Отчёт по 5 этапу индивидуального проекта

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

[Цель работы 1](#_Toc179389973)

[Задание 1](#_Toc179389974)

[Выполнение 5-го этапа индивидуального проекта 1](#_Toc179389975)

[Выводы 10](#_Toc179389976)

[Список литературы 10](#_Toc179389977)

# Цель работы

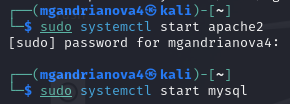
Научиться использовать Burp Suite в Kali Linux.

# Задание

Использование Burp Suite.

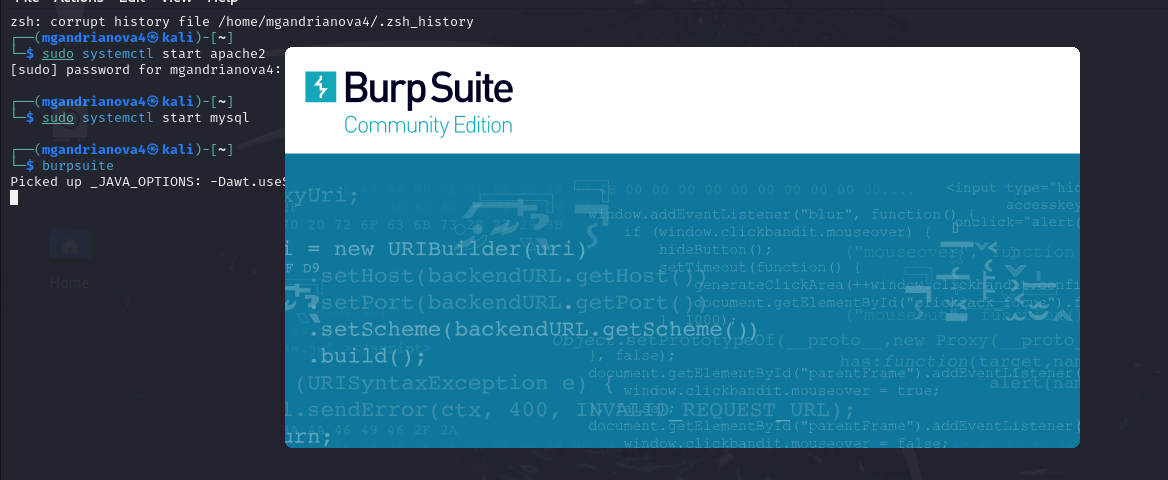
# Выполнение 5-го этапа индивидуального проекта

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



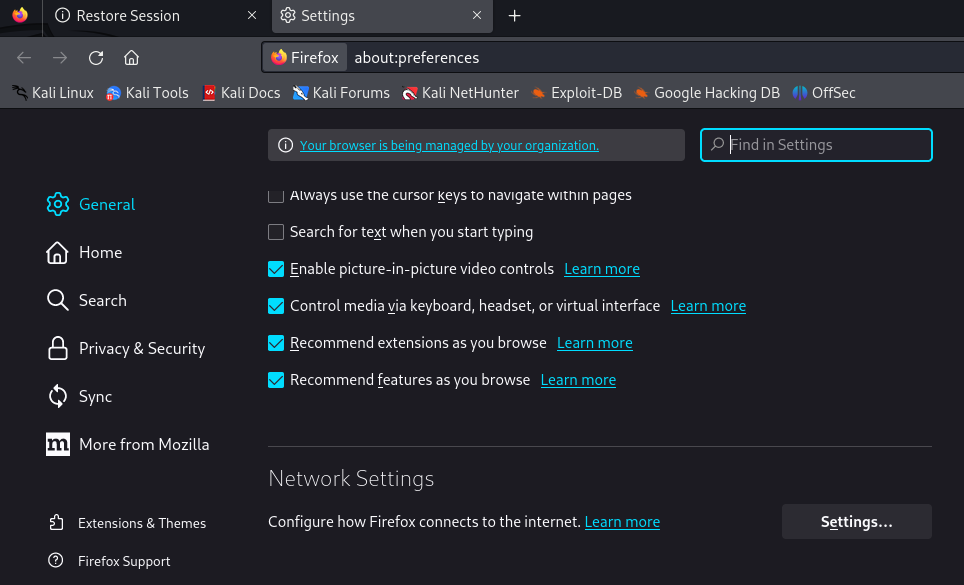
Запуск локального сервера

Запускаю инструмент Burp Suite (рис. [-@fig:002]).



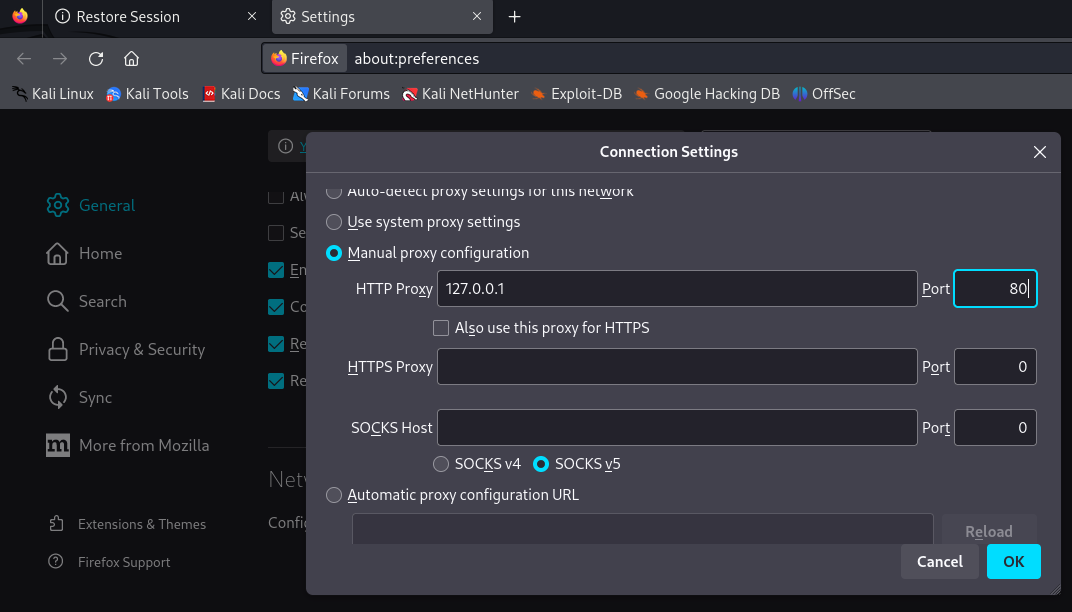
Запуск приложения

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



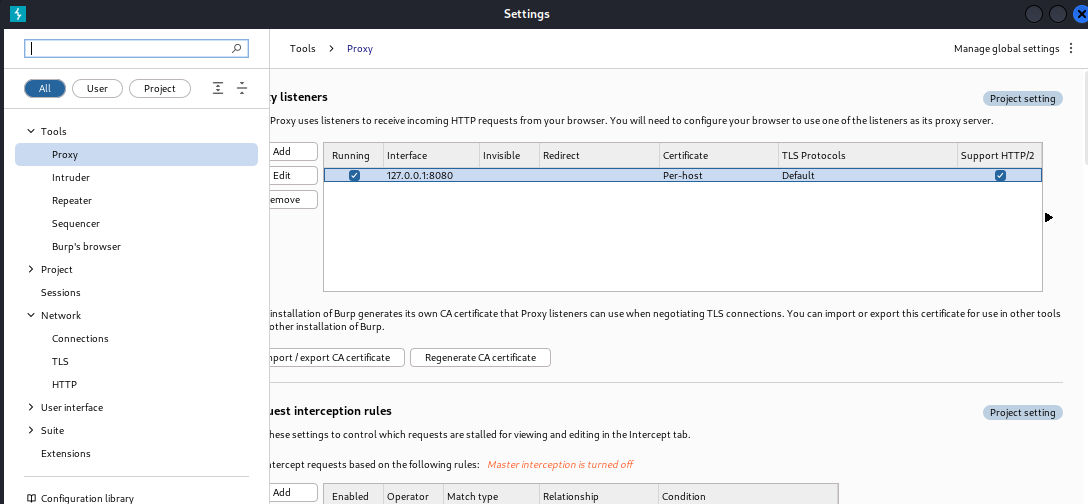
Сетевые настройки браузера

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



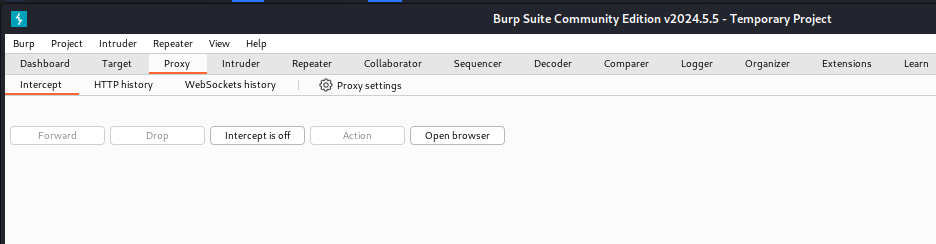
Настройки сервера

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

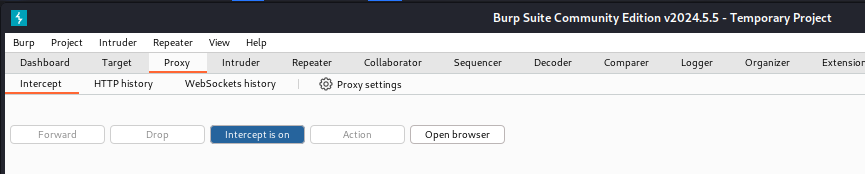


Настройки Burp Suite

Во вкладке Proxy меняю “Intercept is off” на “Intercept is on” (рис. [-@fig:006] и [-@fig:007]).

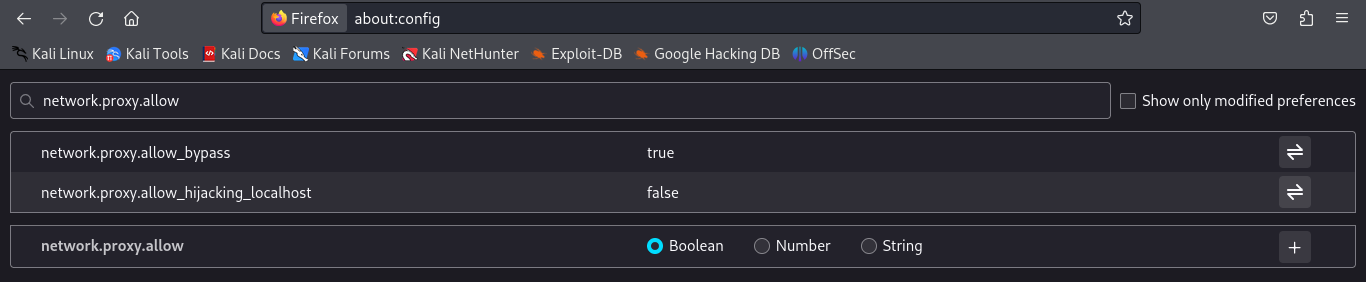


Настройки Proxy

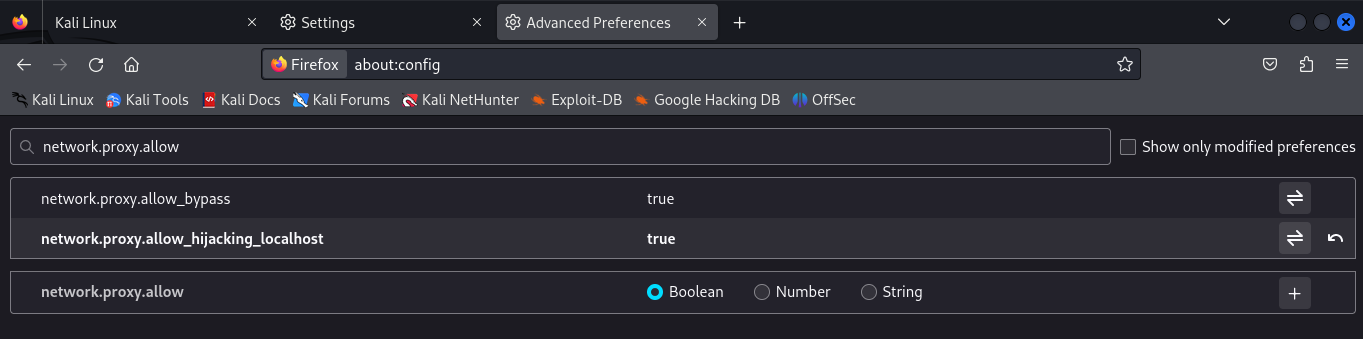


Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, наобходимо установить параметр network\_allow\_hijacking\_loacalhost на true (рис. [-@fig:008] и [-@fig:009]).

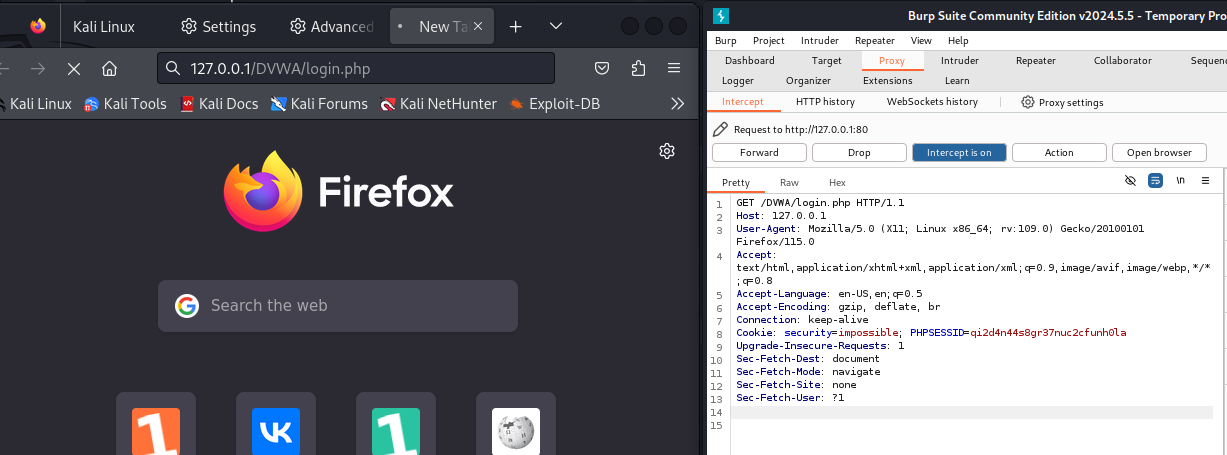


Настройки параметров



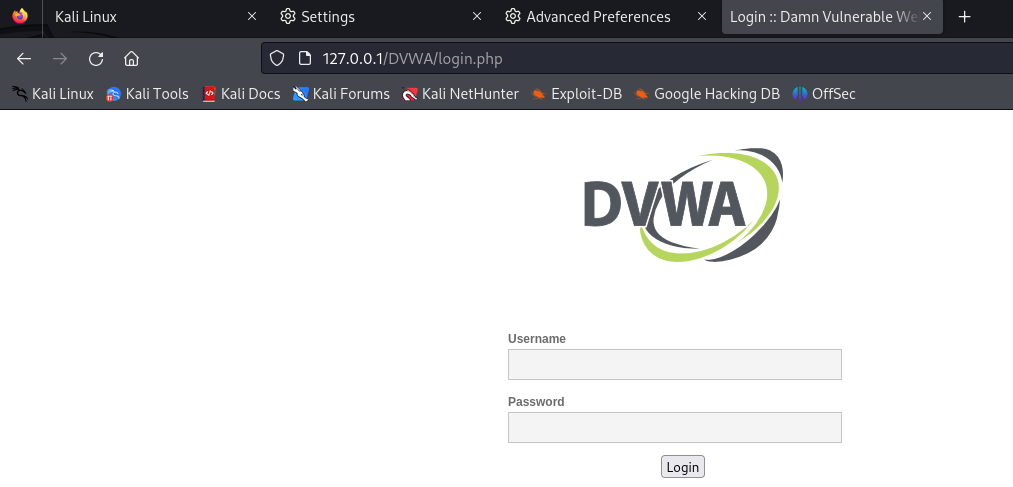
Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:010]).

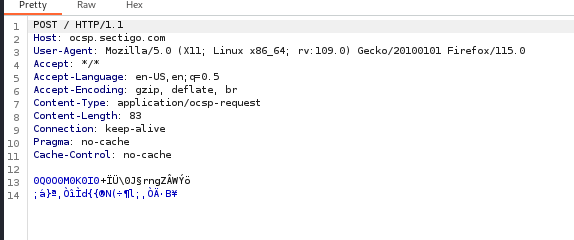


Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:011] и [-@fig:012]).

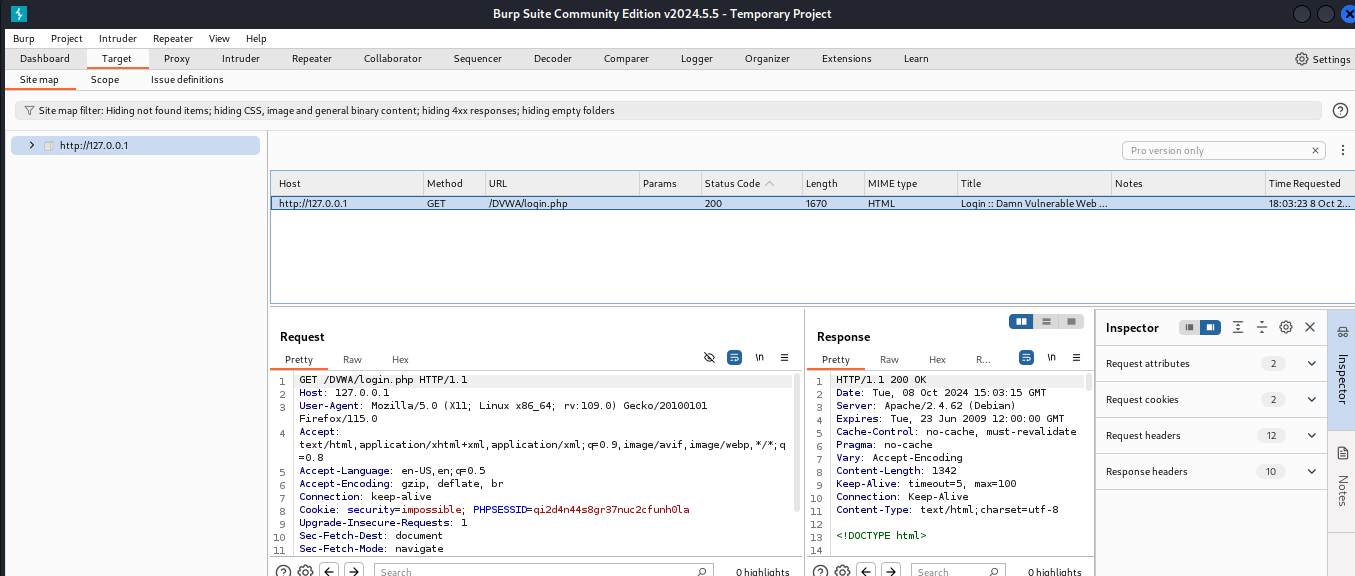


Страница авторизации



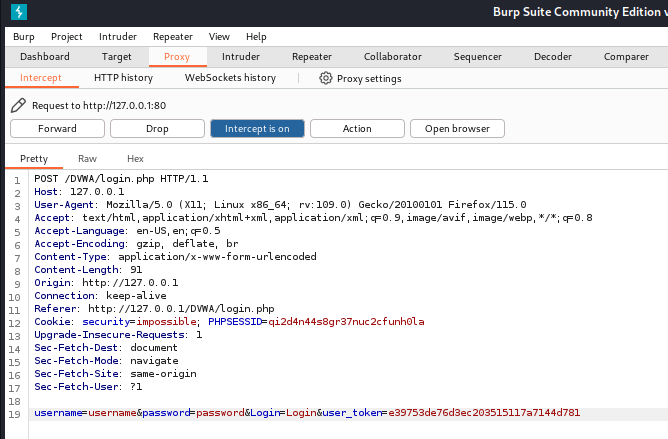
Изменение запроса

История запросов хранится во вкладке Target (рис. [-@fig:013]).



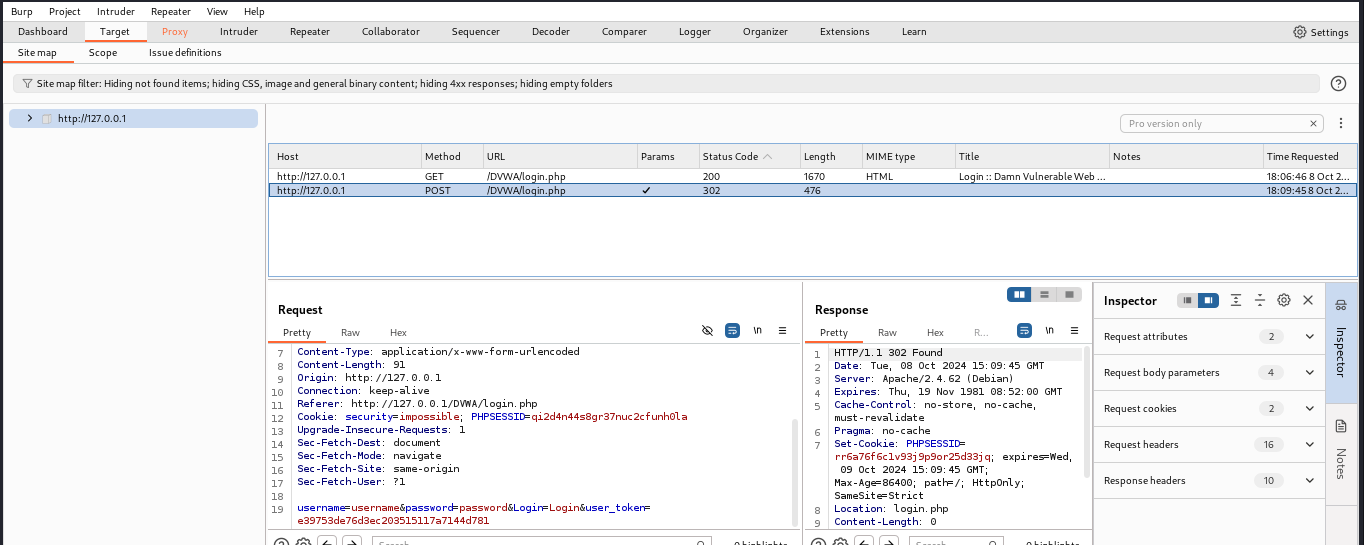
История запросов

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:014]).



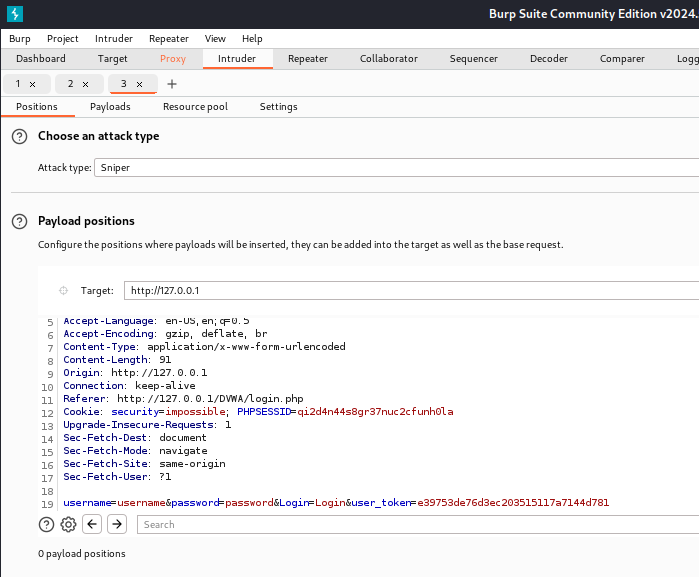
Ввод случайных данных

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:015]).



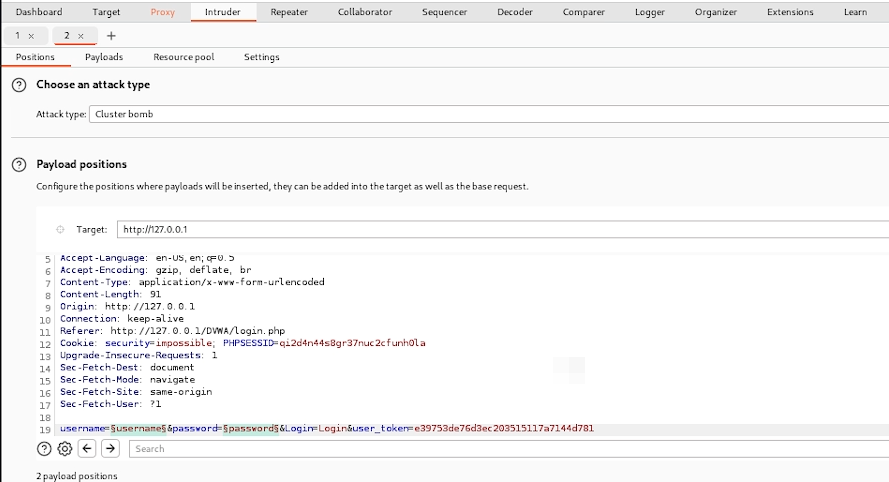
POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:016]).



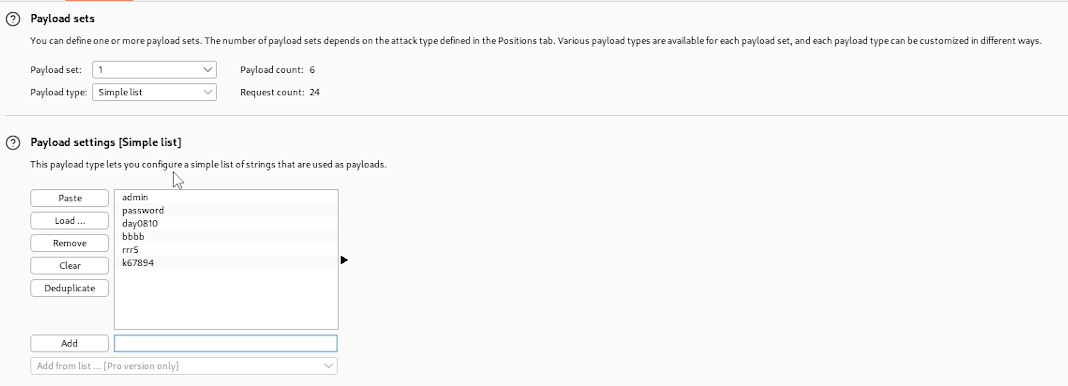
Вкладка Intruder

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:017]).



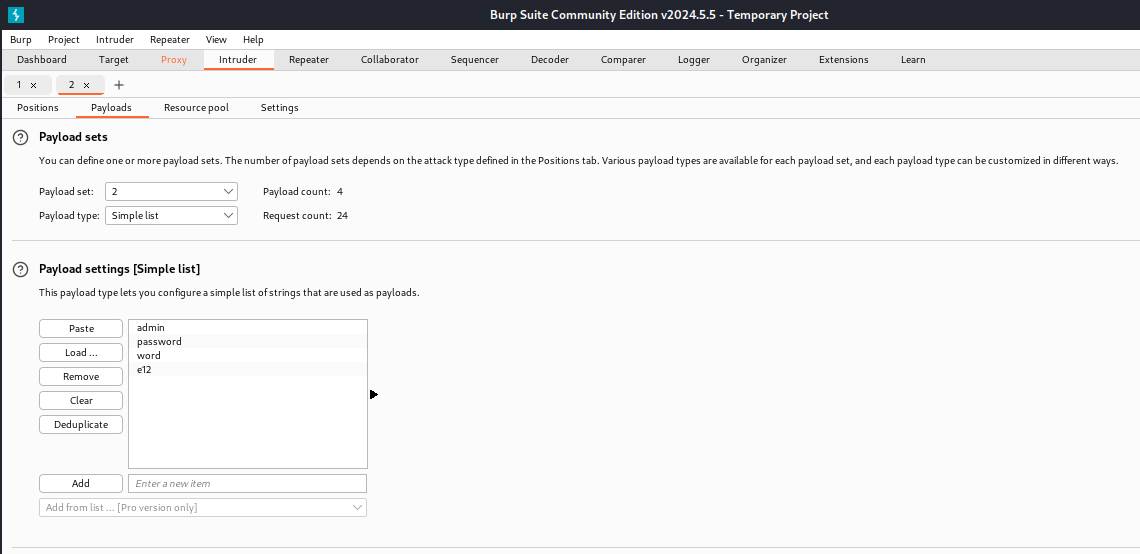
Изменение типа атаки

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:018]).



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:019]).

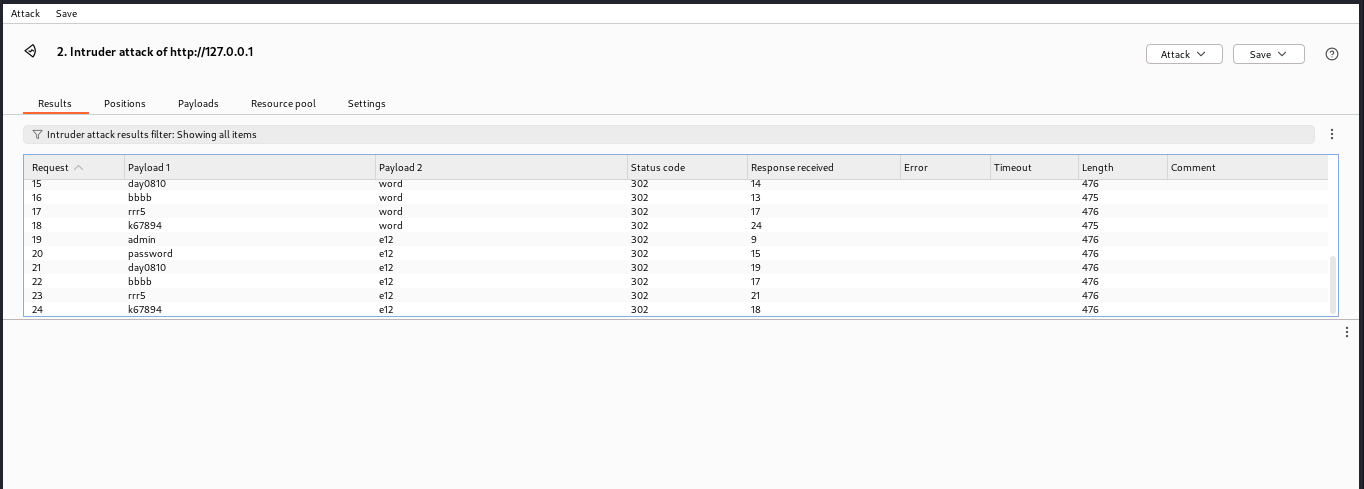


Второй Simple list

Запускаю атаку (рис. [-@fig:020]) и начинаю подбор (рис. [-@fig:021]).

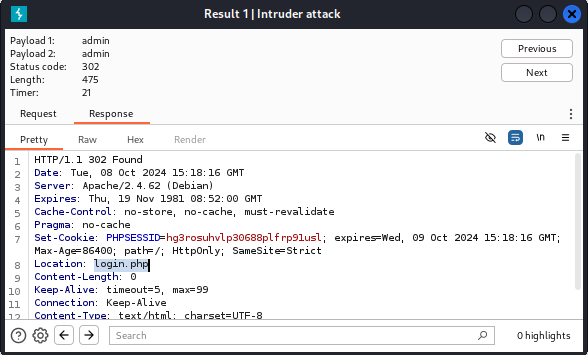
Запуск атаки

Запуск атаки



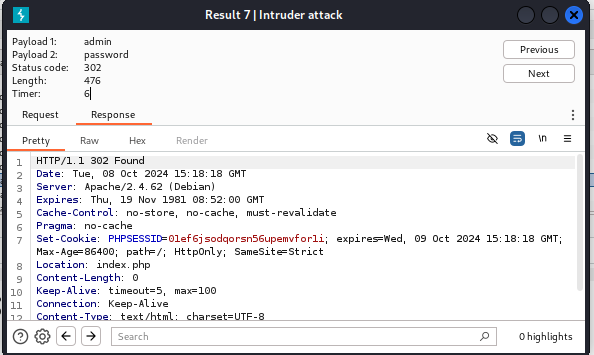
Подбор логина и пароля

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:022]).



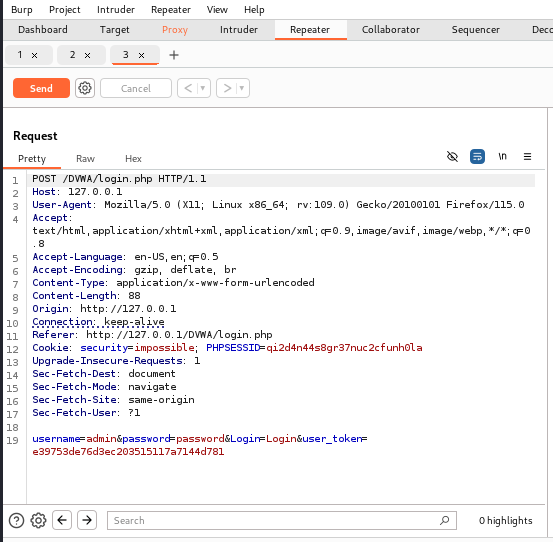
Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [-@fig:023]).



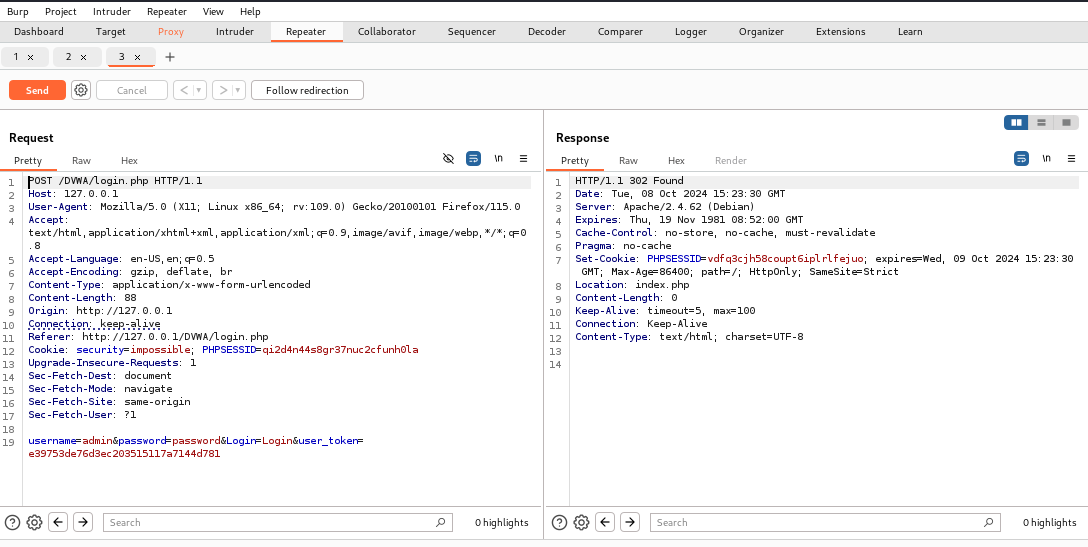
Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater”. Переходим во вкладку “Repeater” (рис. [-@fig:024]).



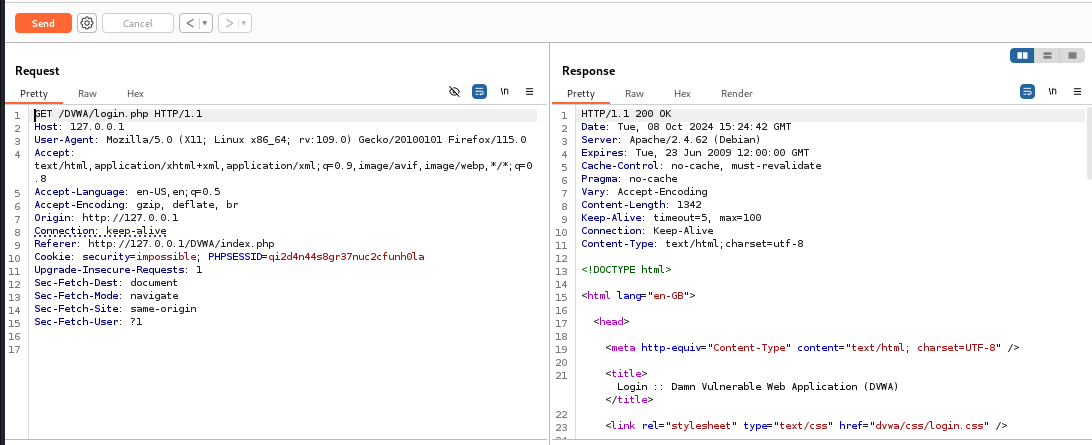
Вкладка Repeater после доп. проверки результата

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. [-@fig:025]).



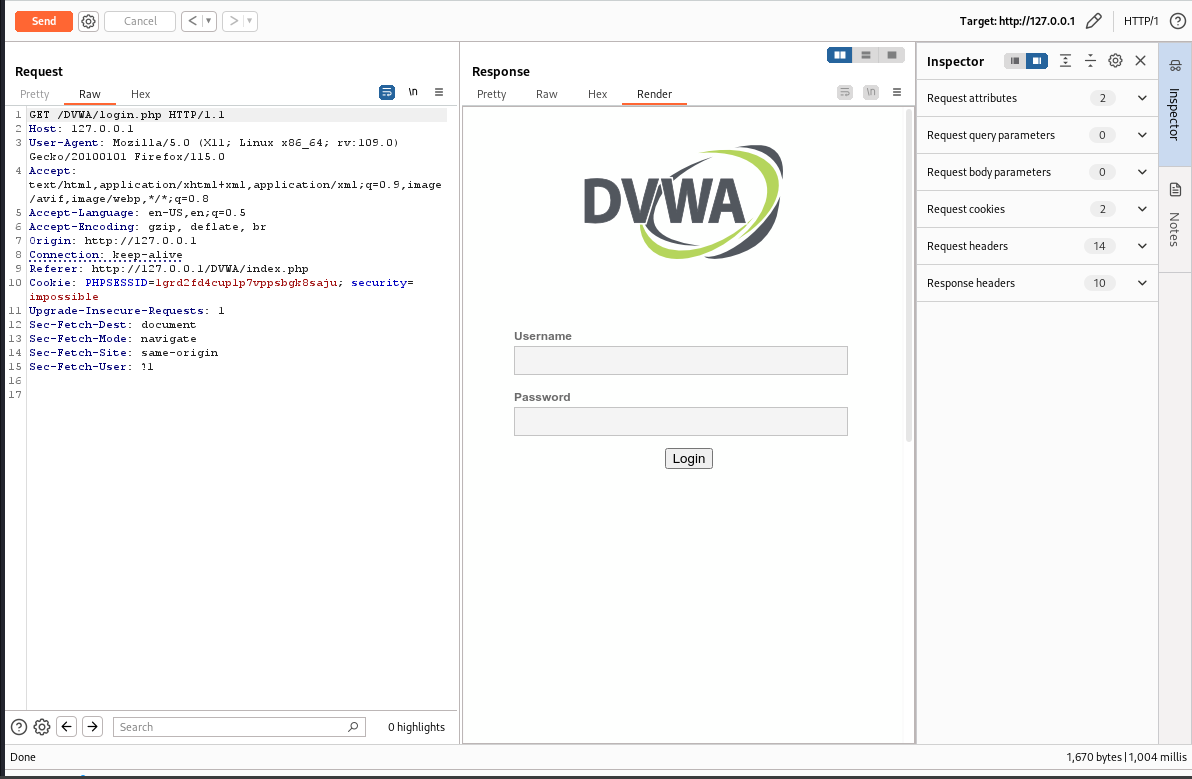
Окно Response

После нажатия на Follow redirection, получим нескомпилированный html код в окне Response (рис. [-@fig:026]).



Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [-@fig:027]).



Полученная страница

# Выводы

При выполнении 5-го этапа индивидуального проекта научилась использовать инструмент Burp Suite в Kali Linux.

# Список литературы

1. Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.