Отчет по идивидуальнной проекте 5

Основы информационной безопасности

Нджову Нелиа

Содержание

# 1 Цель работы

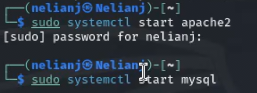
Научиться использовать Burp Suite.

# 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.

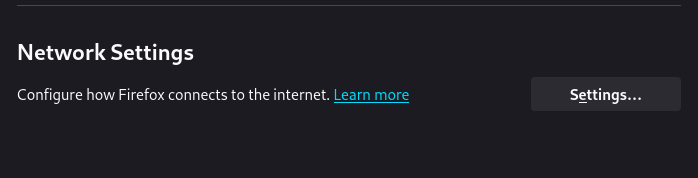
# 3 Выполнение лабораторной работы

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



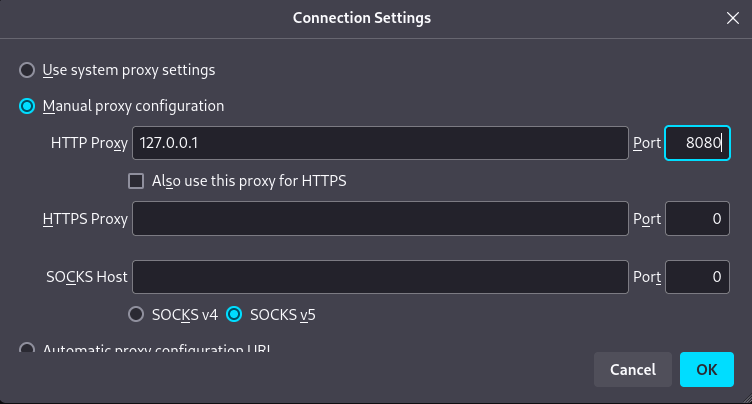
Запуск локального сервера

Я запускаю инструмент Burp Suite. После этого я открываю сетевые настройки браузера, для подготовке к работе(рис.2).



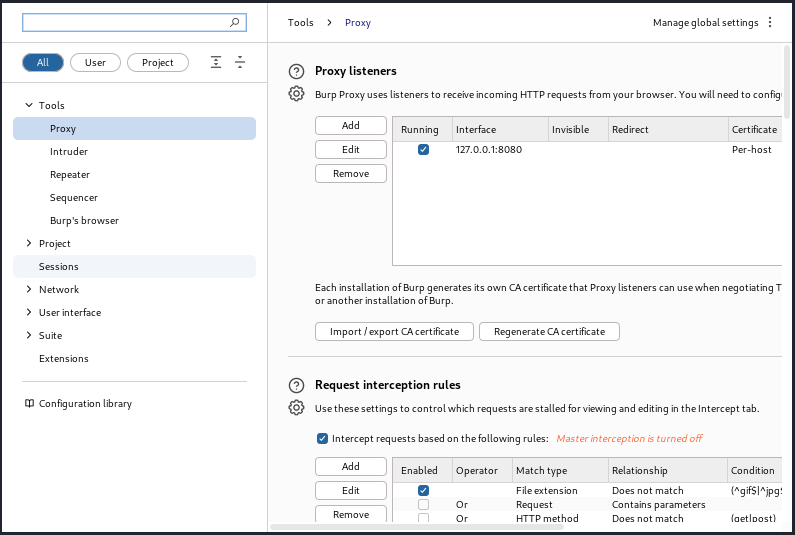
Сетевые настройки браузера

Я изменяю настройки сервера для работы с proxy и захватом данных с помощью Burp Suite(рис.3)



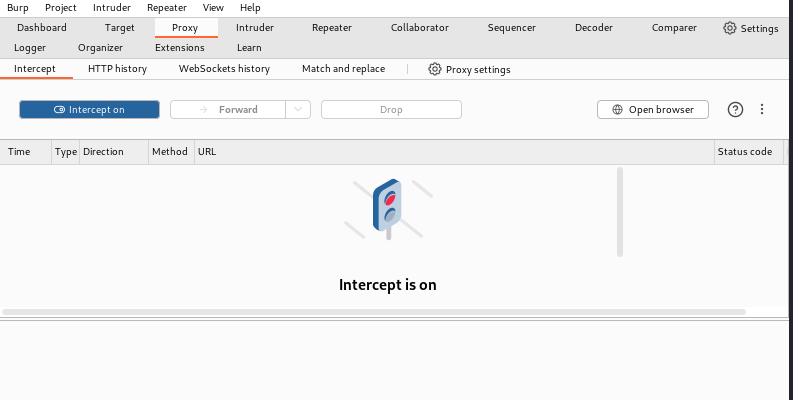
Настройки сервера

Я изменяю настройки Proxy инструмента Burp Suite для дальнейшей работы(рис.4).



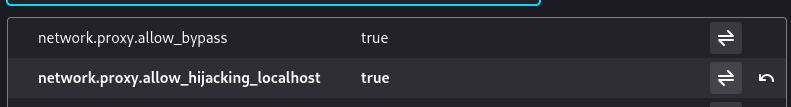
Настройки Burp Suite

Во вкладке Proxy устанавливаю “Intercept is on”(рис.5).



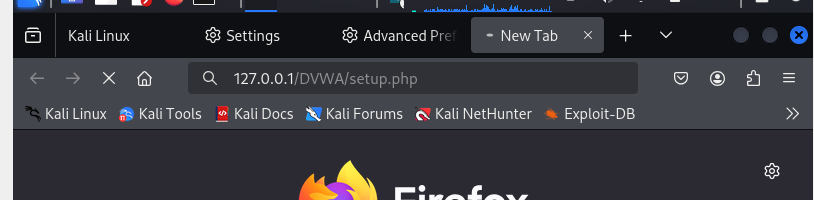
Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, наобходимо установить параметр network\_allow\_hijacking\_loacalhost на true(рис.6).

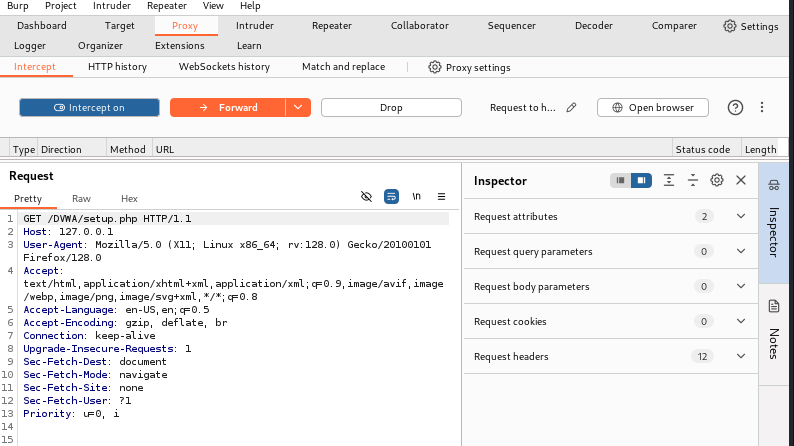


Настройки параметров

Я пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу(рис.7 и рис.8).

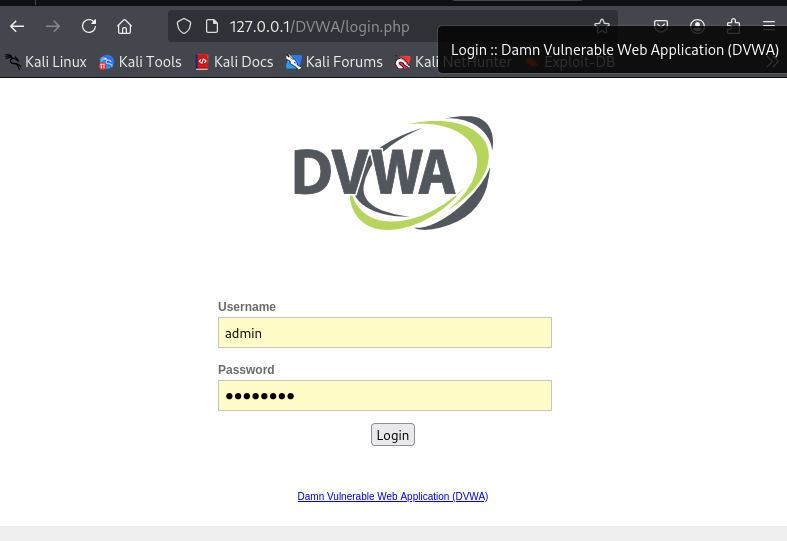


Получаемые запросы сервера

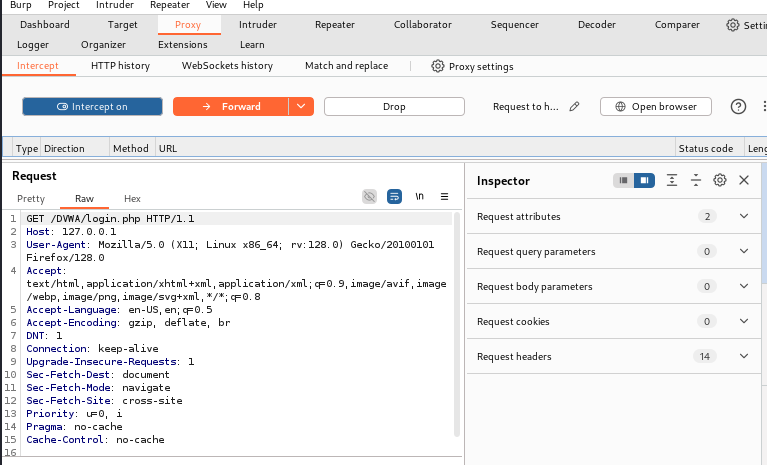


Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся(рис.9 и рис.10).

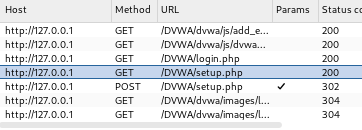


Страница авторизации



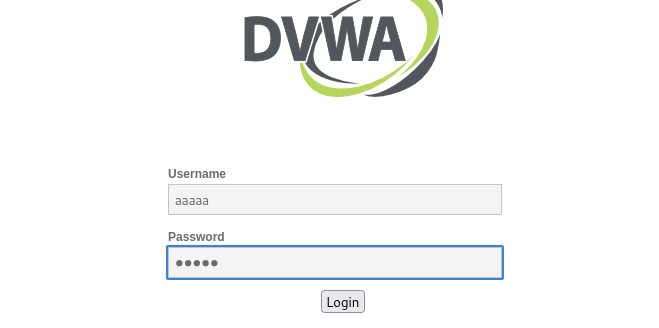
Страница авторизации

История запросов хранится во вкладке Target (рис.11).

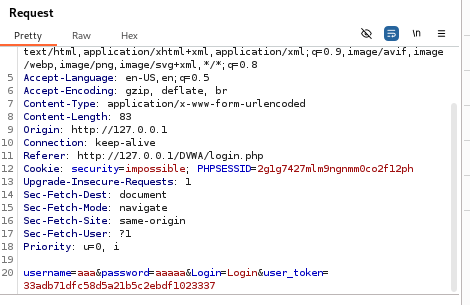


История запросов

Я попробую 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.12 и рис.13).

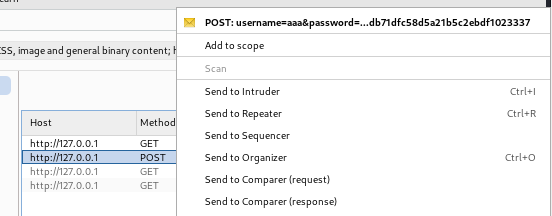


Ввод случайных данных



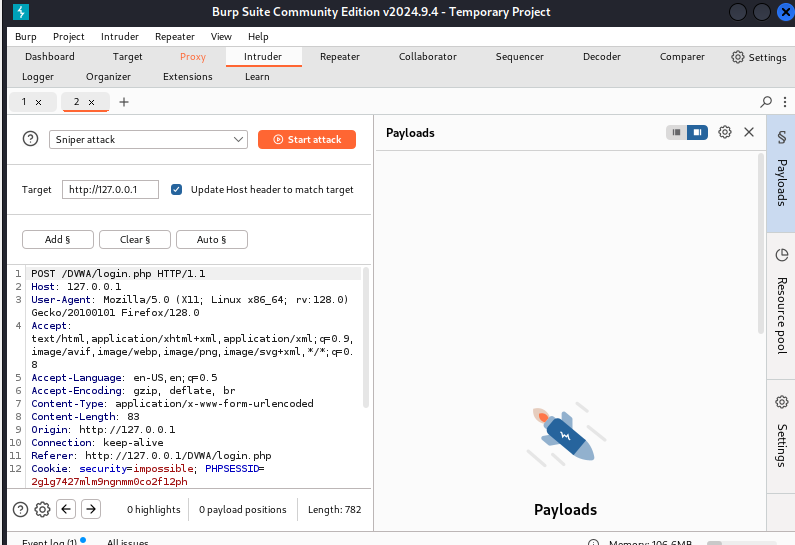
Ввод случайных данных

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.14).



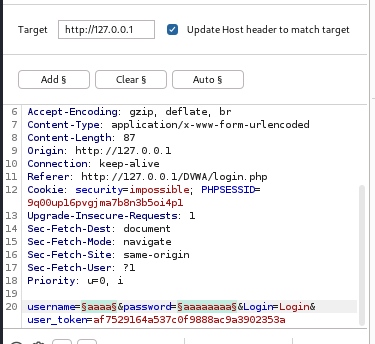
POST-запрос с вводом пароля и логина

Я попадаю на вкладку Intruder, вижу значения по умолчанию у типа атаки и наш запрос(рис.15).



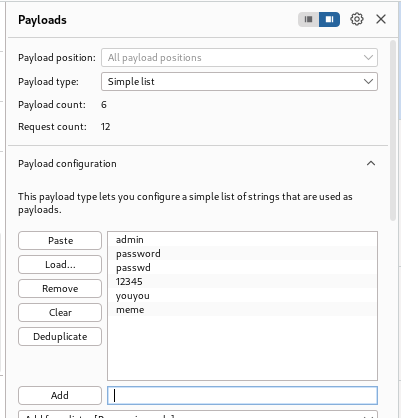
Вкладка Intruder

Я изменяю значение типа атаки на Cluster bomb и проставляю специальные символы у тех данных в форме для ввода, которые буду пробивать(рис.16).



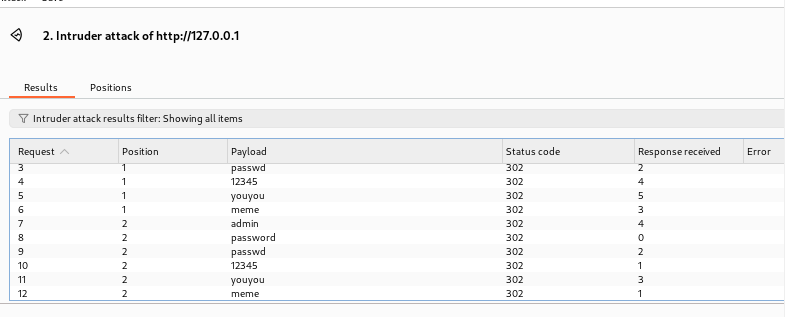
Изменение типа атаки

Так как мне нужно параметра для подбора, то нужно списка со значениями для подбора(рис.17).



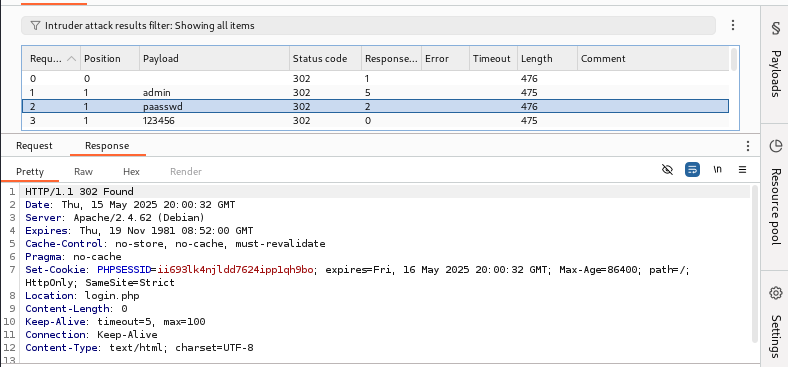
Первый Simple list

Я запускаю атаку и начинаю подбор(рис.18).



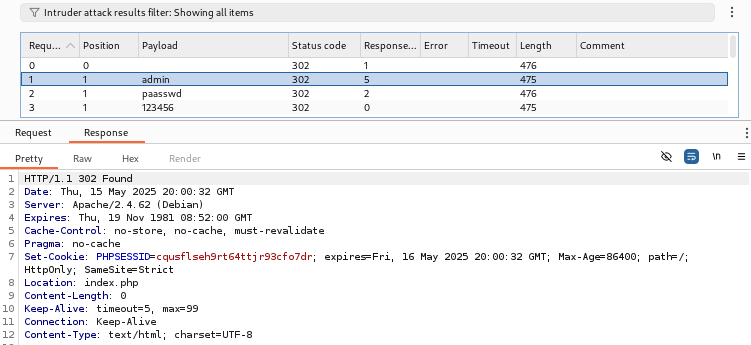
Запуск атаки

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 passwd-password нас перенаправило на login.php, это значит, что пара не подходит(рис.19).



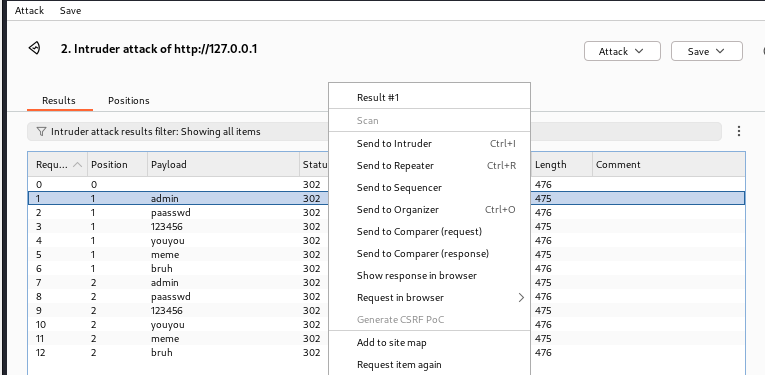
Результат запроса

Я проверяю результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной(рис.20).



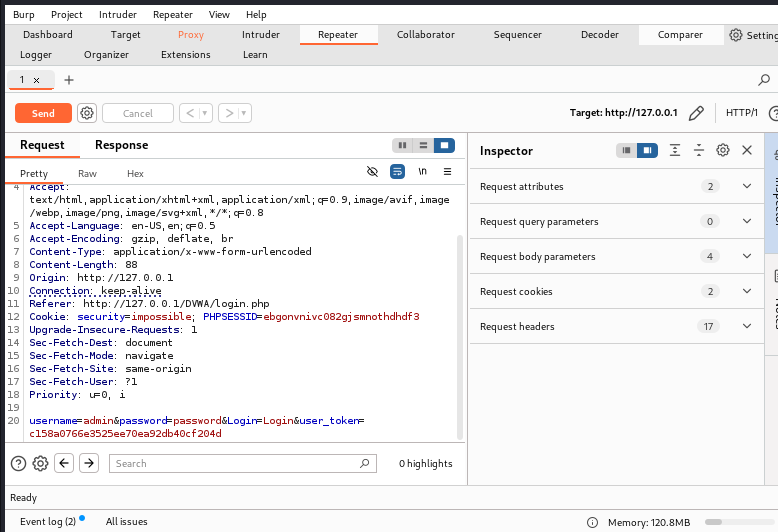
Результат запроса

Дополнительная проверка с использованием Repeater, нажимаю на нужный мне запрос правой кнопкой мыши и жмем “Send to Repeater” (рис.21).



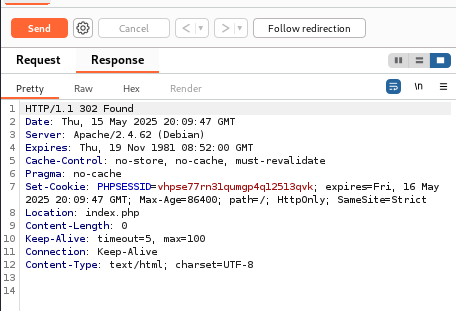
Дополнительная проверка результата

Я перехожу во вкладку “Repeater”(рис.22).



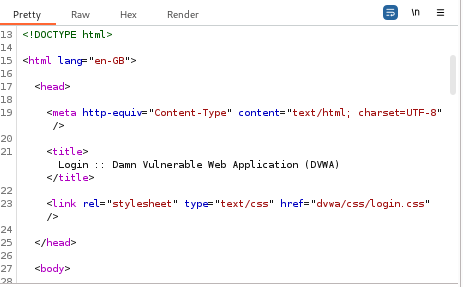
Вкладка Repeater

Нажимаю”send”, получаю в Response в результат перенаправление на index.php(рис.23).



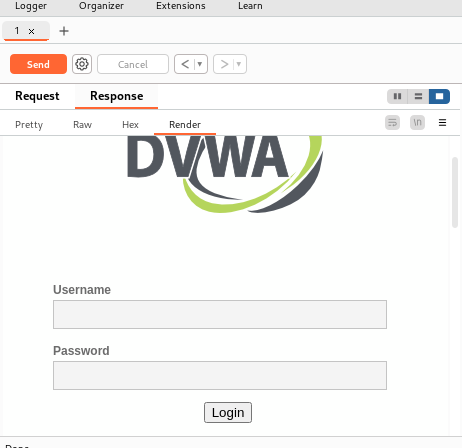
Окно Response

После нажатия на Follow redirection, получим нескомпилированный html код в окне Response(рис.24).



Изменение в окне Response

Далее в подокне Render получаю то, как выглядит полученная страница (рис.25).



Полученная страница

# 4 Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

# Список литературы

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