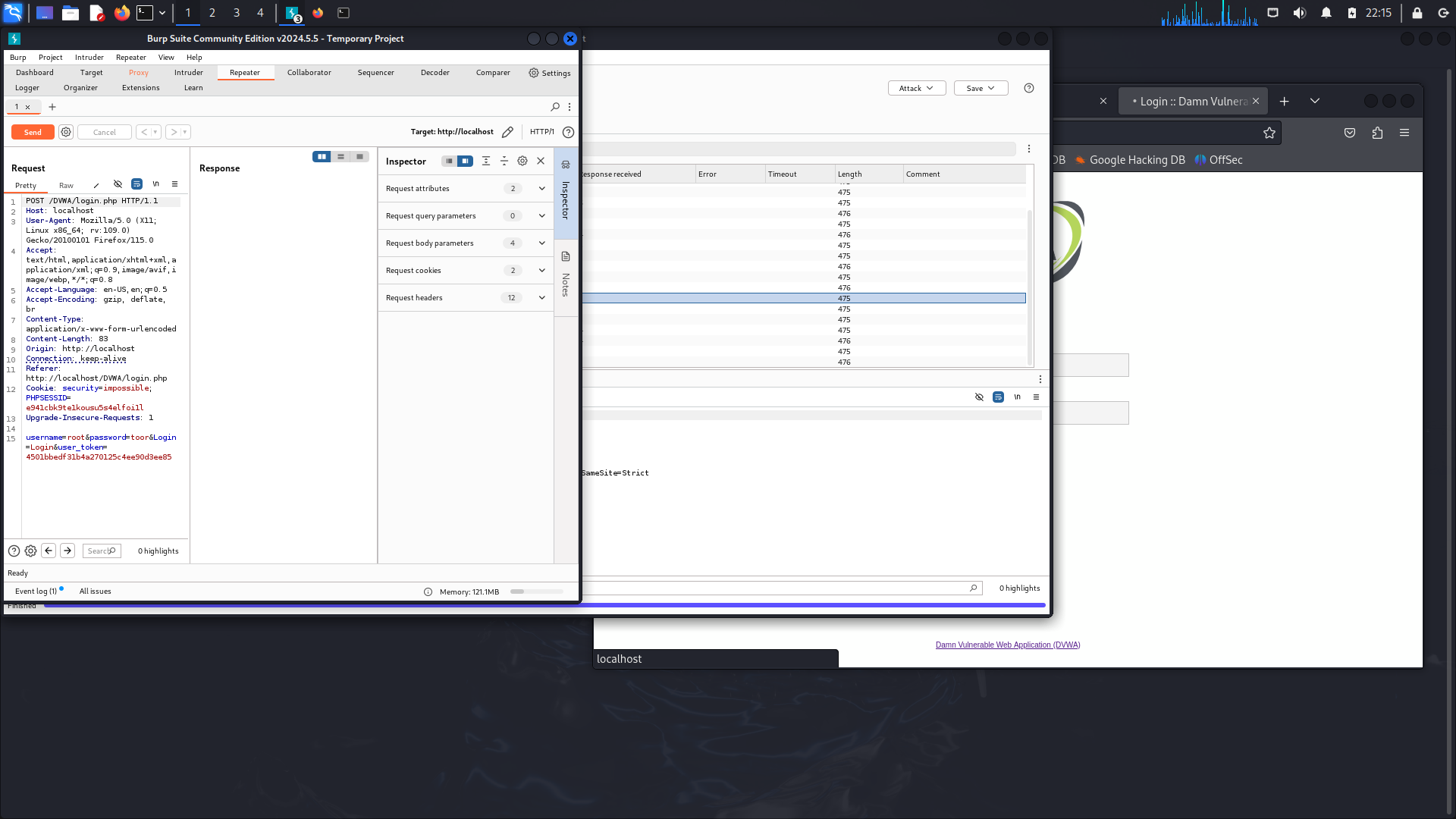


Рис. 14: Repeater

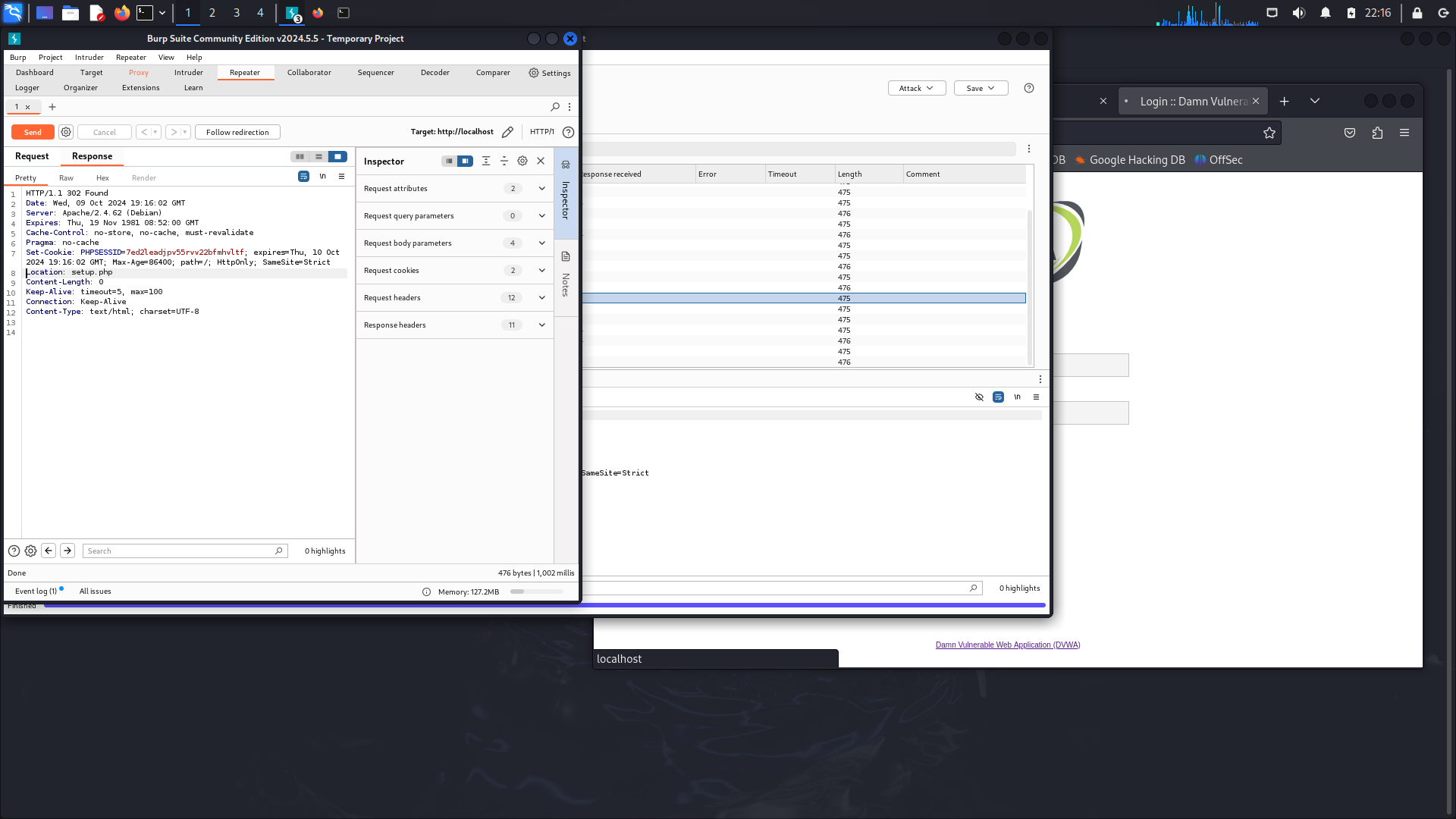


Рис. 15: Повторная проверка

Нажимаем на Follow redirection и получаем не скомпилированный html код в окне Response (рис. 16).

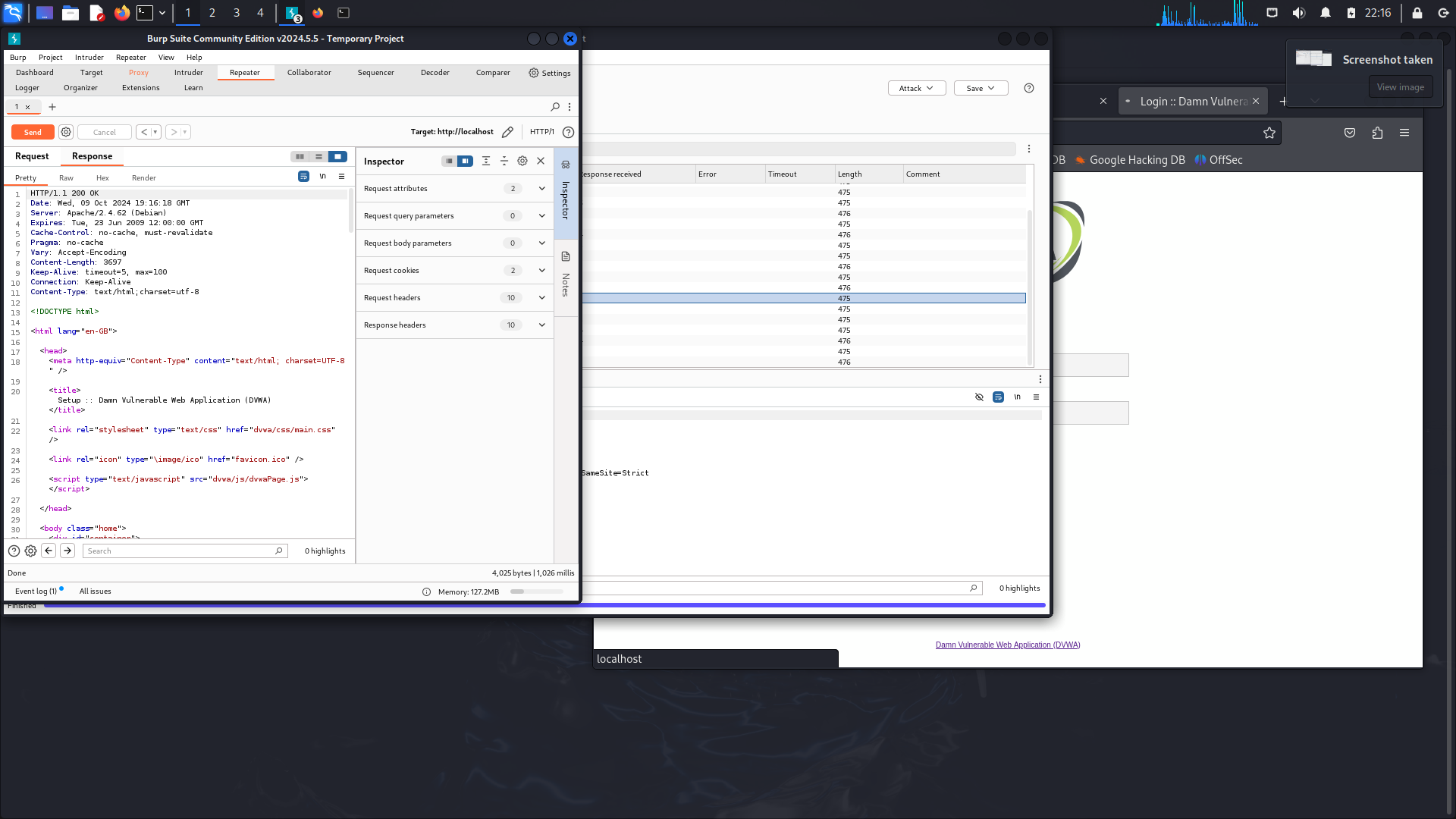


Рис. 16: HTML

В подокне Render получаем вид страницы в браузере (рис. 17).

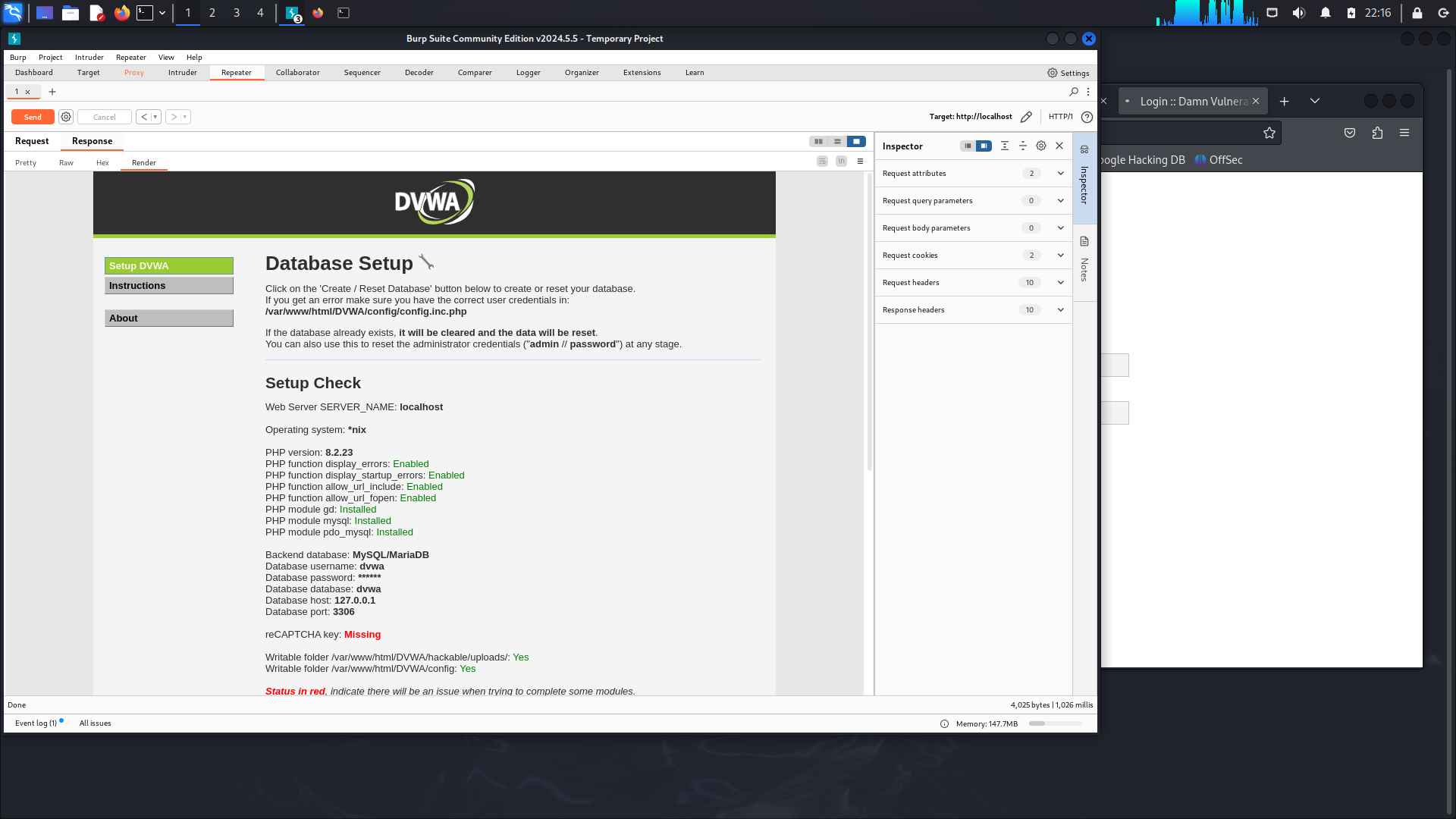


Рис. 17: DVWA

# 3 Выводы

Мы научились пользоваться Burp Suite.

# Список литературы