Отчет по выполнению идивидуального проекта. Этап №5

Основы информационной безопасности

Назармамадов Умед Джамшедович

Содержание

# 1 Цель работы

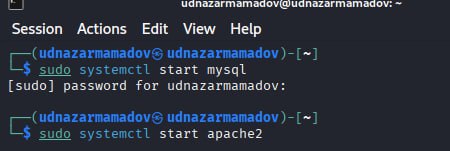
Научиться использовать Burp Suite.

# 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. [1].

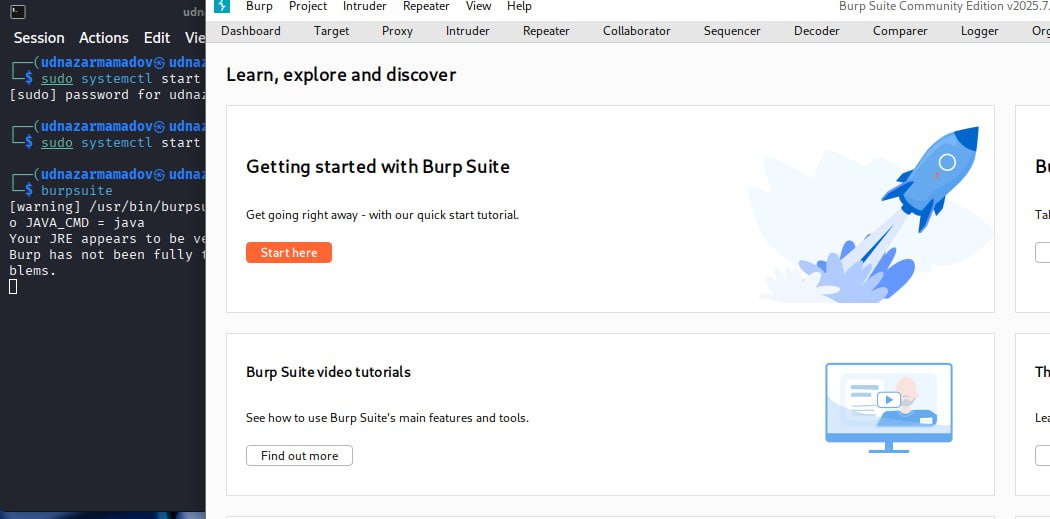
# 3 Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. [**fig:001?**]).



Запуск локального сервера

Запускаю инструмент Burp Suite (рис. [**fig:002?**]).



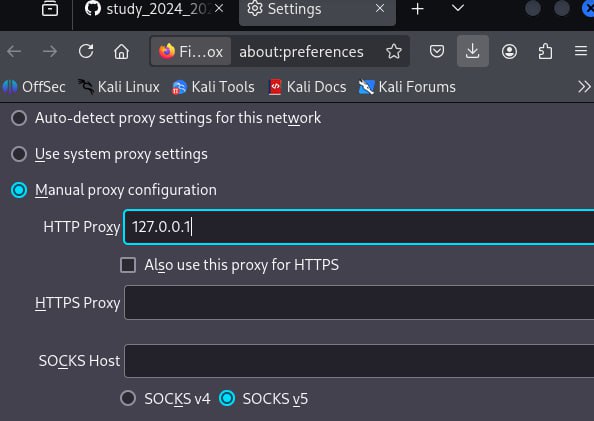
Запуск приложения

Открываю сетевые настройки браузера, для подготовке к работе (рис. [**fig:003?**]).



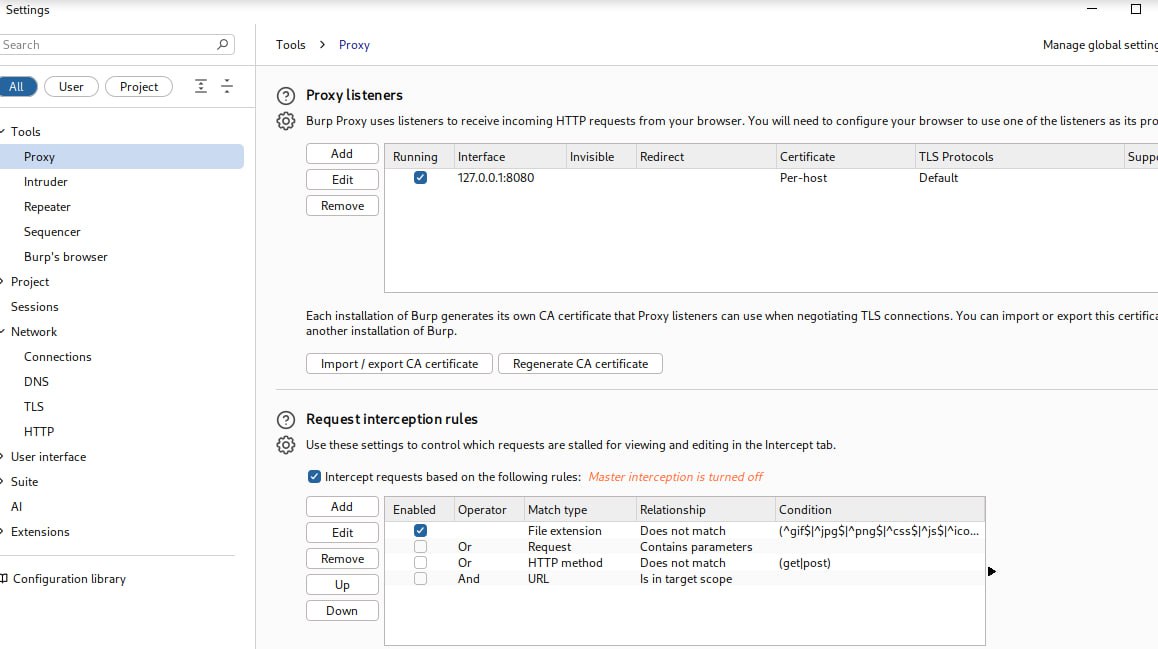
Сетевые настройки браузера

Изменение настроек сервера для работы с proxy и захватом данных с помощью Burp Suite (рис. [**fig:004?**]).



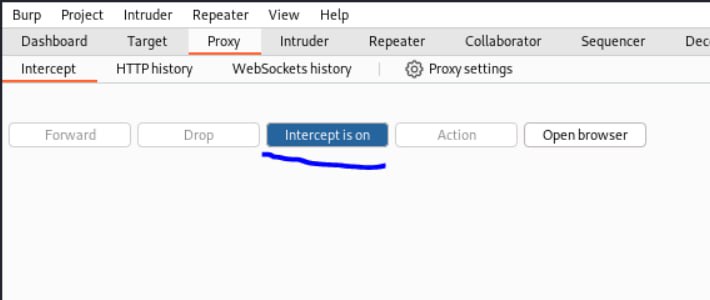
Настройки сервера

Изменяю настройки Proxy инструмента Burp Suite для дальнейшей работы (рис. [**fig:005?**]).



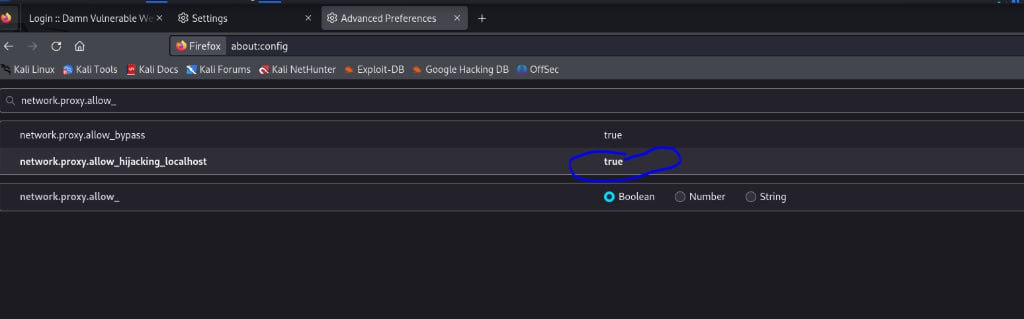
Настройки Burp Suite

Во вкладке Proxy устанавливаю “Intercept is on” (рис. [**fig:006?**]).



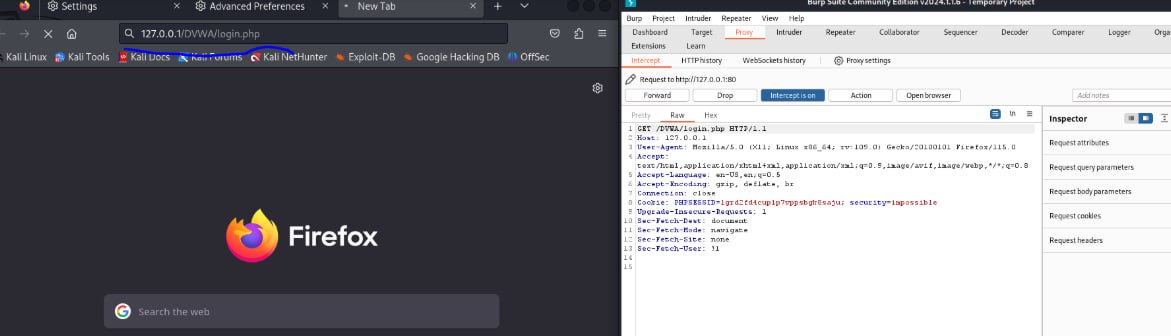
Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, наобходимо установить параметр network\_allow\_hijacking\_loacalhost на true (рис. [**fig:007?**]).



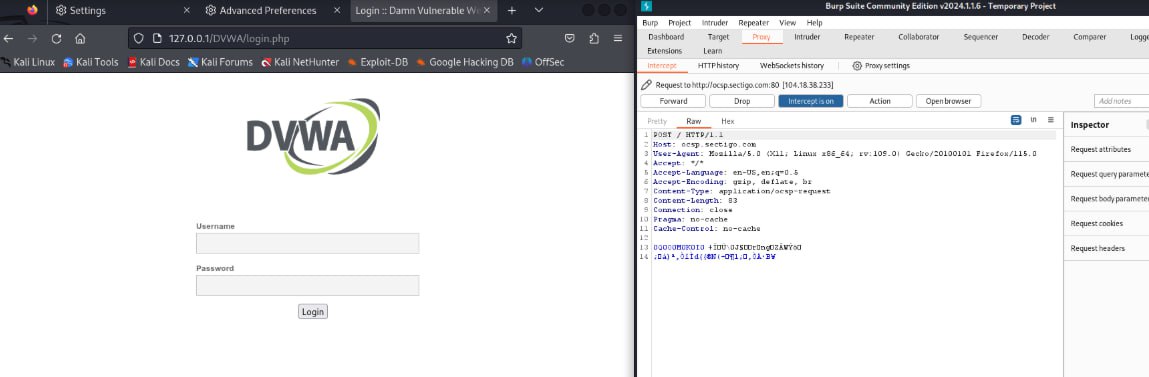
Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [**fig:008?**]).



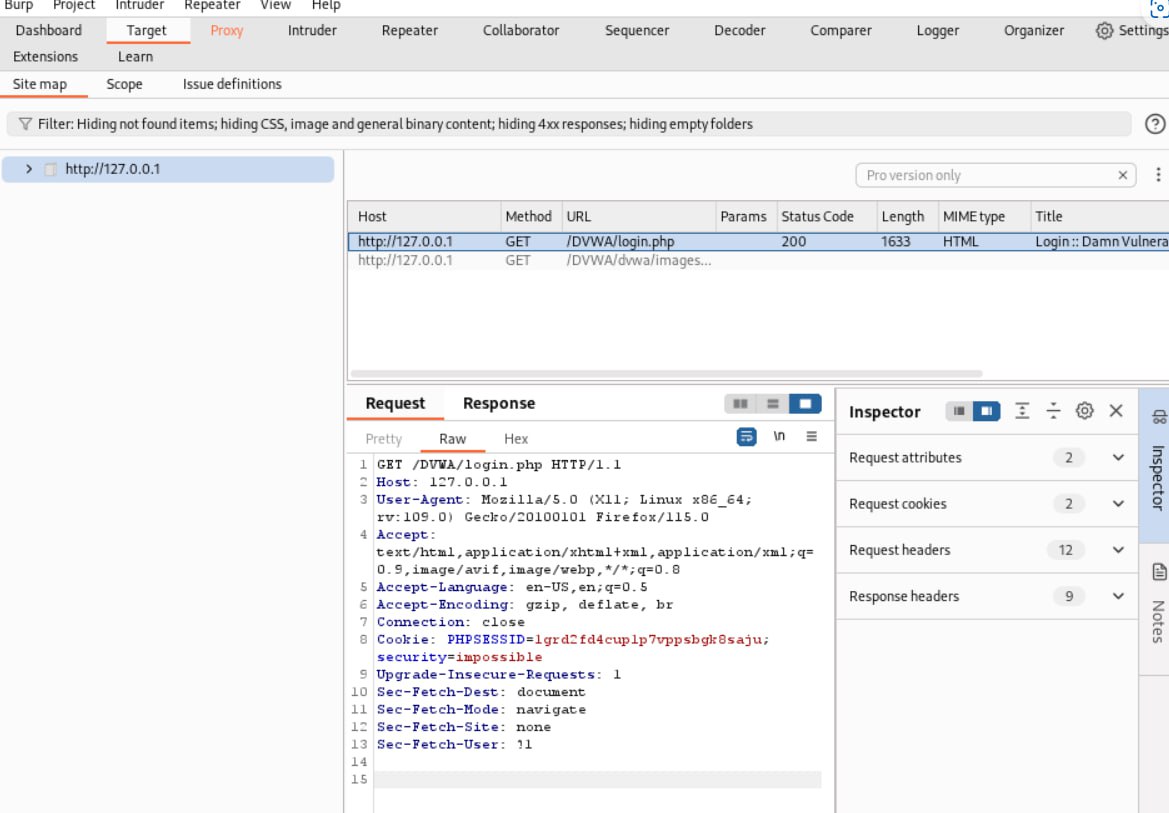
Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [**fig:009?**]).



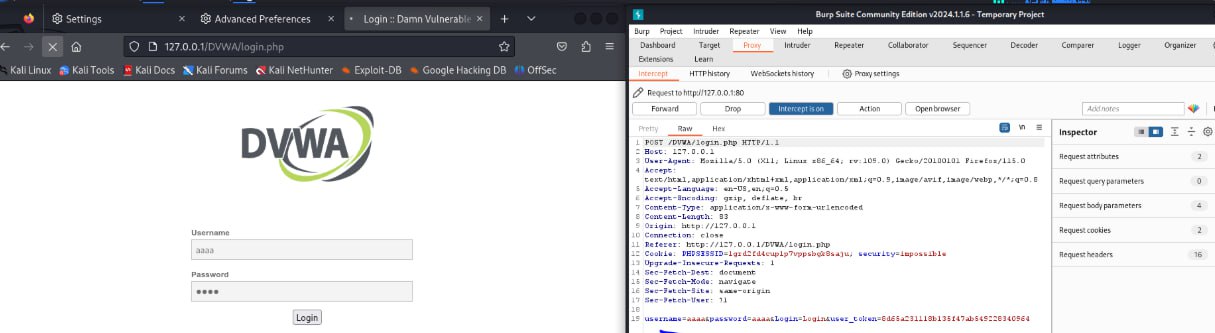
Страница авторизации

История запросов хранится во вкладке Target (рис. [**fig:010?**]).



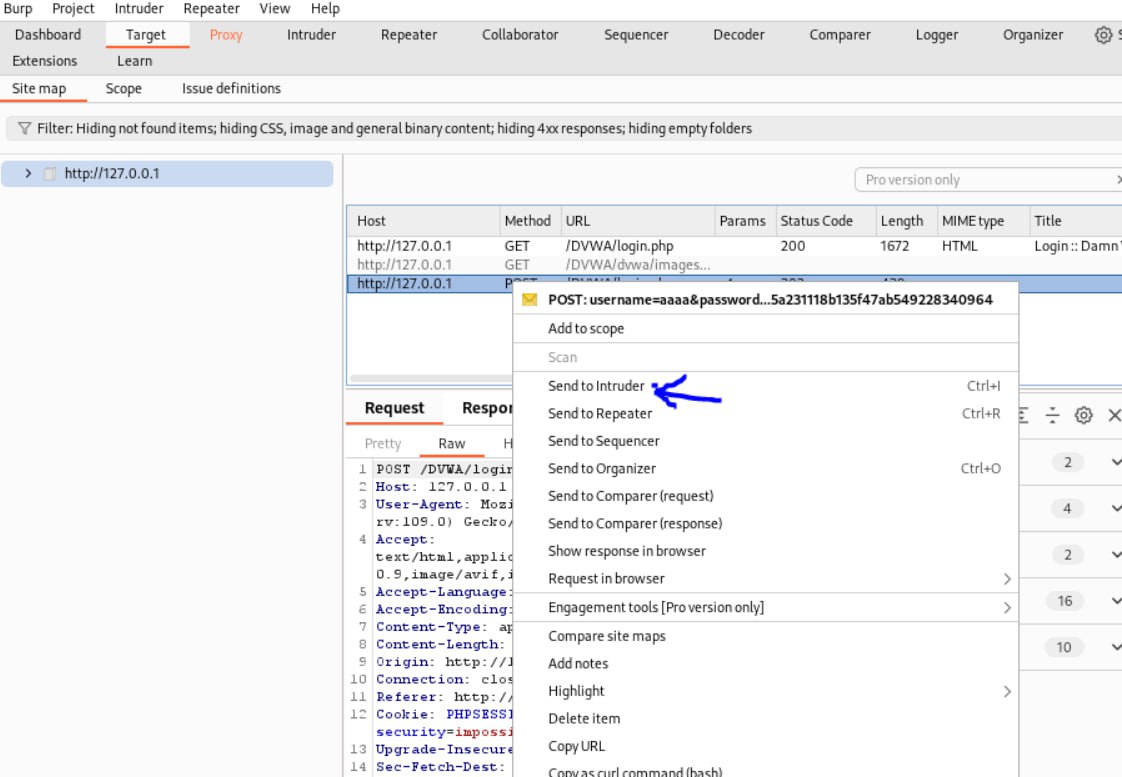
История запросов

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. [**fig:011?**]).



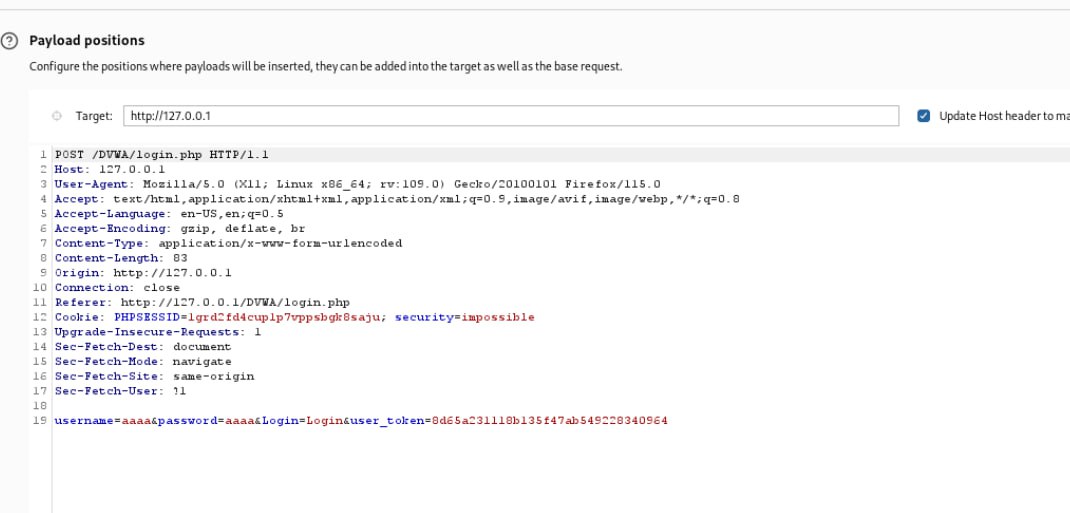
Ввод случайных данных

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. [**fig:012?**]).



POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. [**fig:013?**]).



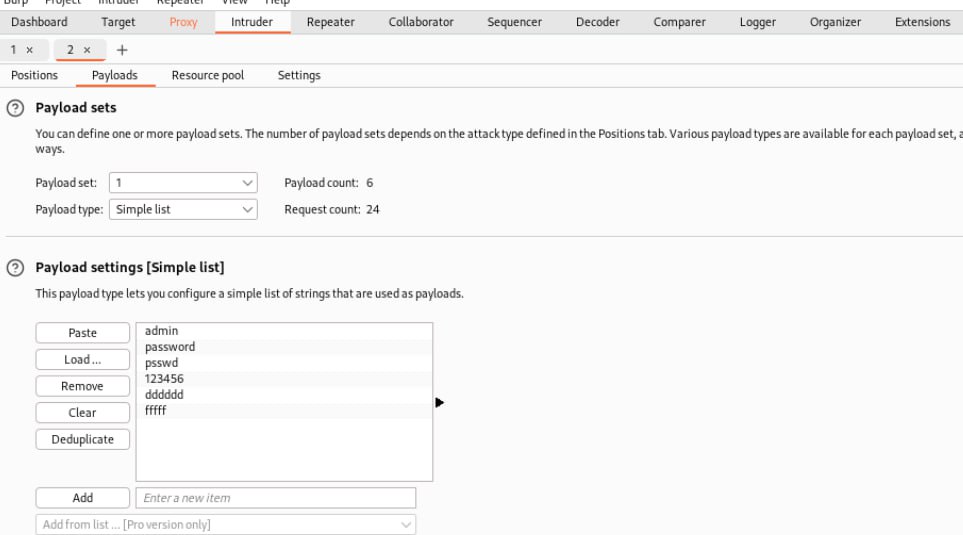
Вкладка Intruder

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. [**fig:014?**]).



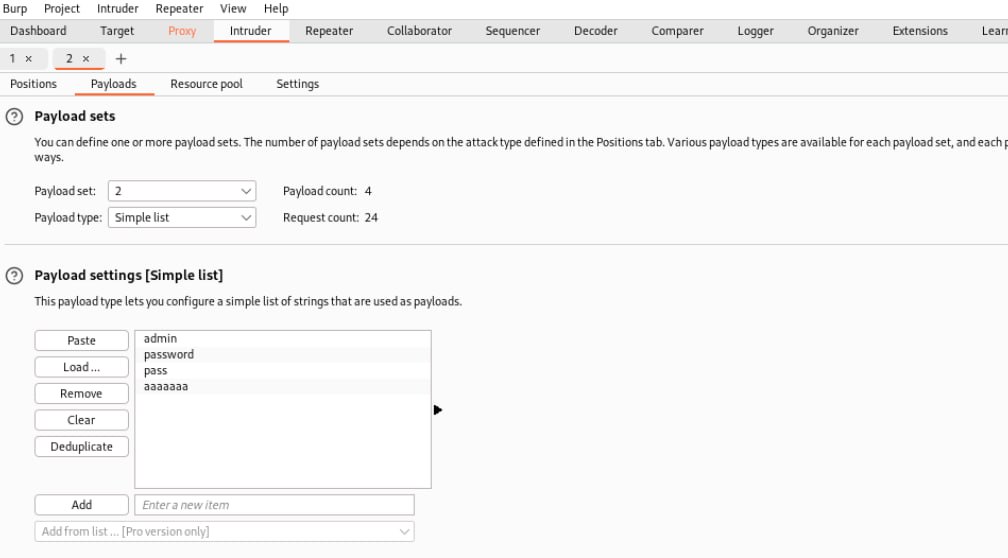
Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. [**fig:015?**]).



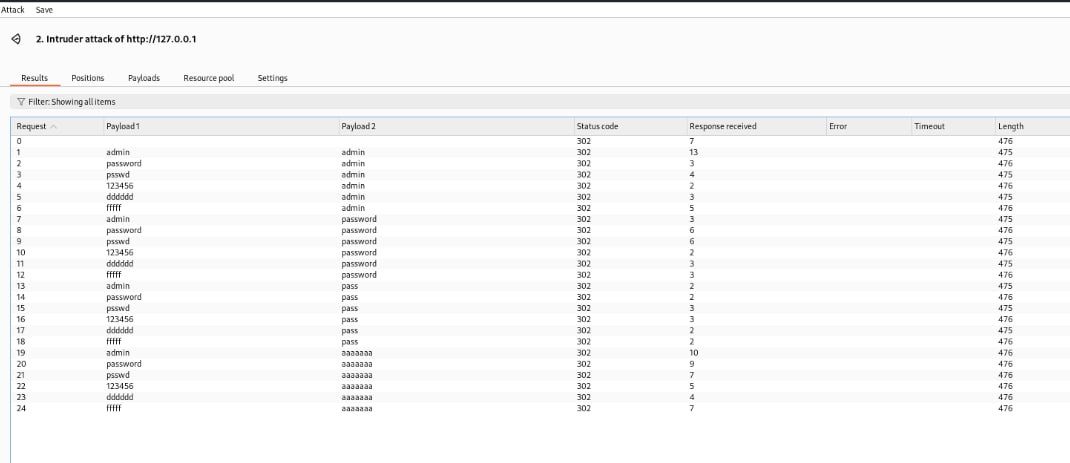
Первый Simple list

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. [**fig:016?**]).



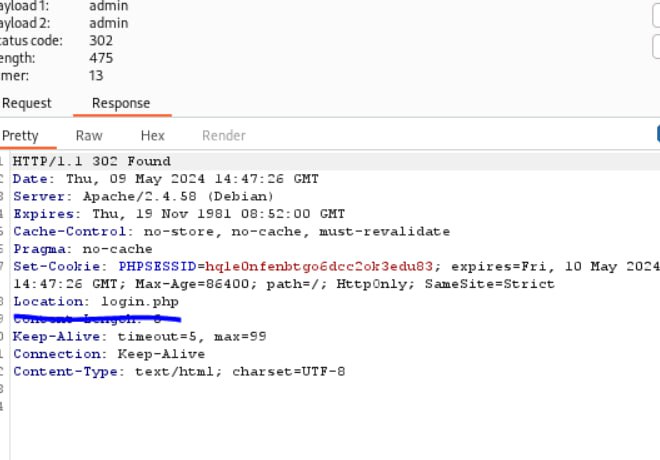
Второй Simple list

Запускаю атаку и начинаю подбор (рис. [**fig:017?**]).



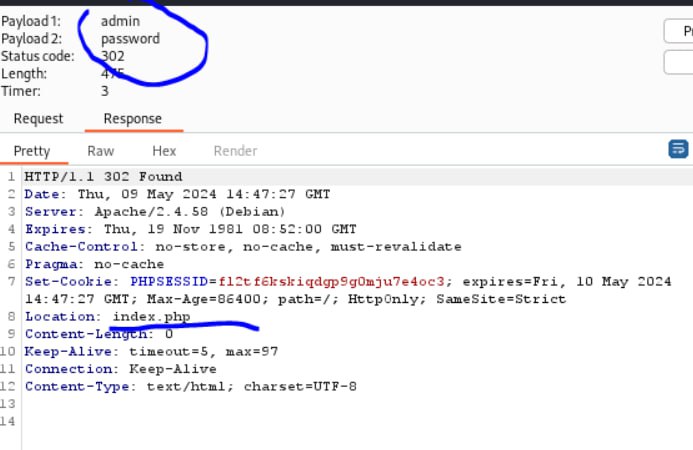
Запуск атаки

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. [**fig:018?**]).



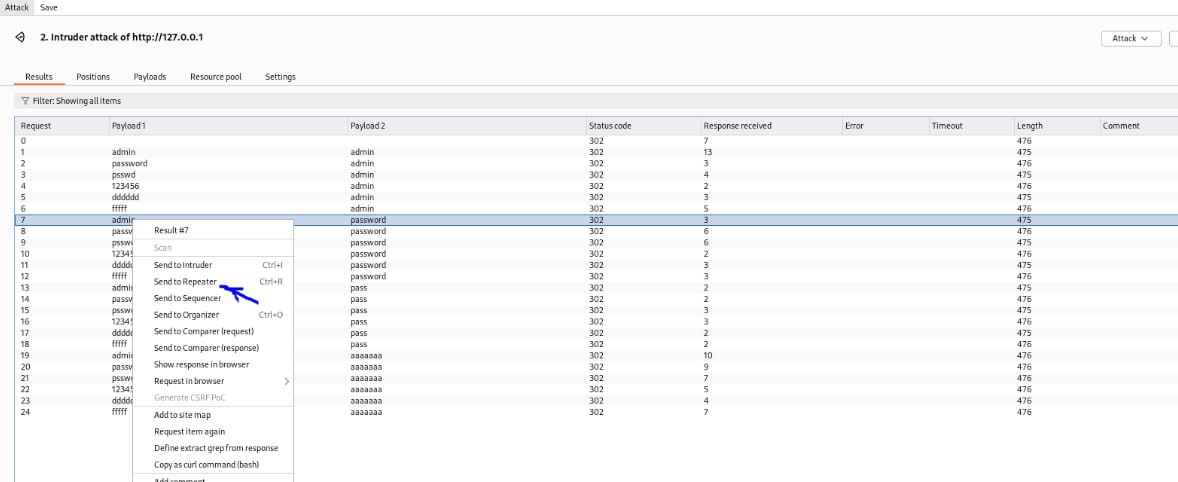
Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [**fig:019?**]).



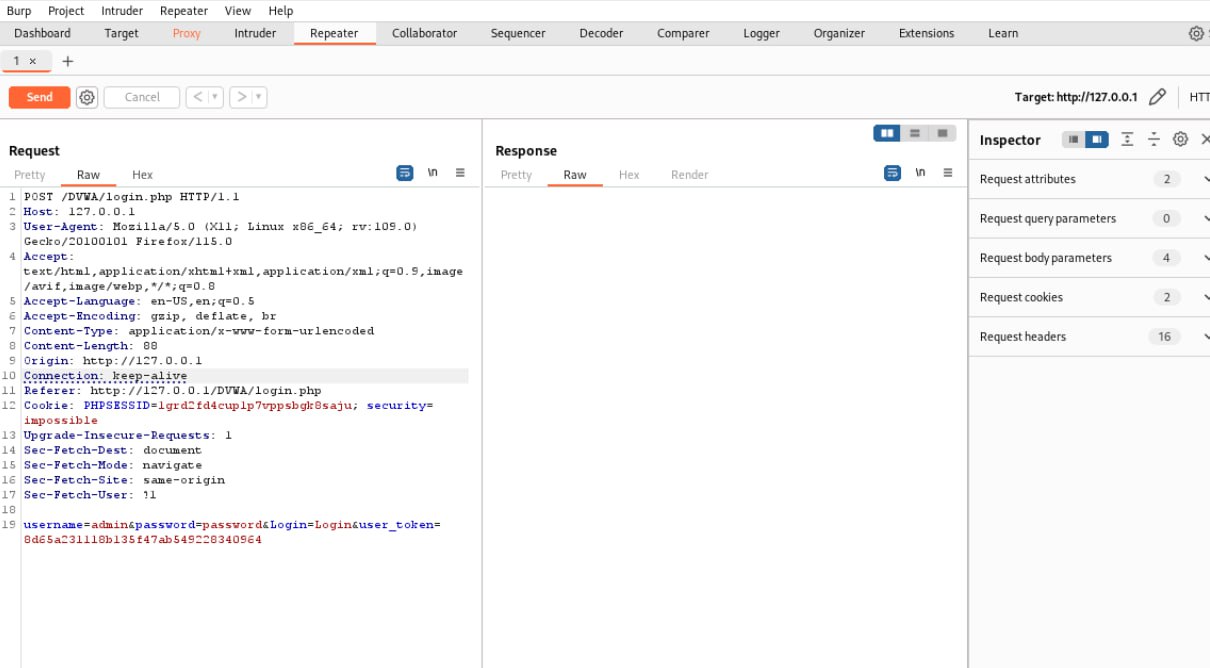
Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater” (рис. [**fig:020?**]).



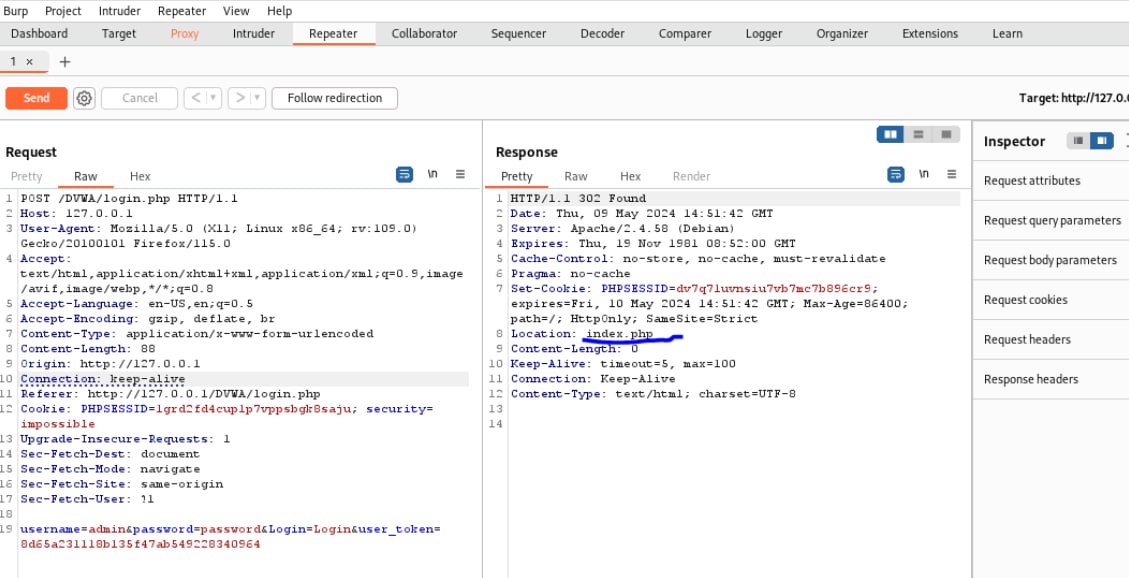
Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. [**fig:021?**]).



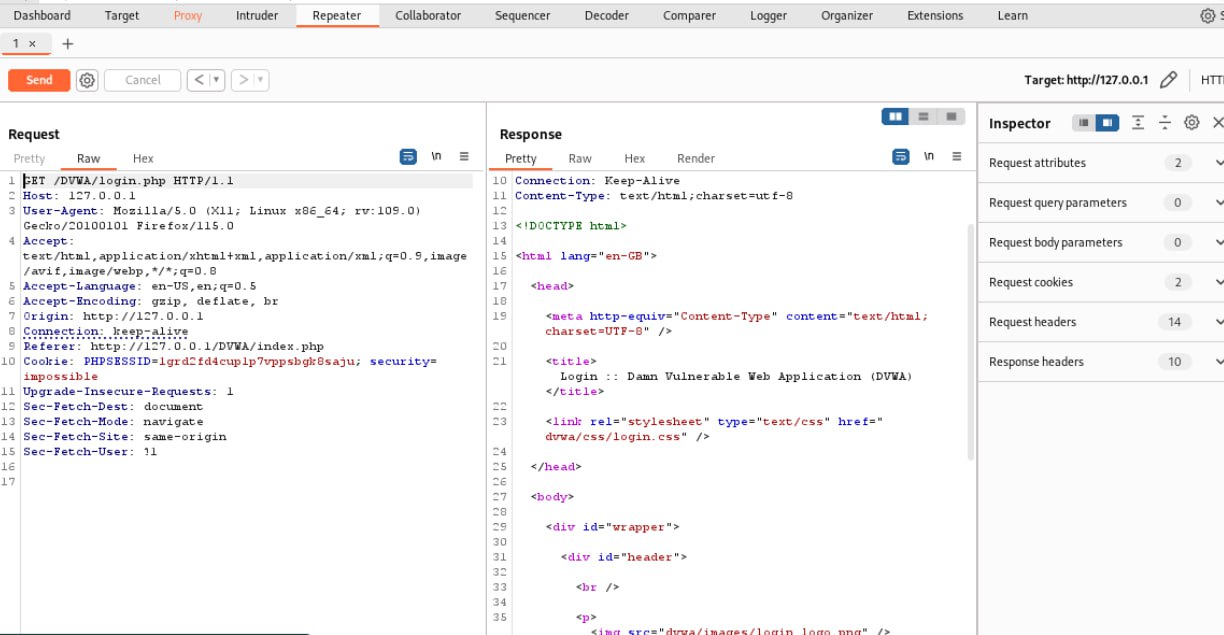
Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. [**fig:022?**]).



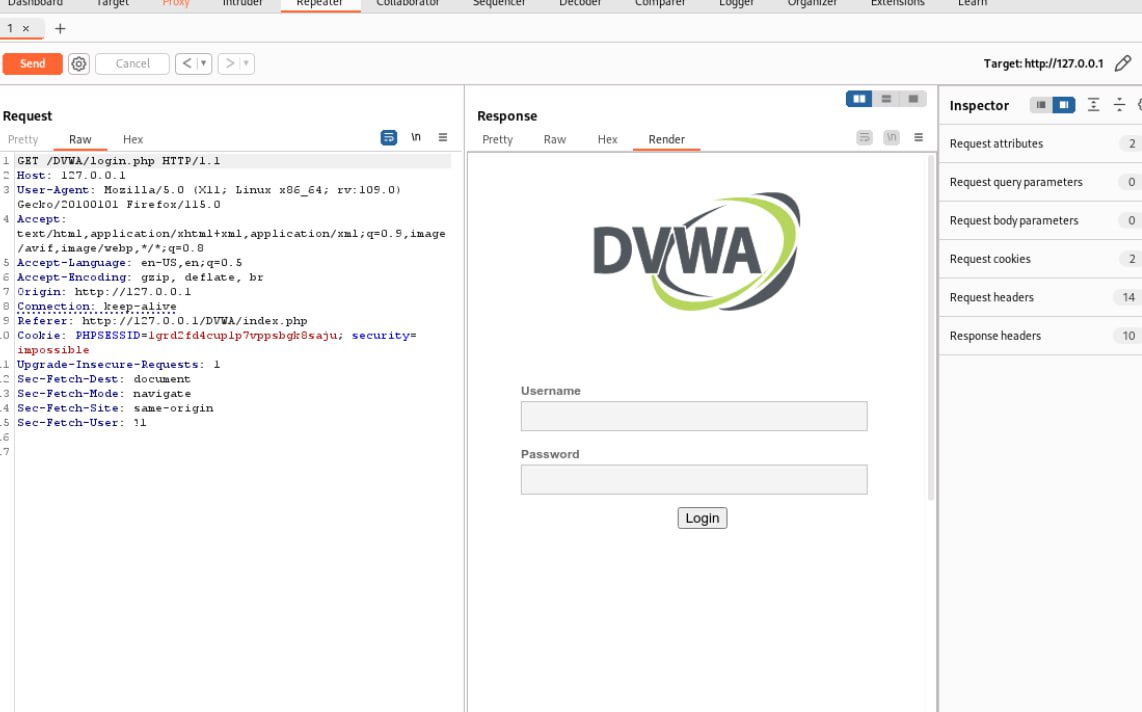
Окно Response

После нажатия на Follow redirection, получим нескомпилированный html код в окне Response (рис. [**fig:023?**]).



Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [**fig:024?**]).



Полученная страница

# 4 Выводы

При выполнении лабораторной работы я научился использовать инструмент Burp Suite.

# Список литературы

1. Ш. Парасрам Т.Х.и.др. А. Замм. Kali Linux: Тестирование на проникновение и безопасность: для профессионалов. Питер, 2022. 448 с.