Отчёт по этапу №5 индивидуального проекта

Основы информационной безопасности

Мурашов Иван Вячеславович

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Научиться использовать Burp Suite.

# 2 Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений. [**parasram?**].

# 3 Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. 1).

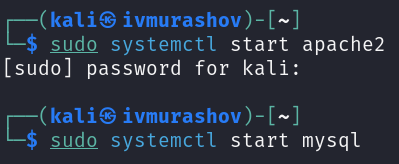


Рис. 1: Запуск локального сервера

Запускаю инструмент Burp Suite (рис. 2).

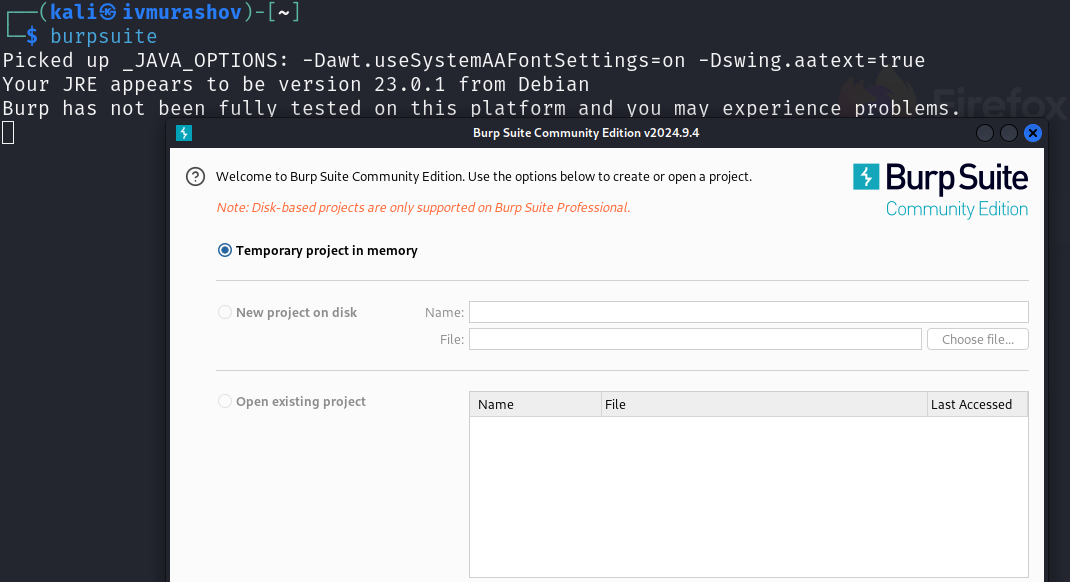


Рис. 2: Запуск приложения

Открываю сетевые настройки браузера, для подготовке к работе (рис. 3).

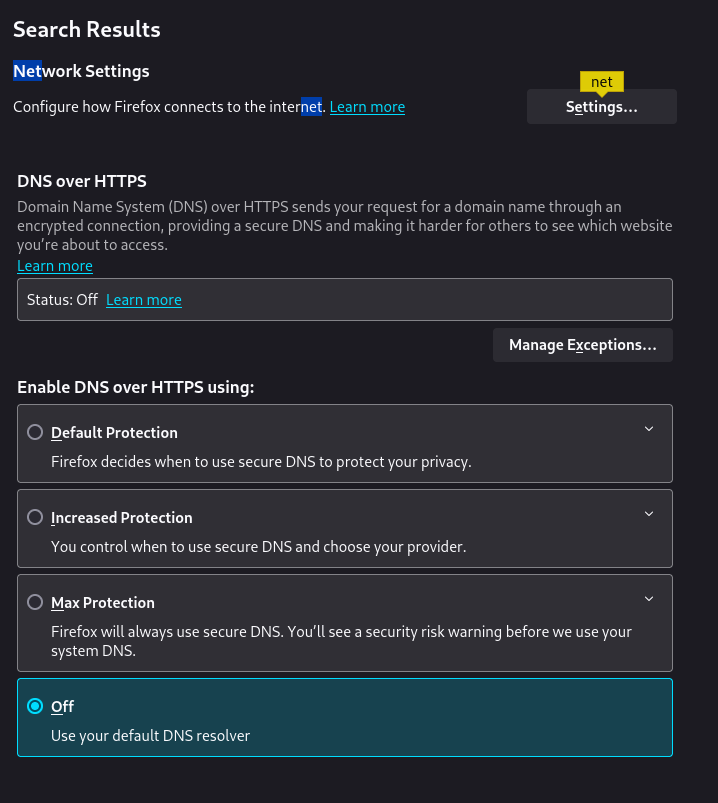


Рис. 3: Сетевые настройки браузера

Изменение настроек сервера для работы с proxy и захватом данных с помощью Burp Suite (рис. 4).

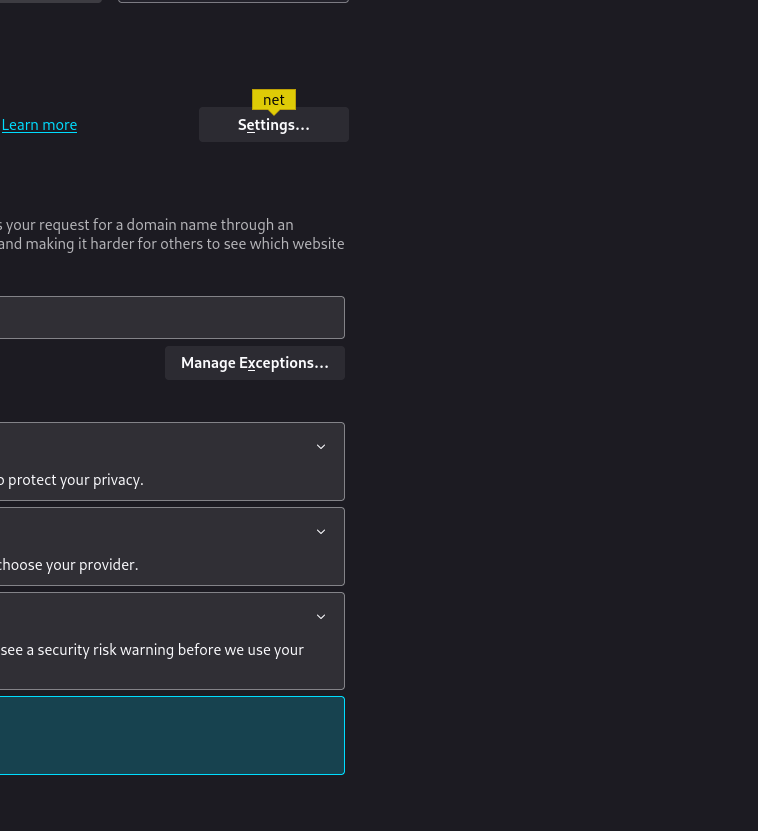


Рис. 4: Настройки сервера

Изменяю настройки Proxy инструмента Burp Suite для дальнейшей работы (рис. 5).

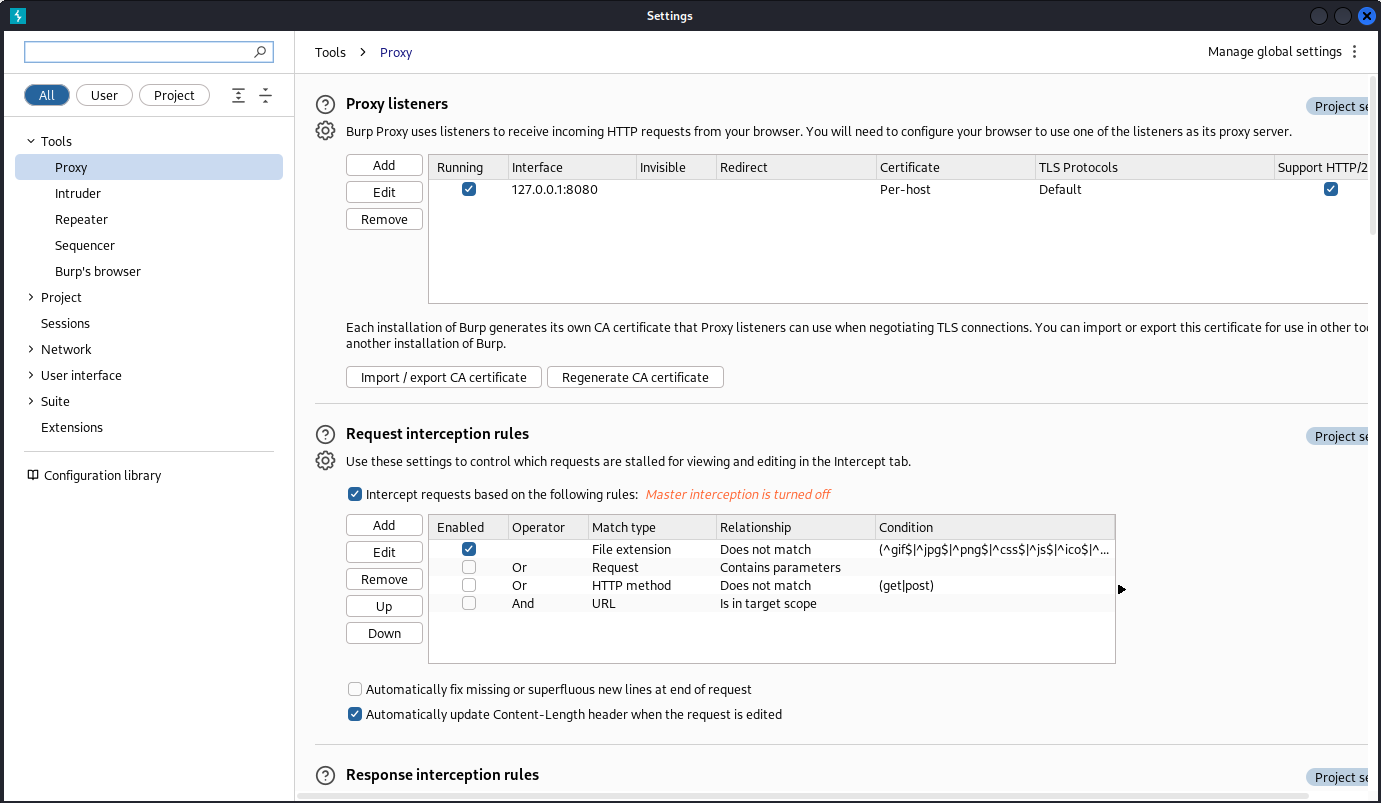


Рис. 5: Настройки Burp Suite

Во вкладке Proxy устанавливаю “Intercept is on” (рис. 6).

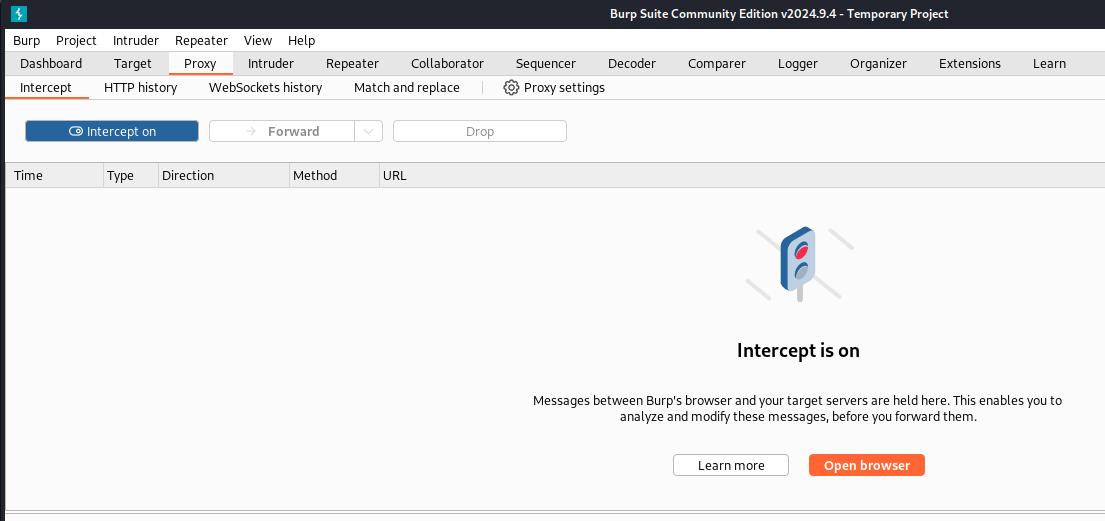


Рис. 6: Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, наобходимо установить параметр network\_allow\_hijacking\_loacalhost на true (рис. 7).

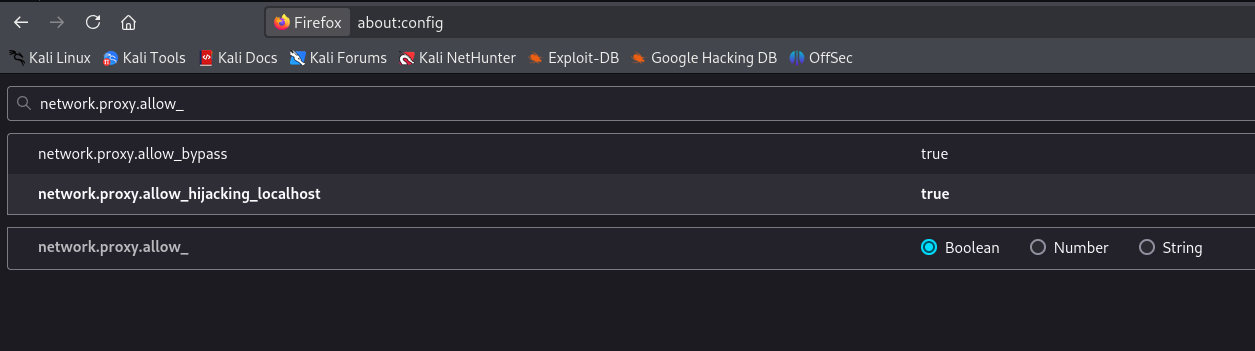


Рис. 7: Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. 8).

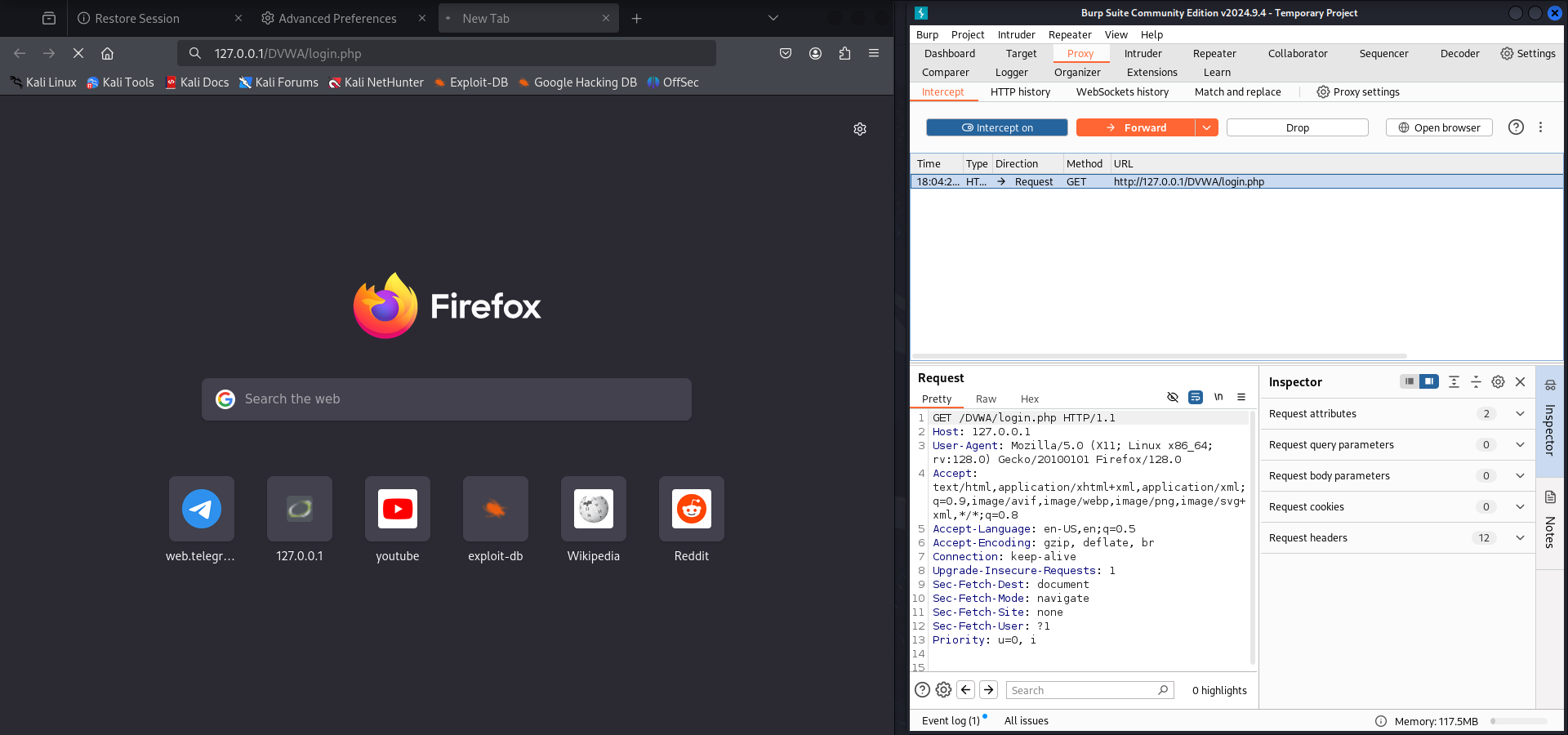


Рис. 8: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. 9).

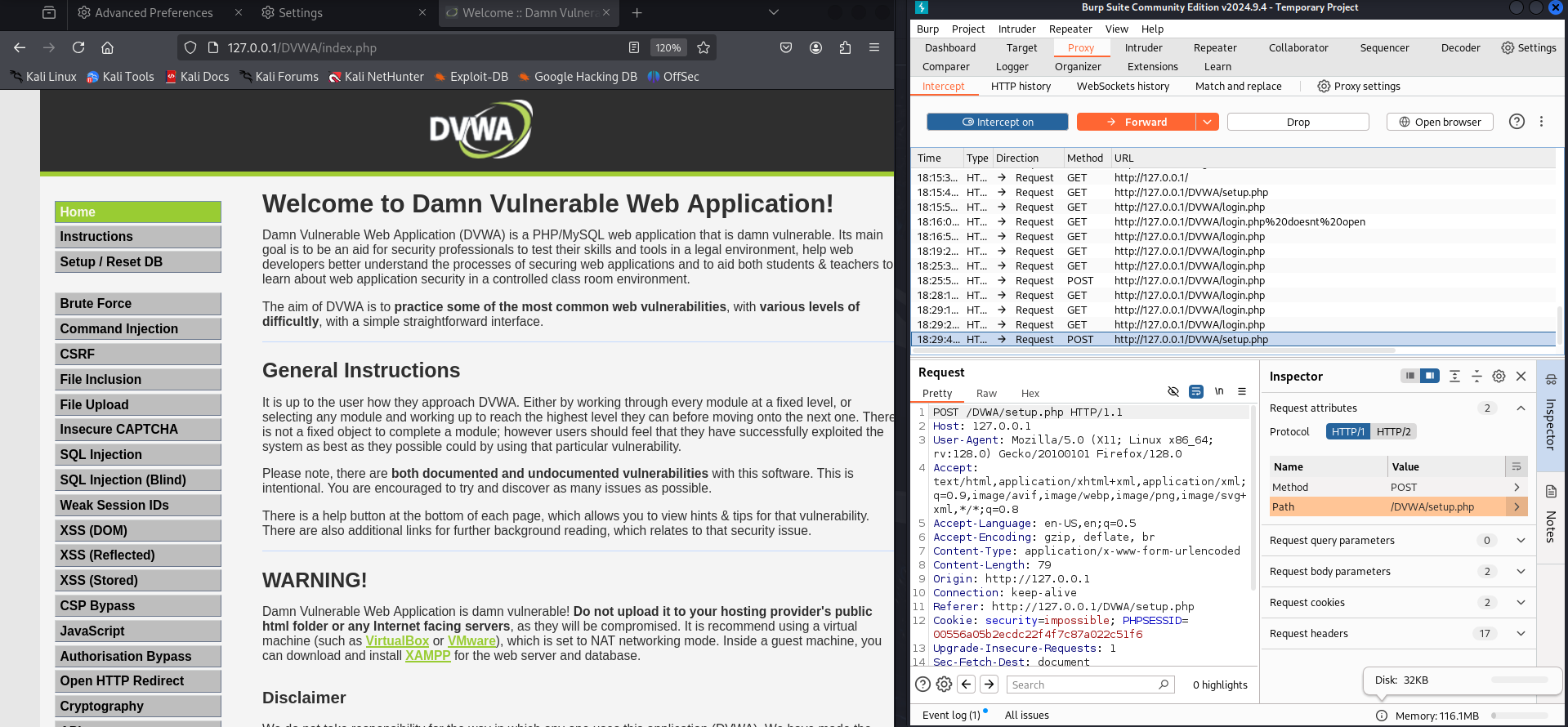


Рис. 9: Страница авторизации

История запросов хранится во вкладке Target (рис. 10).

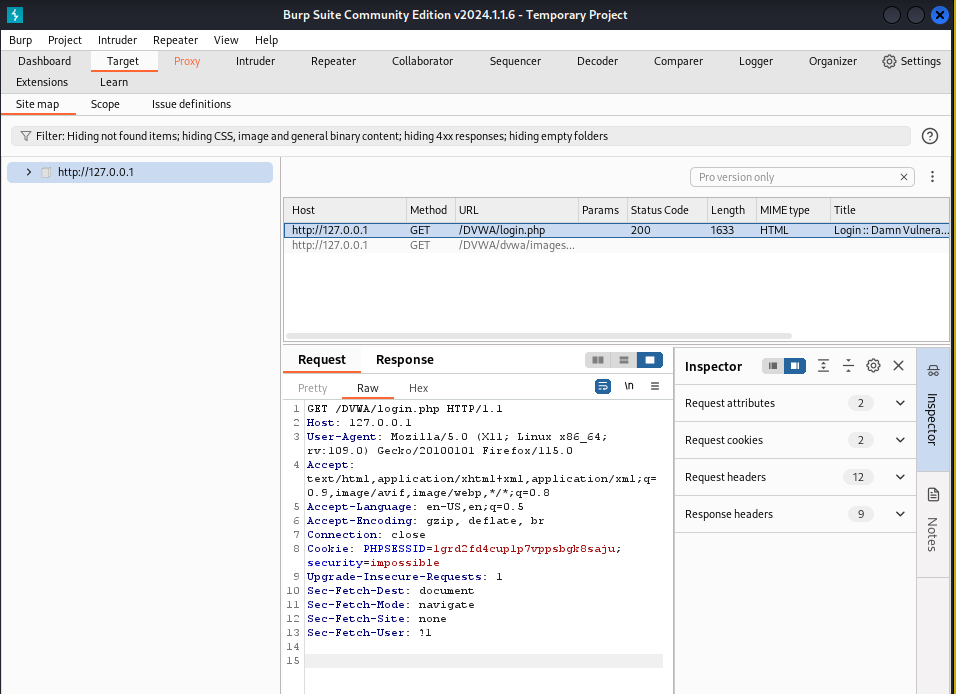


Рис. 10: История запросов

Попробуем ввести неправильные, случайные данные в веб-приложении и нажмем Login. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода (рис. 11).

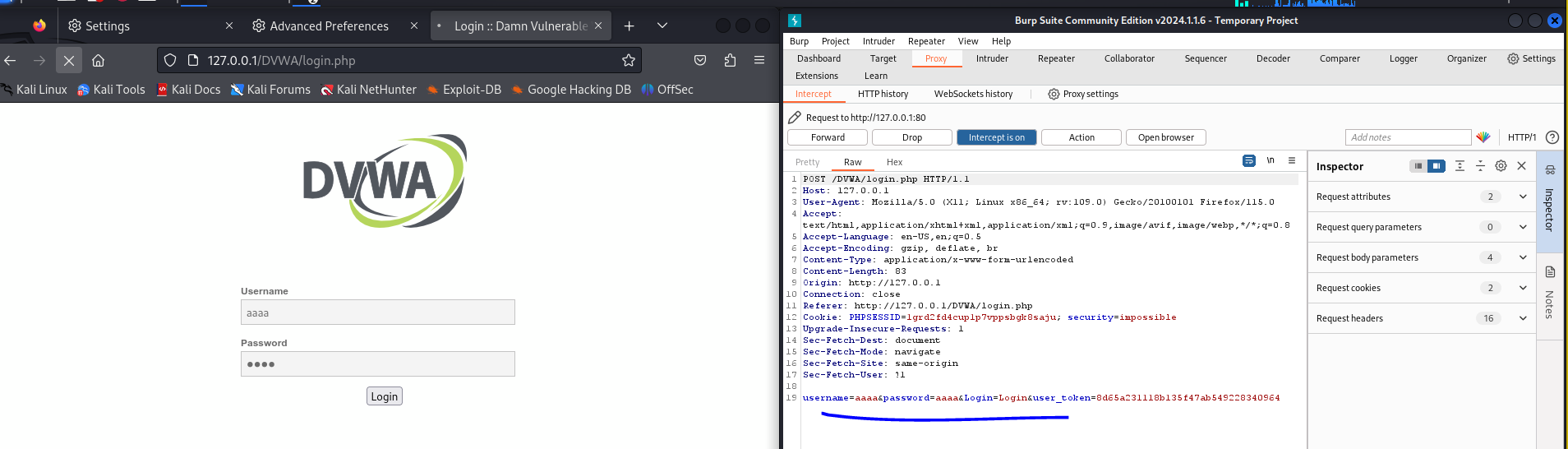


Рис. 11: Ввод случайных данных

Этот запрос так же можно найти во вкладке Target, там же жмем правой кнопкой мыши на хост нужного запроса, и далее нажимаем “Send to Intruder” (рис. 12).

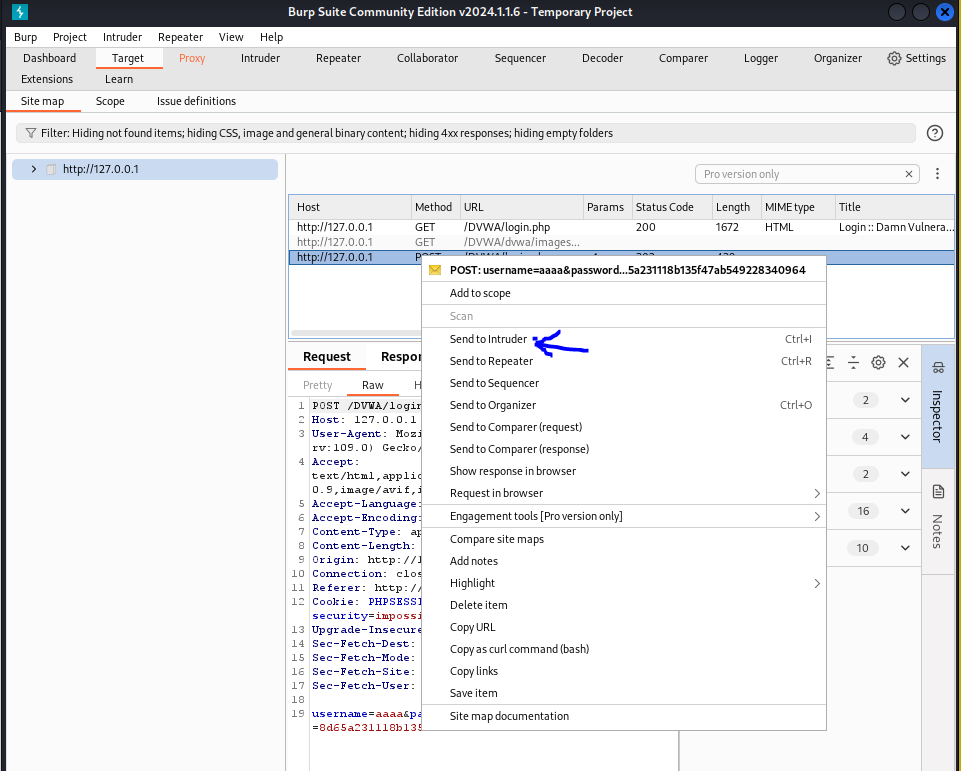


Рис. 12: POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. 13).

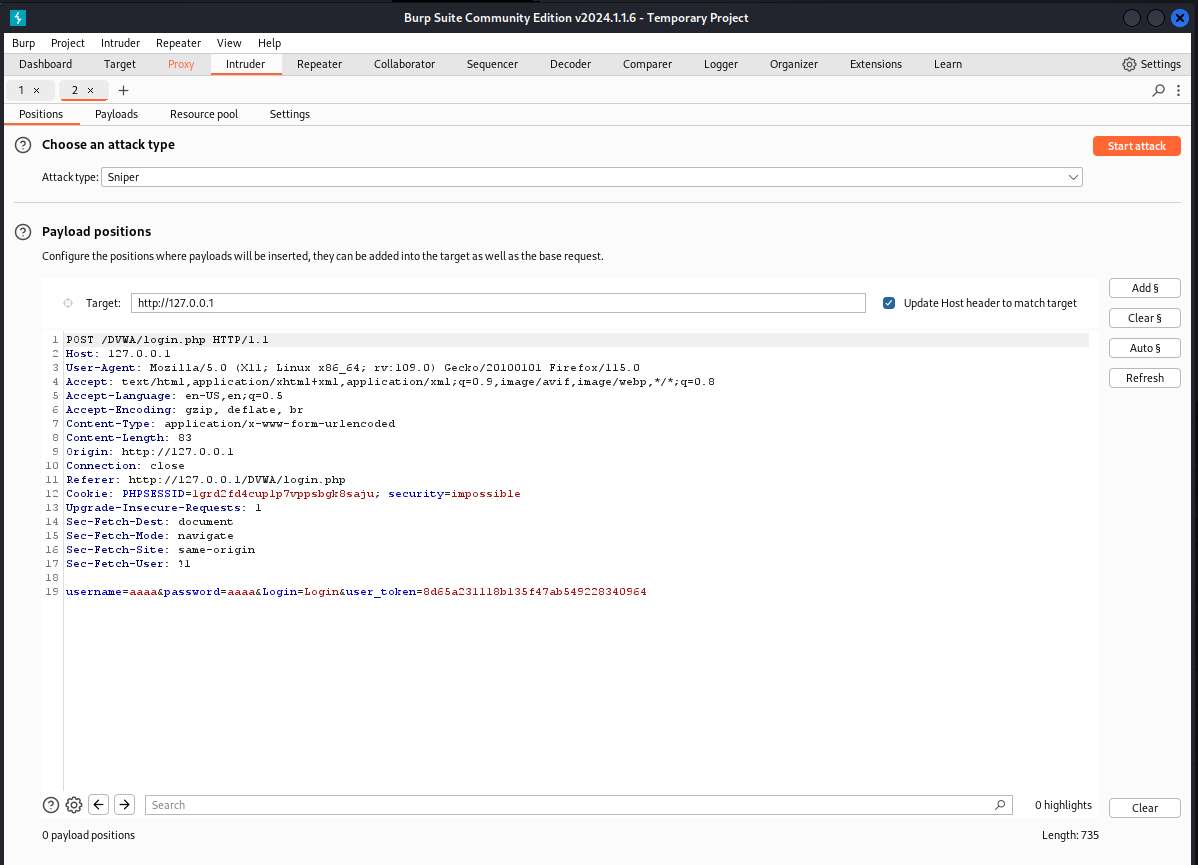


Рис. 13: Вкладка Intruder

Изменяем значение типа атаки на Cluster bomb и проставляем специальные символы у тех данных в форме для ввода, которые будем пробивать, то есть у имени пользователя и пароля (рис. 14).

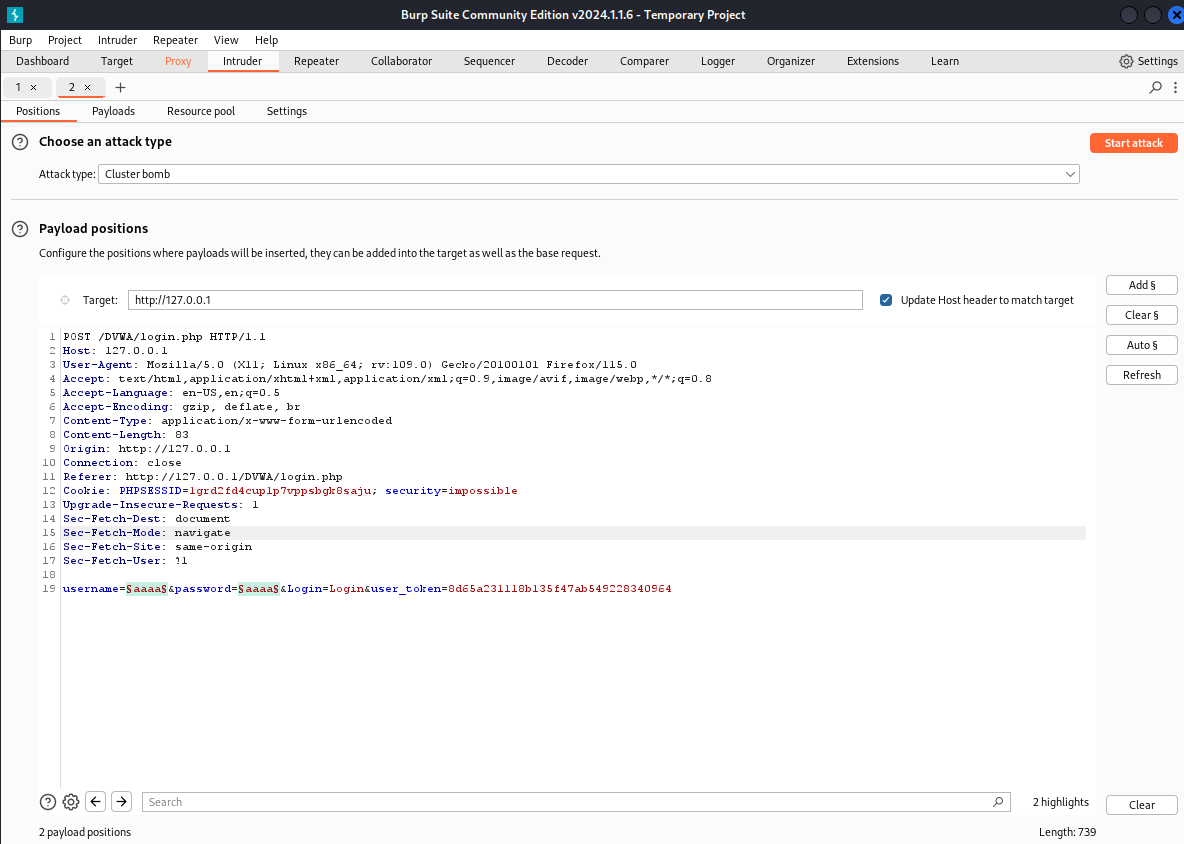


Рис. 14: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. 15).

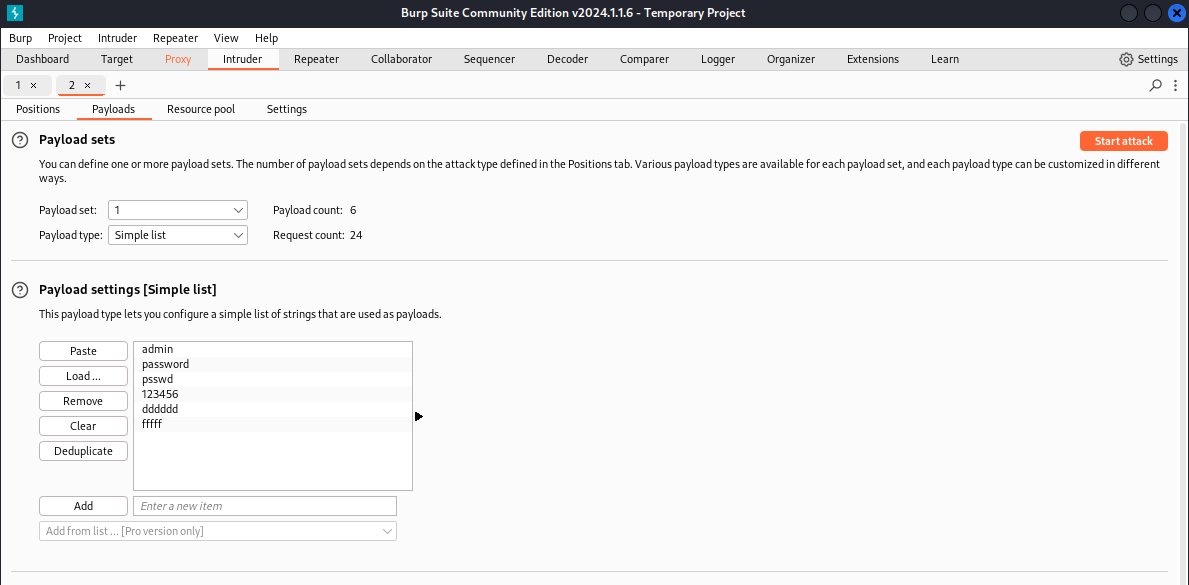


Рис. 15: Первый Simple list

Переключаемся на второй список и добавляем значения в него. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль (рис. 16).

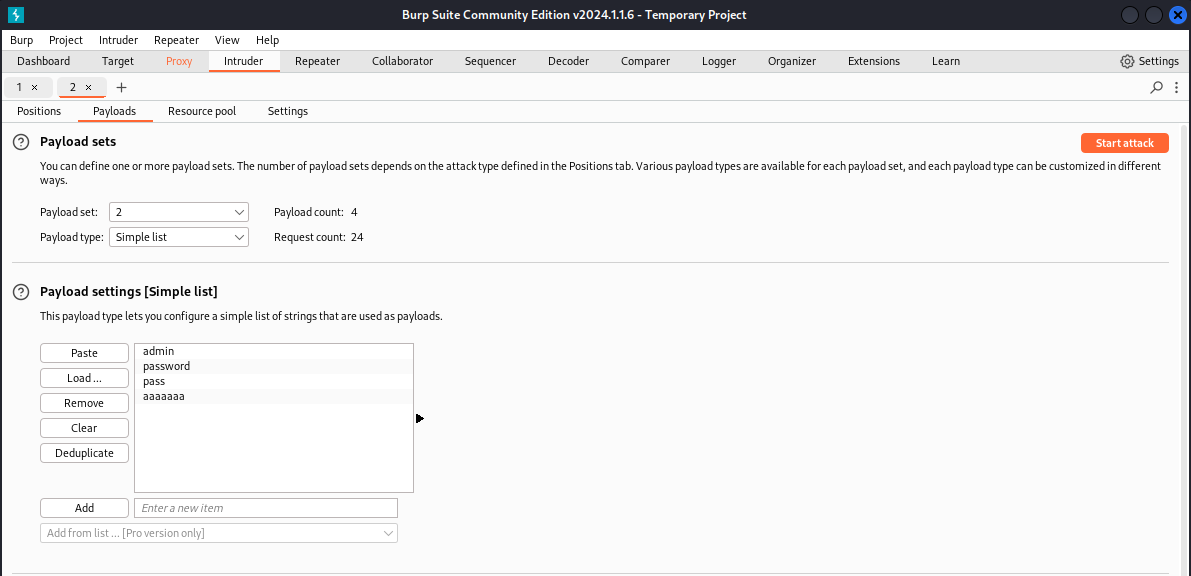


Рис. 16: Второй Simple list

Запускаю атаку и начинаю подбор (рис. 17).

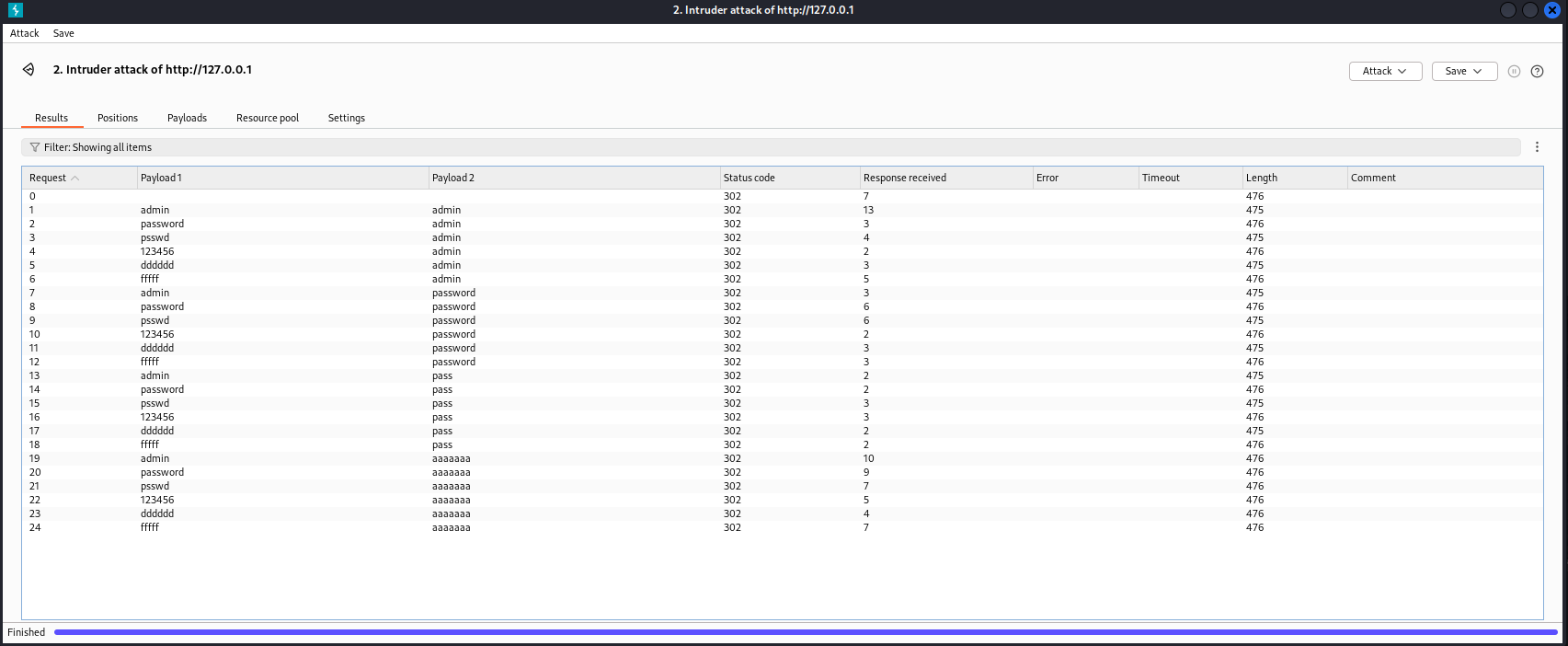


Рис. 17: Запуск атаки

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит (рис. 18).

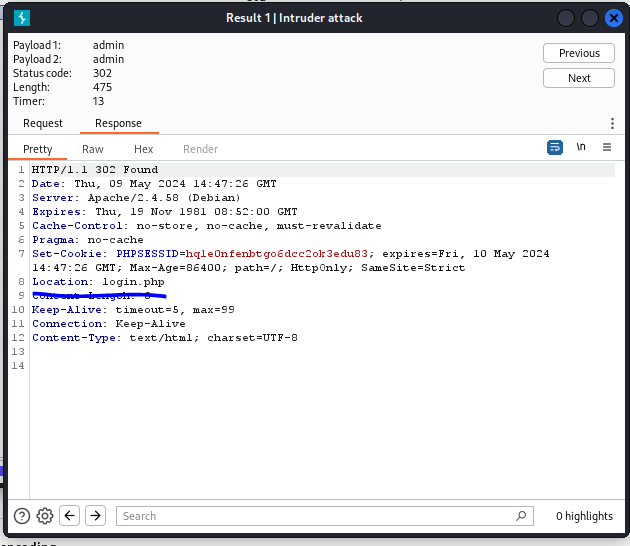


Рис. 18: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. 19).

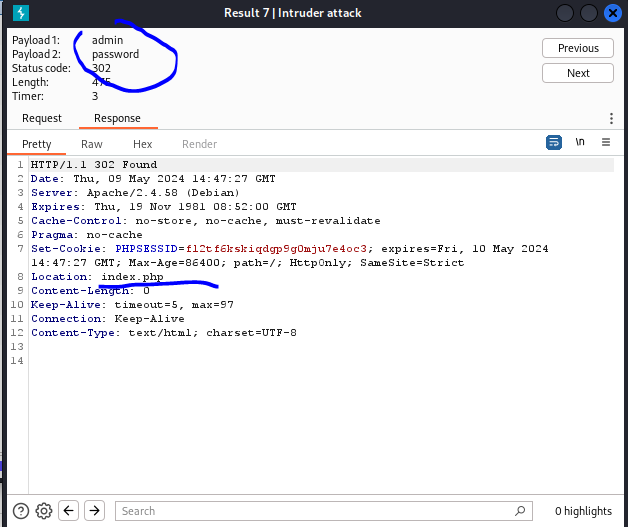


Рис. 19: Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater” (рис. 20).

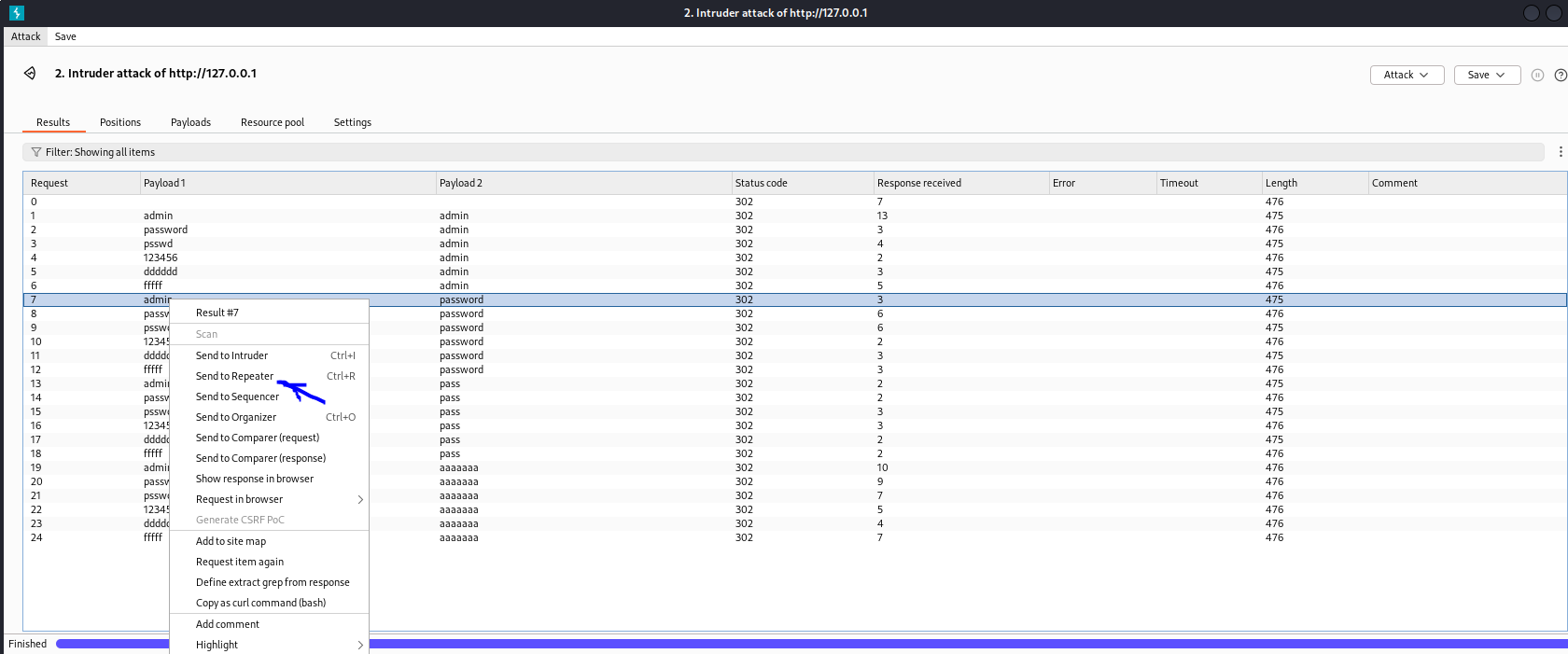


Рис. 20: Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. 21).

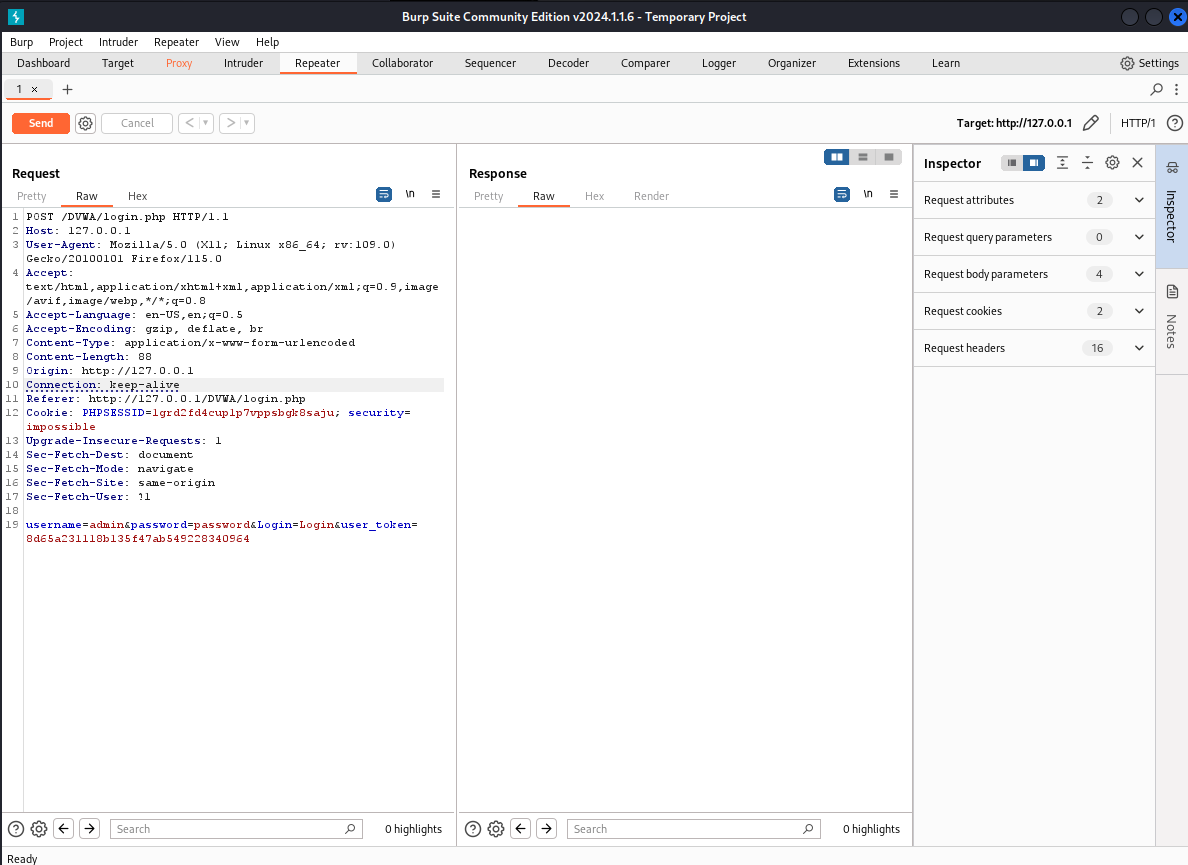


Рис. 21: Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. 22).

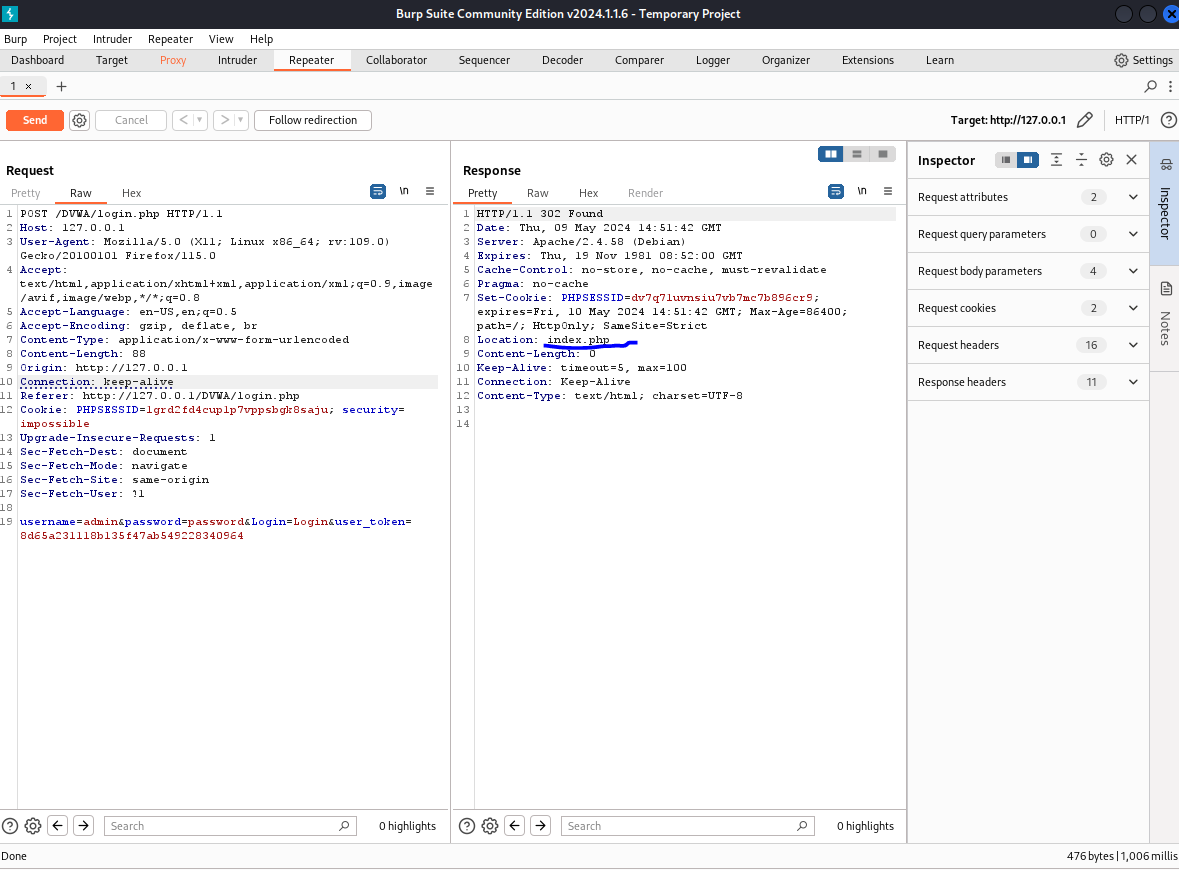


Рис. 22: Окно Response

После нажатия на Follow redirection, получим нескомпилированный html код в окне Response (рис. 23).

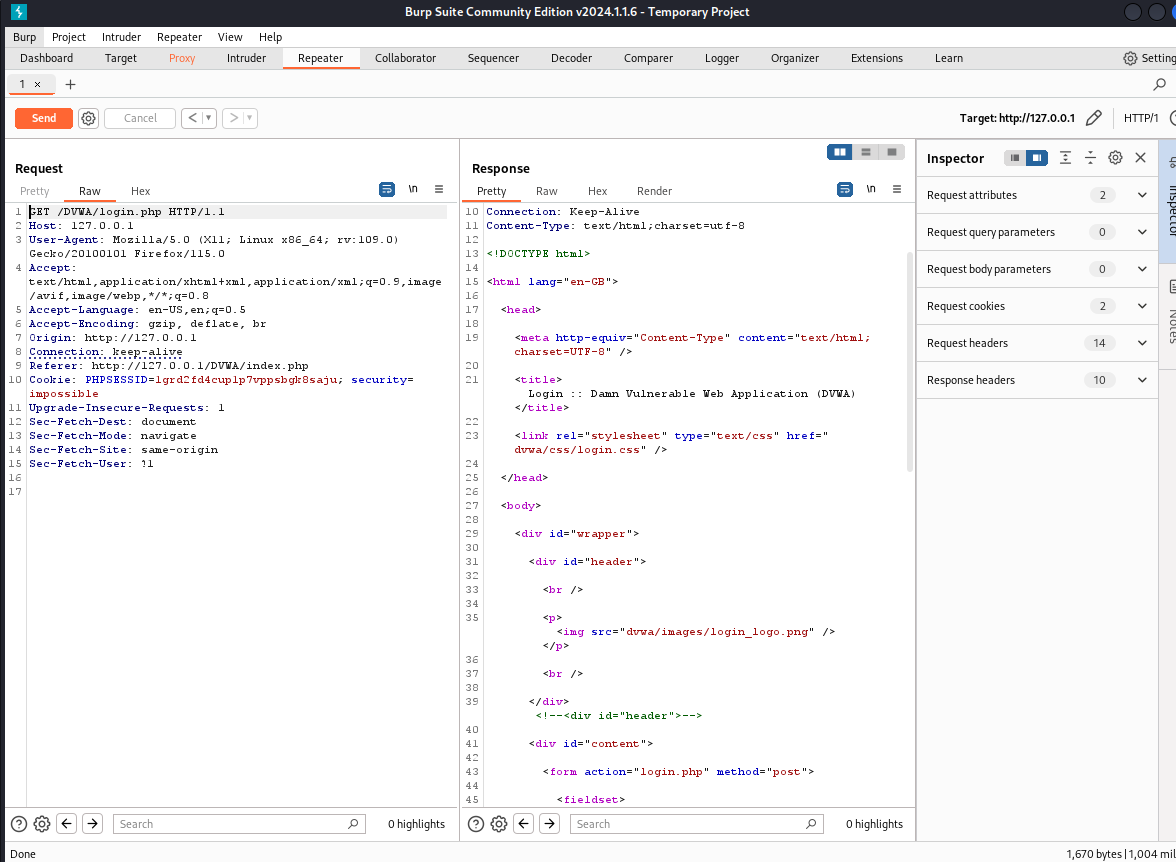


Рис. 23: Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. 24).

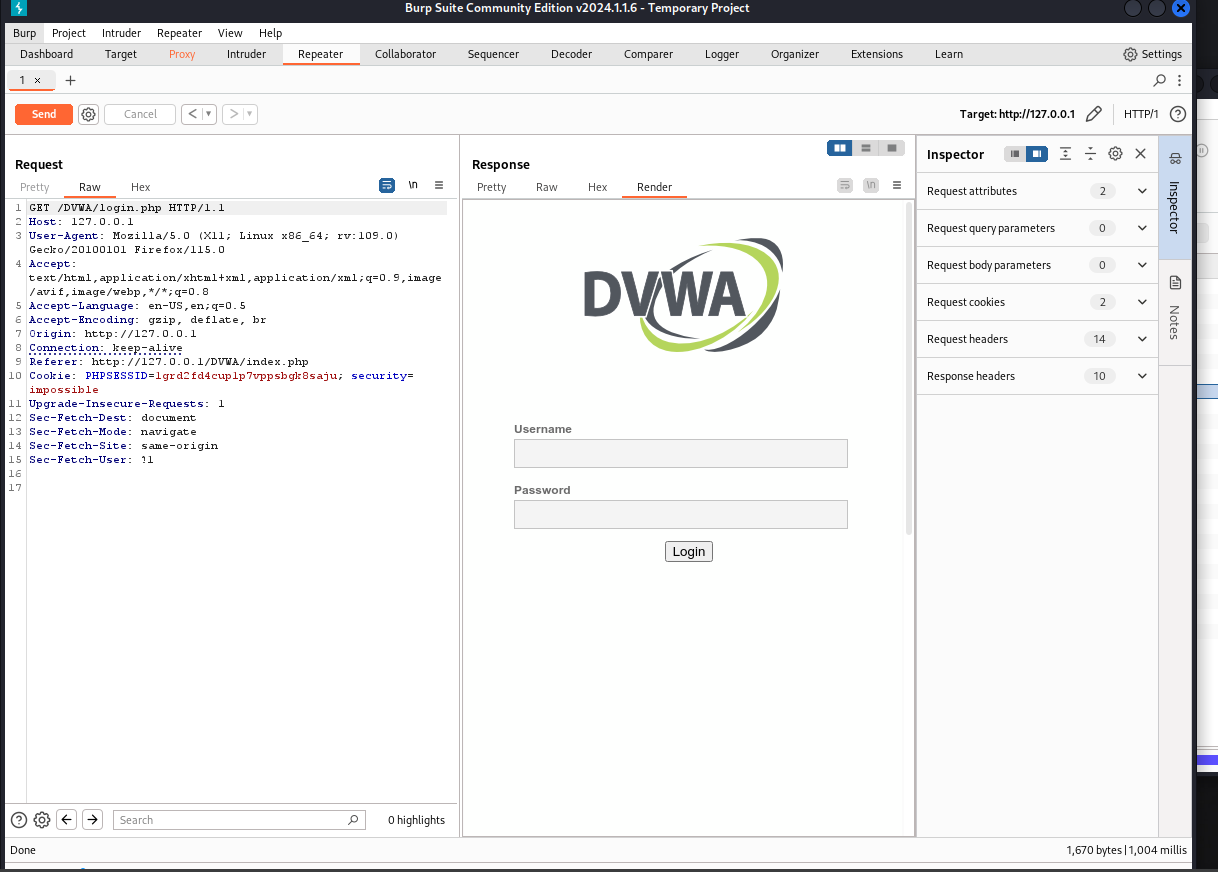


Рис. 24: Полученная страница

# 4 Выводы

При выполнении лабораторной работы были приобретены практические навыки по использованию инструмента Burp Suite.