Отчёт по индивидуальному проекту. Этап №5

дисциплина: Информационная безопасность

Морозова Ульяна

Содержание

Список иллюстраций

1 Цель работы

Использование Burp Suite.

2 Выполнение лабораторной работы

1. Запустим необходимые для работы приложения такие, как Apache (рис. 2.1).

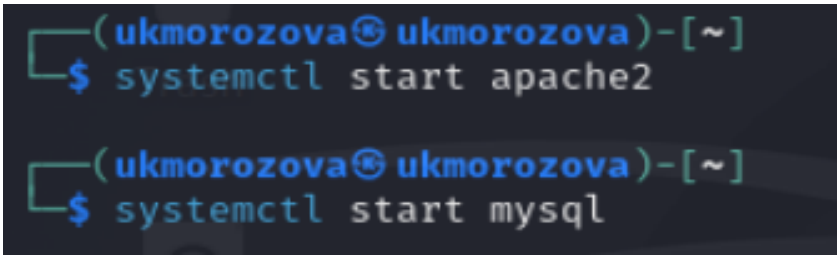

Рис. 2.1: Подготовительный этап

Запускаем Burp Suite через терминал (рис. 2.2 - рис. 2.3).

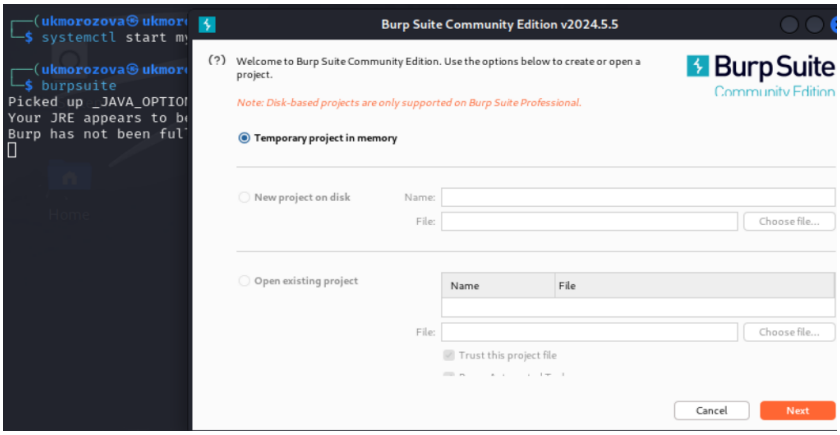

Рис. 2.2: Запуск Burp Suite

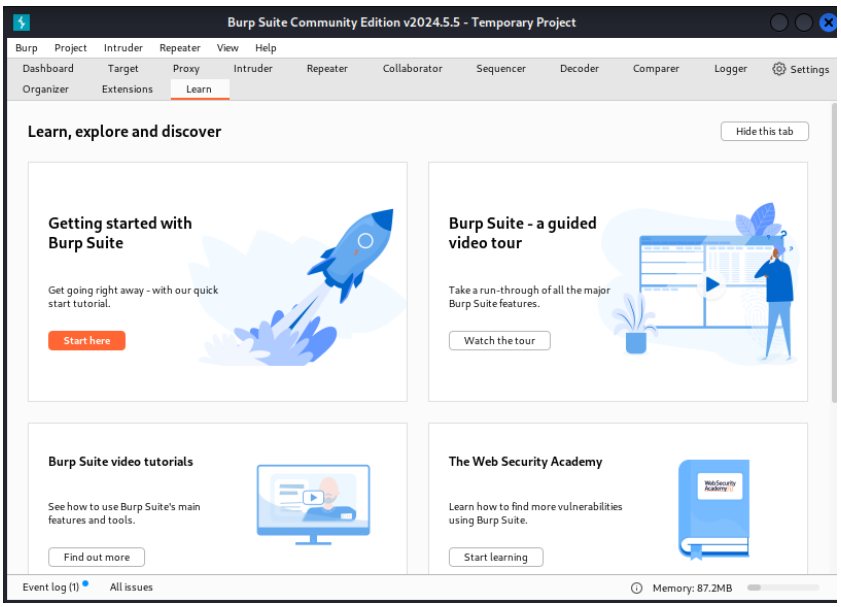

Рис. 2.3: Интерфейс Burp Suite

2. Во вкладке Proxy убедимся, что Intercept включен (рис. 2.4).

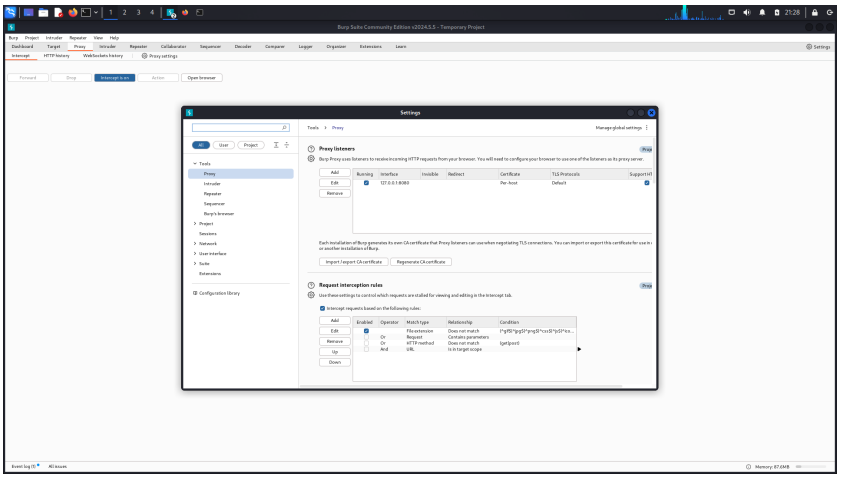

Рис. 2.4: Intercept is on

Далее в настройках браузера Mozilla устанавливаем Proxy на наш localhost 127.0.0.1 (рис. 2.5) и также устанавливаем параметр true на network.proxy.allow_hijacking_localho (рис. 2.6).

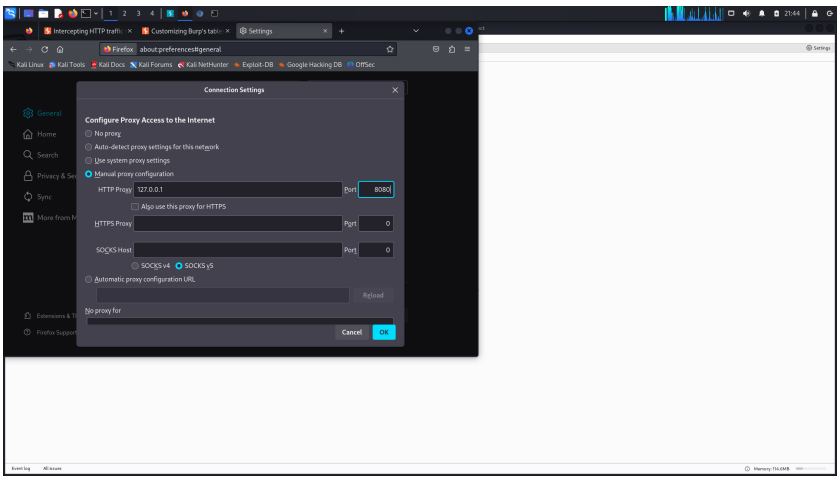

Рис. 2.5: Настройка Proxy

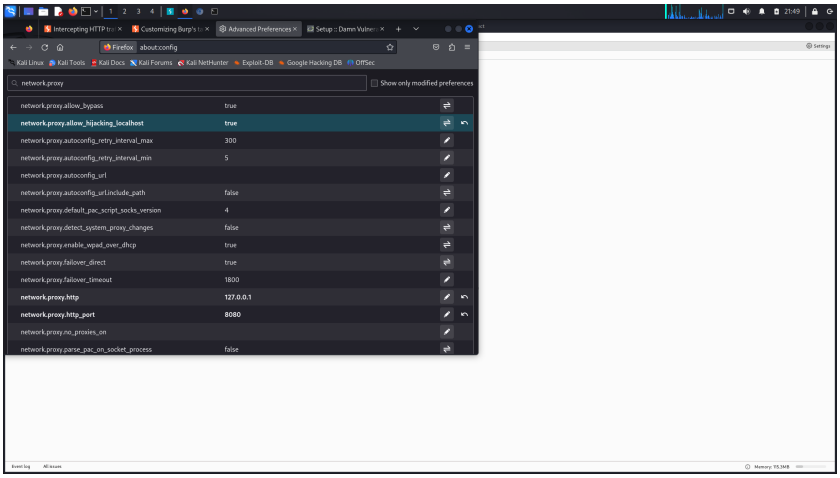

Рис. 2.6: network.proxy.allow_hijacking_localhost

3. Теперь пытаемся зайти на страницу входа DVWA и видим, что наш сигнал был перехвачен Burp Suite (рис. 2.7).

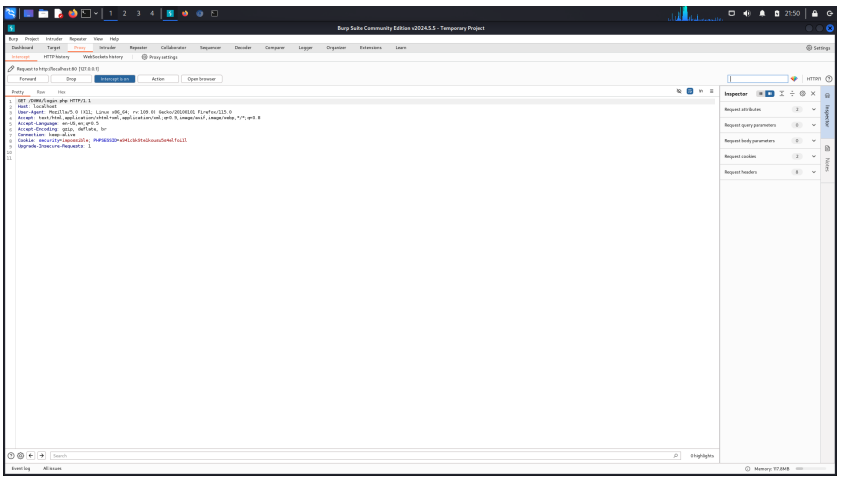

Рис. 2.7: Перехват сигнала

Нажимаем Forward и переходим на вкладку Target (рис. 2.8), 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. 2.9).

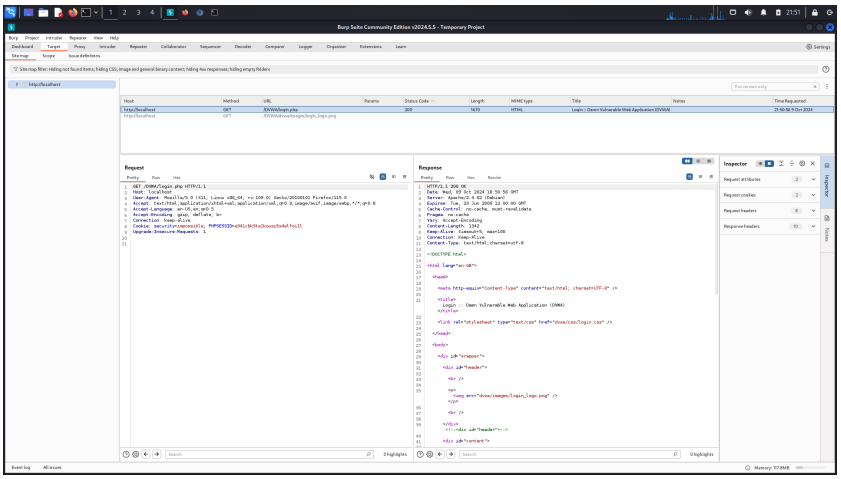

Рис. 2.8: Target

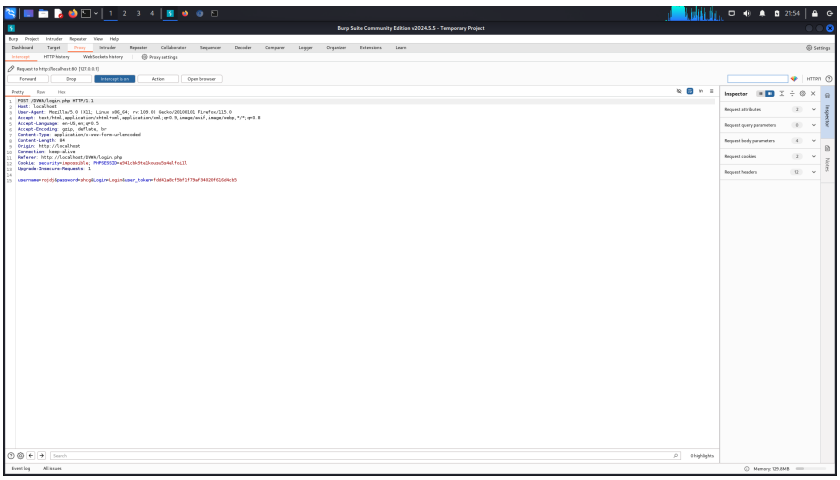

Рис. 2.9: Отслеживание запросов

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. 2.10).

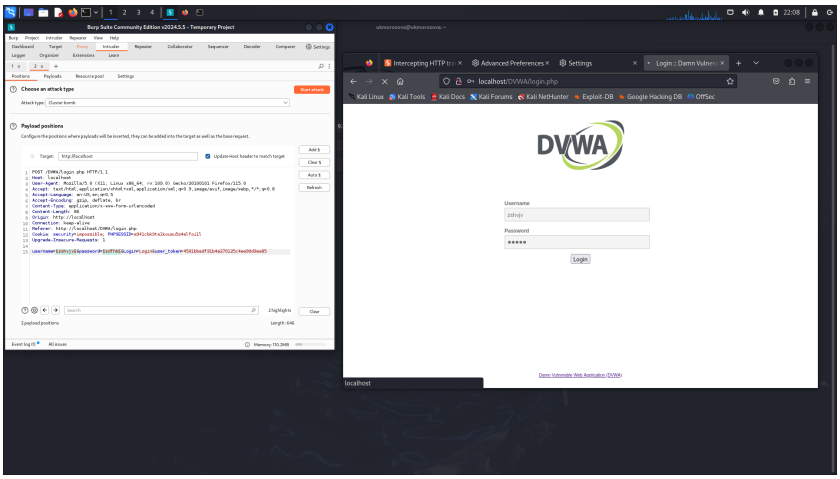

Рис. 2.10: Intruder

В Payloads заполняем случайными данные для подбора логина и пароля (рис. 2.11 - рис. 2.12)

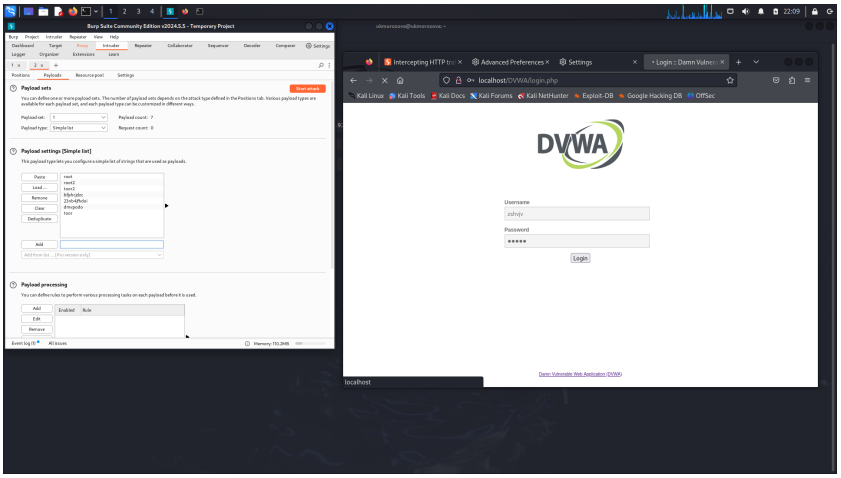

Рис. 2.11: Логин

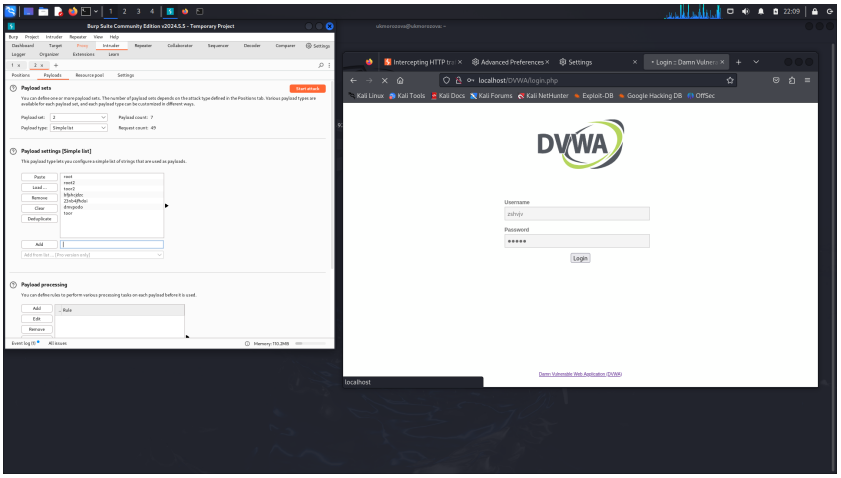

Рис. 2.12: Пароль

После нажатия кнопки Start Attack программа начинает перебирать всевозможные комбинации для входа (рис. 2.13). Находим единственно верную комбинацию и отправляем в Repeater (рис. 2.14) для повторной проверки и убеждаемся, что данные подходят (рис. 2.15).

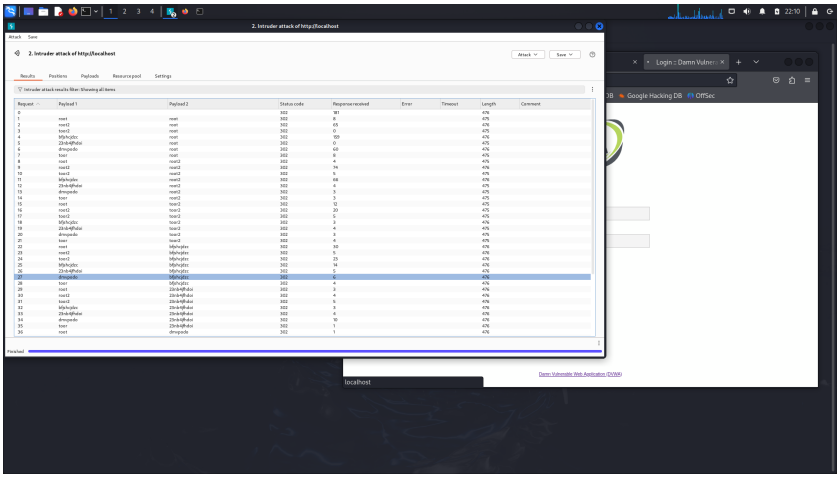

Рис. 2.13: Подбор пароля

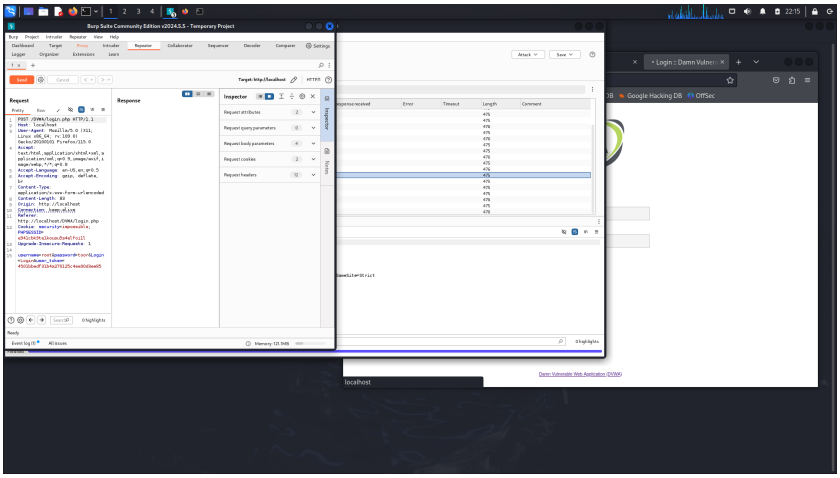

Рис. 2.14: Repeater

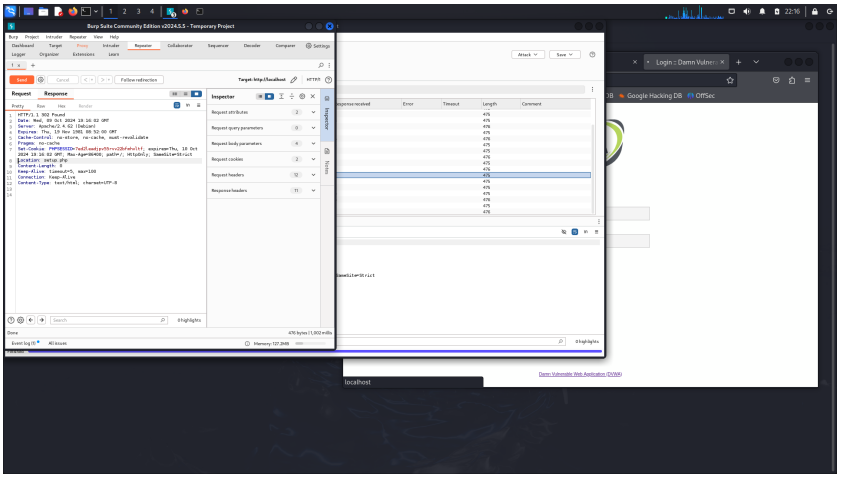

Рис. 2.15: Повторная проверка

Нажимаем на Follow redirection и получаем не скомпилированный html код в окне Response (рис. 2.16).

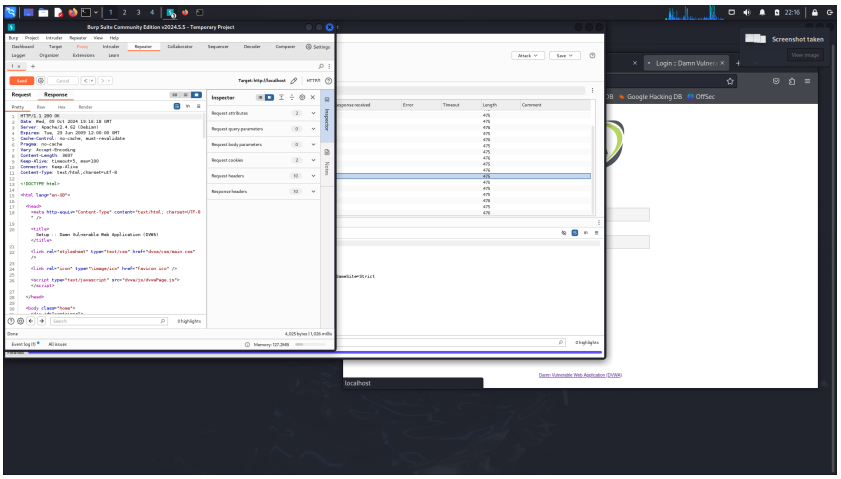

Рис. 2.16: HTML

В подокне Render получаем вид страницы в браузере (рис. 2.17).

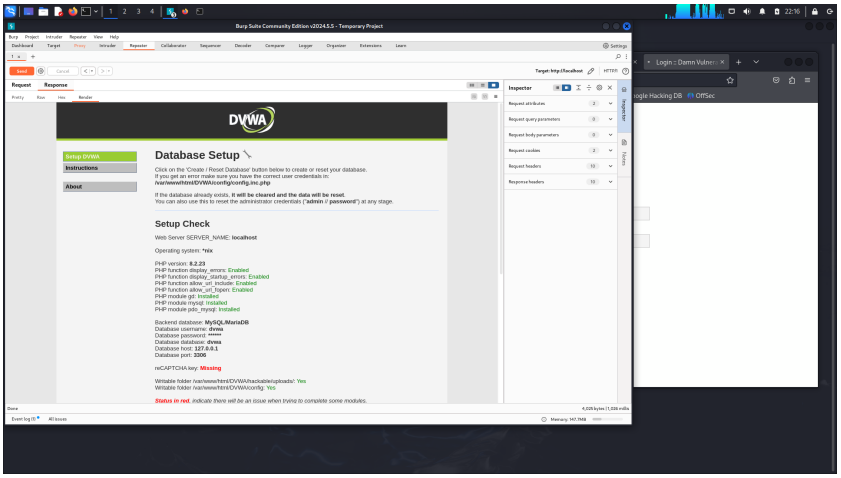
Burp Suite Community Edition v2024.5.5 - Temporary Project
DVWA
Database Setup
Setup DVWA
Instructions
About
Setup Check

Рис. 2.17: DVWA

3 Выводы

Мы научились пользоваться Burp Suite.