Отчет по 5 этапу индивидуального проекта

Основы информационной безопасности

Чванова Ангелина Дмитриевна, НПИбд02-21

Содержание

Список иллюстраций

Список таблиц

Цель работы

Научиться использовать Burp Suite.

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.

Выполнение лабораторной работы

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

Рис. 1: Запуск локального сервера

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

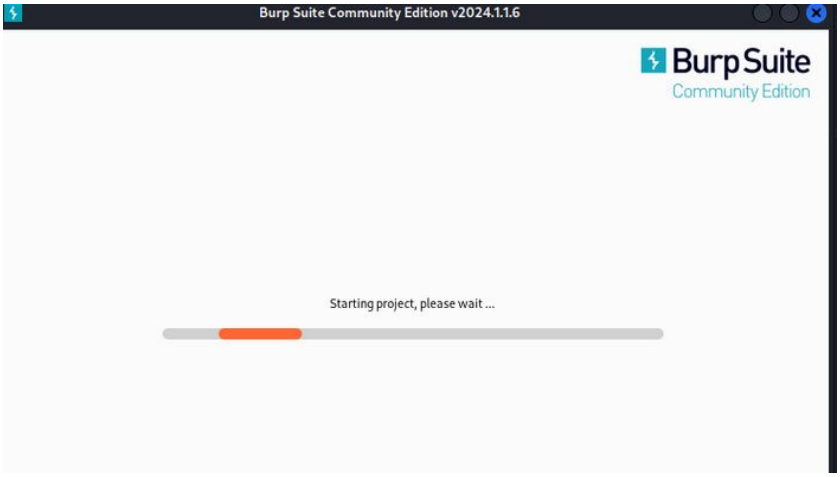

Рис. 2: Запуск приложения

Открываем сетевые настройки браузера для подготовки к работе (рис. [-@fig:003]).

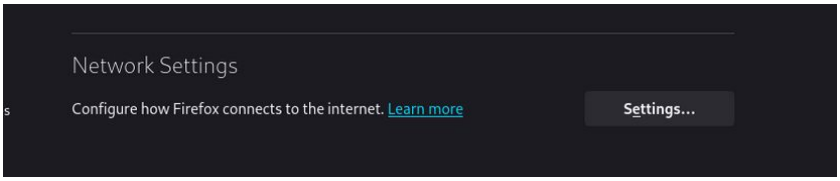

Рис. 3: Сетевые настройки браузера

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

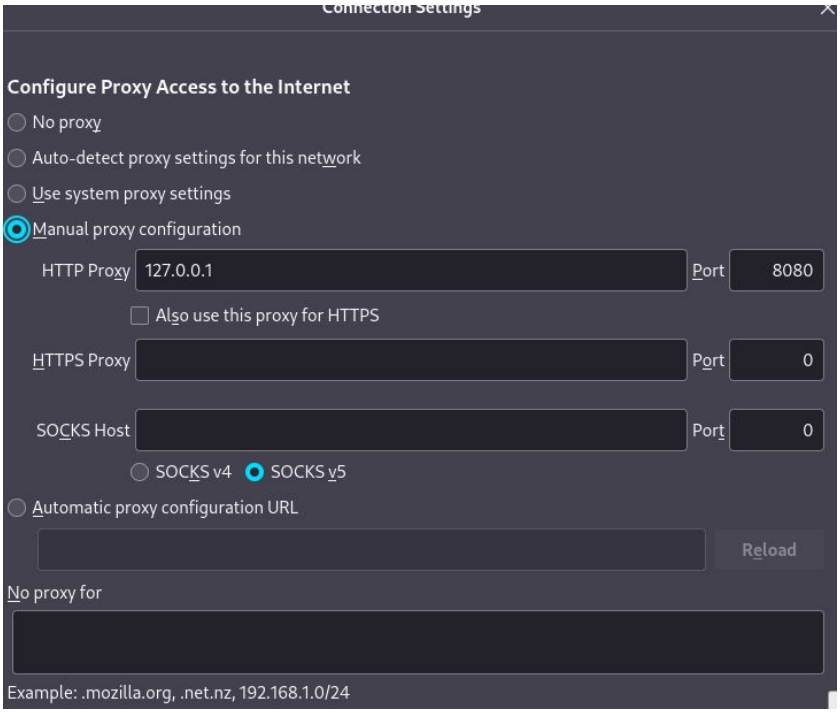

Рис. 4: Настройки сервера

Изменяем настройки Proxy инструмента Burp Suite (рис. [-@fig:005]).

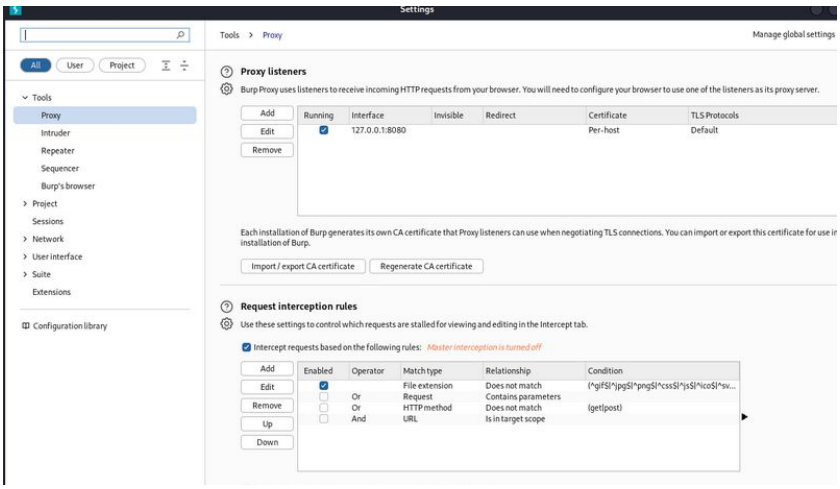

Рис. 5: Настройки Burp Suite

Устанавливаем значение “Intercept is on” во вкладке Proxy (рис. [-@fig:006]).

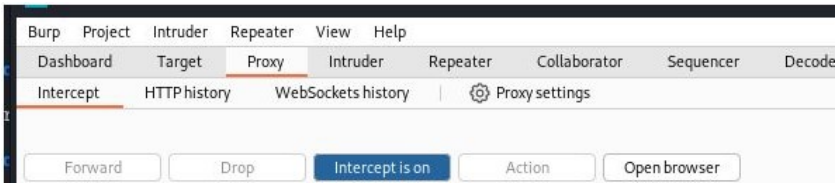

Рис. 6: Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_loacalhost` на `true` (рис. [-@fig:007]).

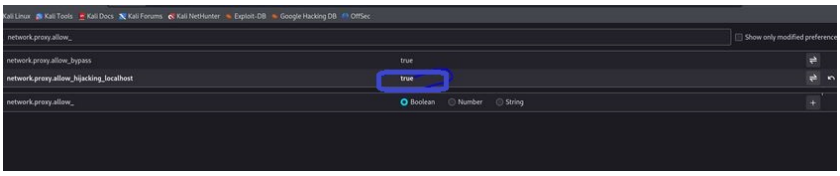

Рис. 7: Настройки параметров

При входе в браузер на DVWA, во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:008]).

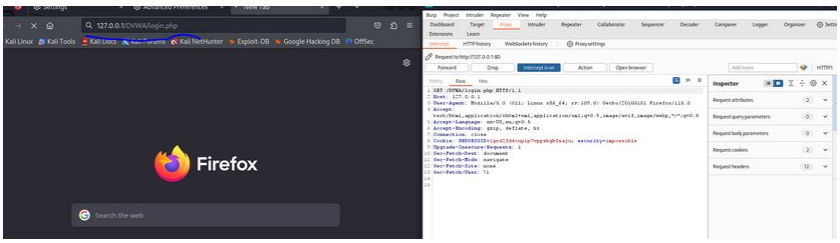

Рис. 8: Получаемые запросы сервера

Загружаем страницу авторизации, текст запроса поменялся (рис. [-@fig:009]).

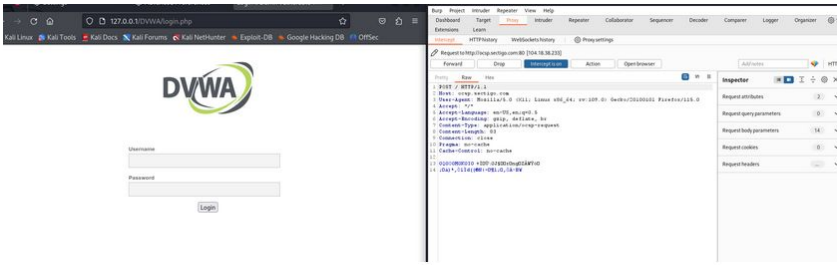

Рис. 9: Страница авторизации

История запросов хранится во вкладке Target (рис. [-@fig:010]).

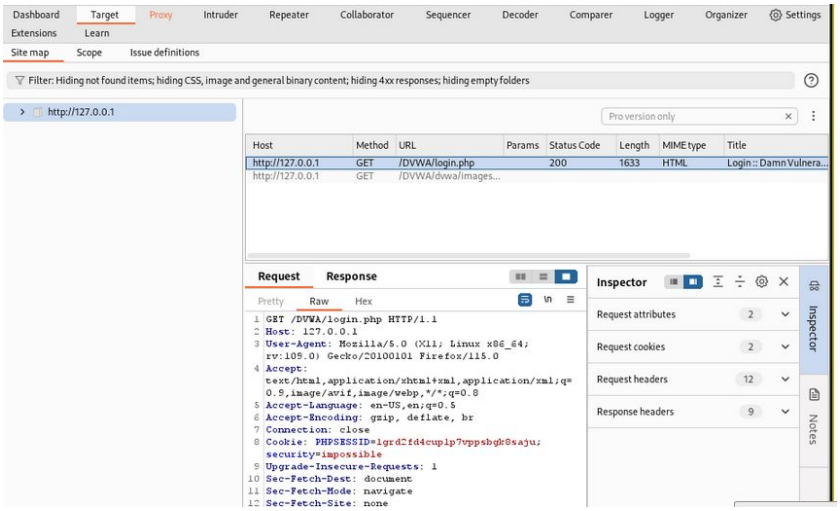

Рис. 10: История запросов

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. [-@fig:011]).

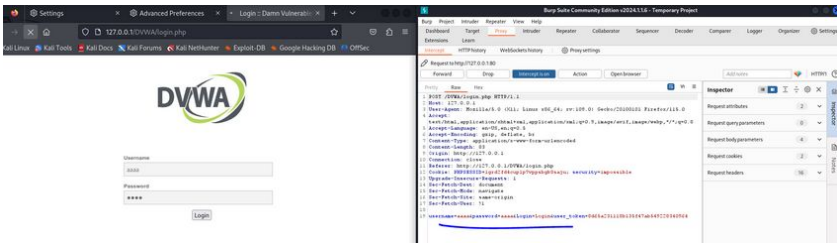

Рис. 11: Ввод случайных данных

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. [-@fig:012]).

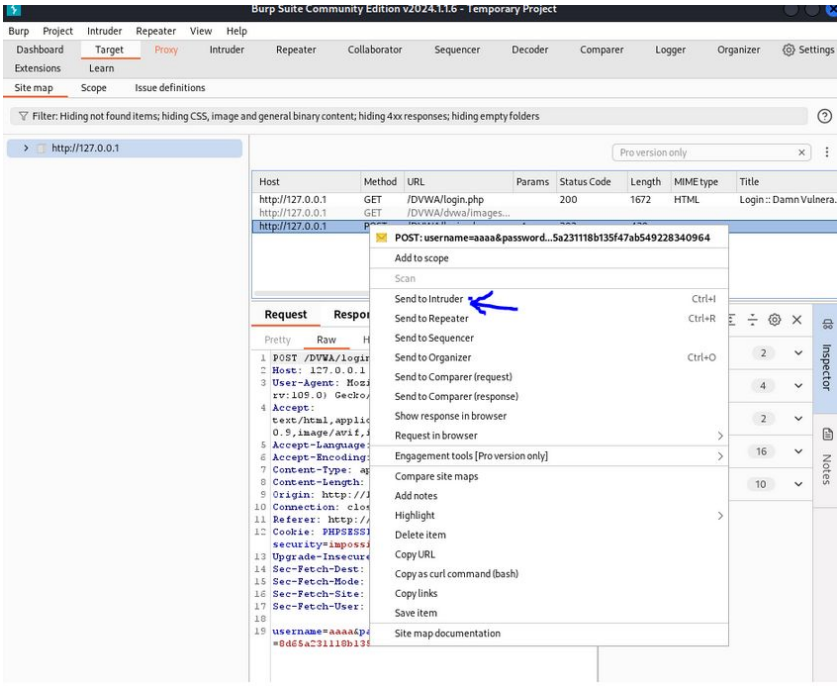

Рис. 12: POST-запрос с вводом пароля и логина

На вкладке Intruder видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:013]).

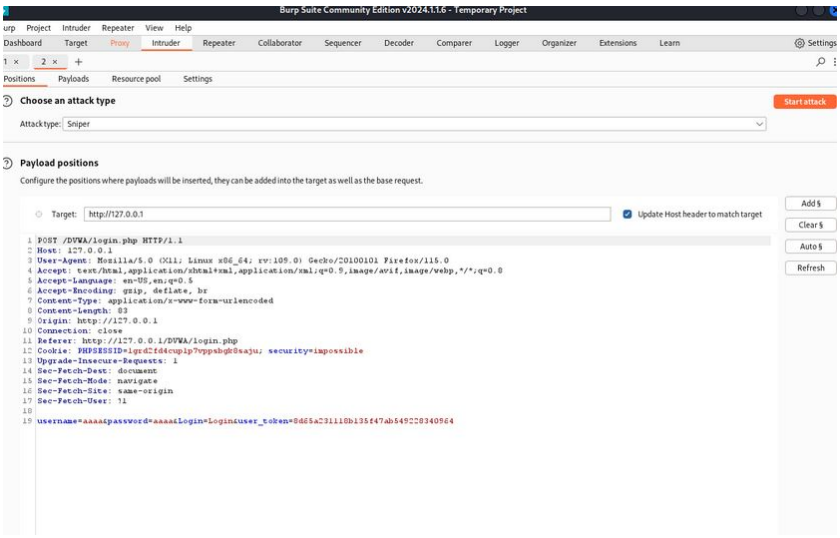

Рис. 13: Вкладка Intruder

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. [-@fig:014]).

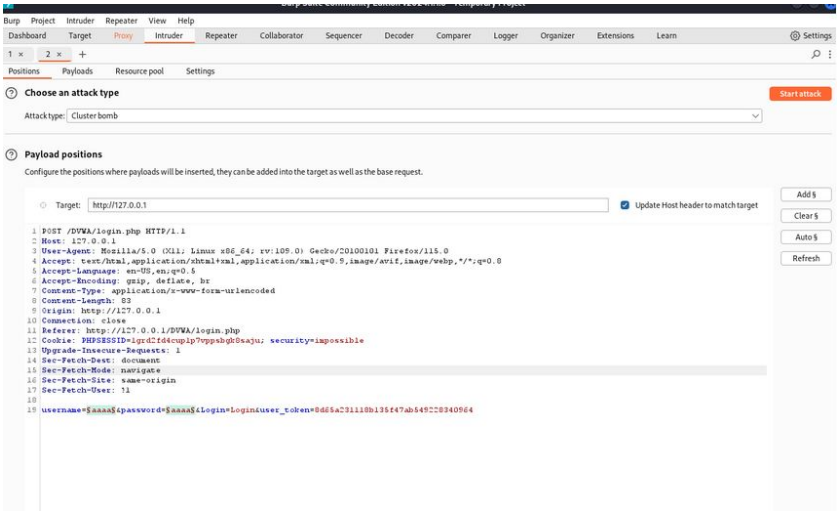

Рис. 14: Изменение типа атаки

Так как мы отметили 2 параметра для подбора, то нам необходимо 2 списка со значениями для подбора. Заполняем первый список в `Payload setting` (рис. [-@fig:015]).

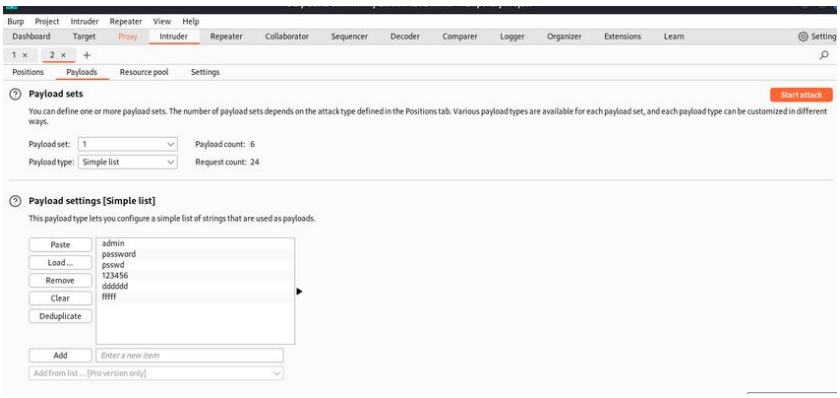

Рис. 15: Первый Simple list

Заполняем значениями второй список. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль (рис. [-@fig:016]).

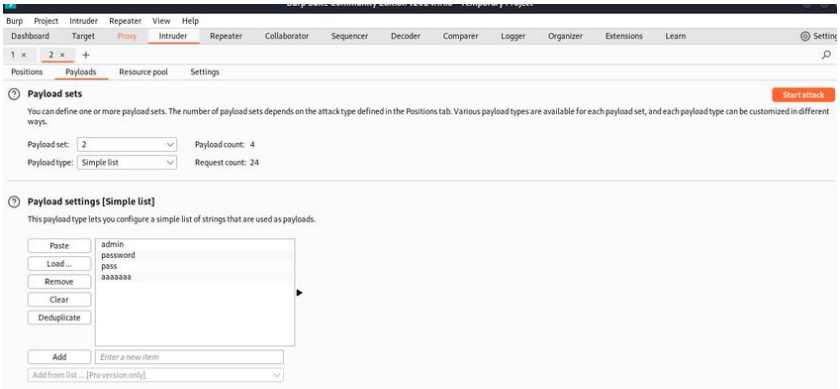

Рис. 16: Второй Simple list

Запускаем атаку и начинаем подбор (рис. [-@fig:017]).

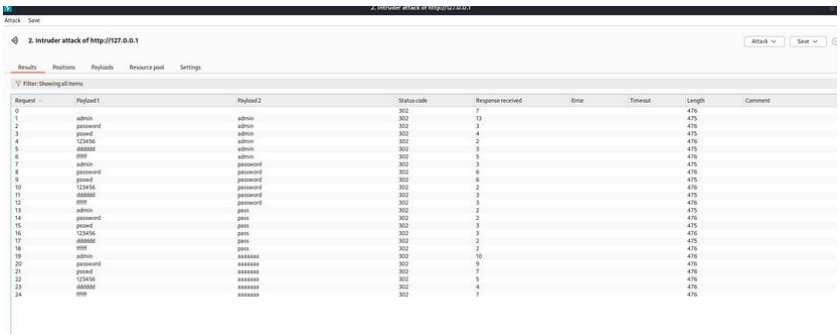

Рис. 17: Запуск атаки

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. [-@fig:018]).

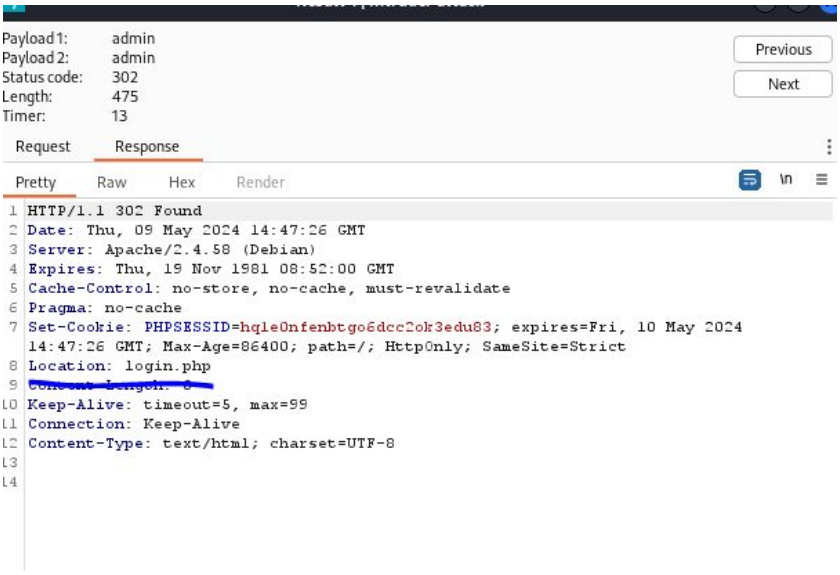

Рис. 18: Результат запроса

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

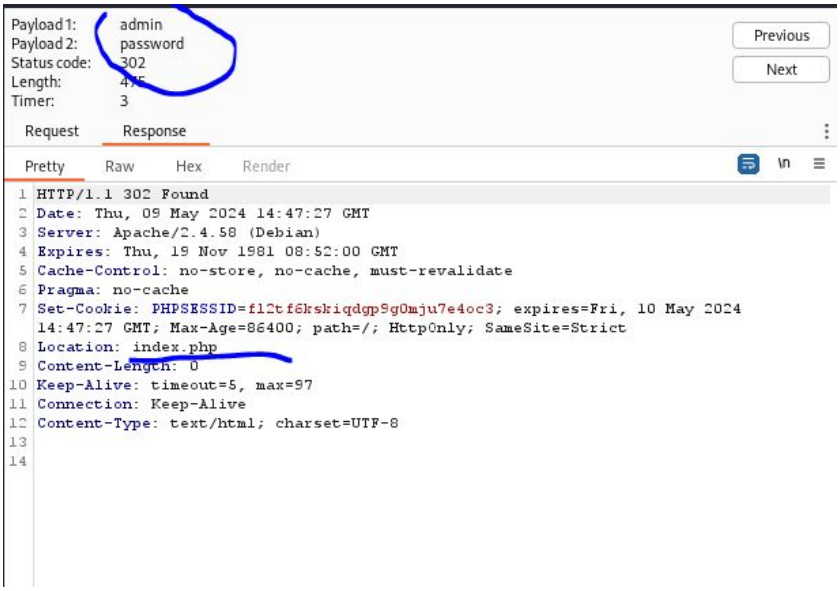

Рис. 19: Результат запроса

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

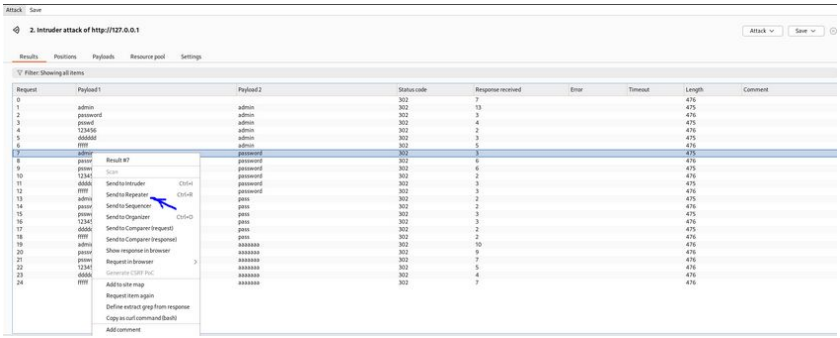

Рис. 20: Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. [-@fig:021]).

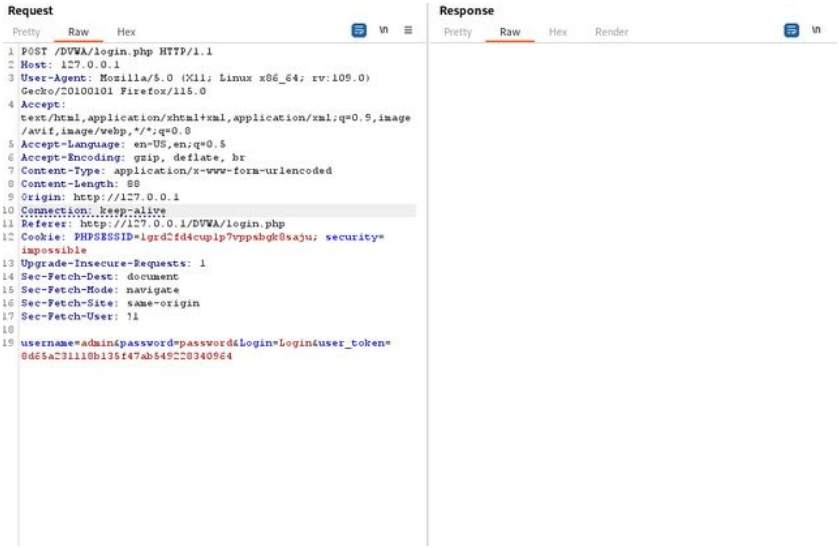

Рис. 21: Вкладка Repeater

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

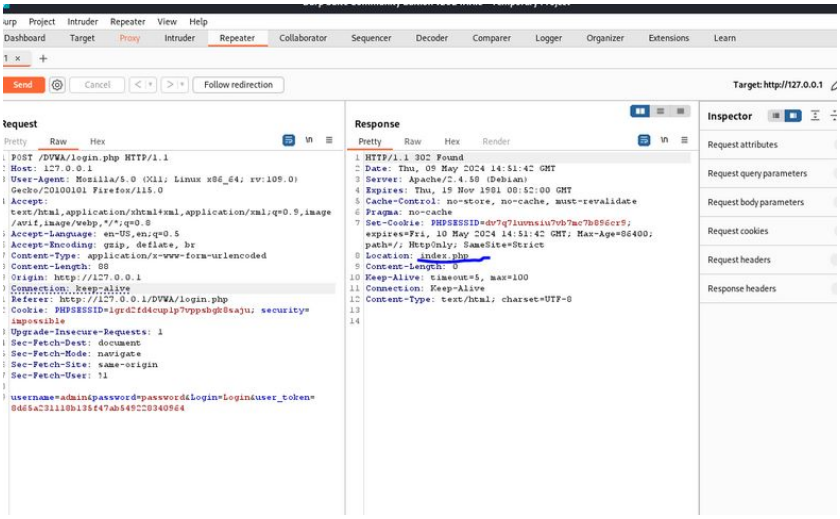

Рис. 22: Окно Response

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

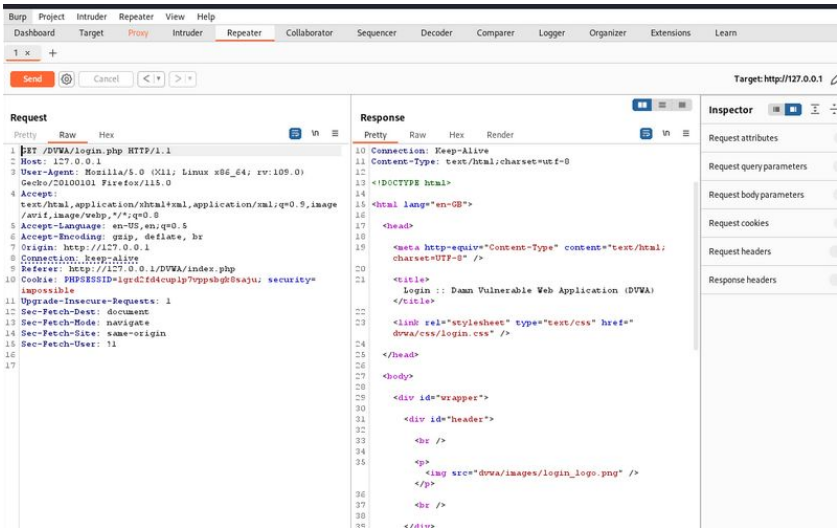

Рис. 23: Изменение в окне Response

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

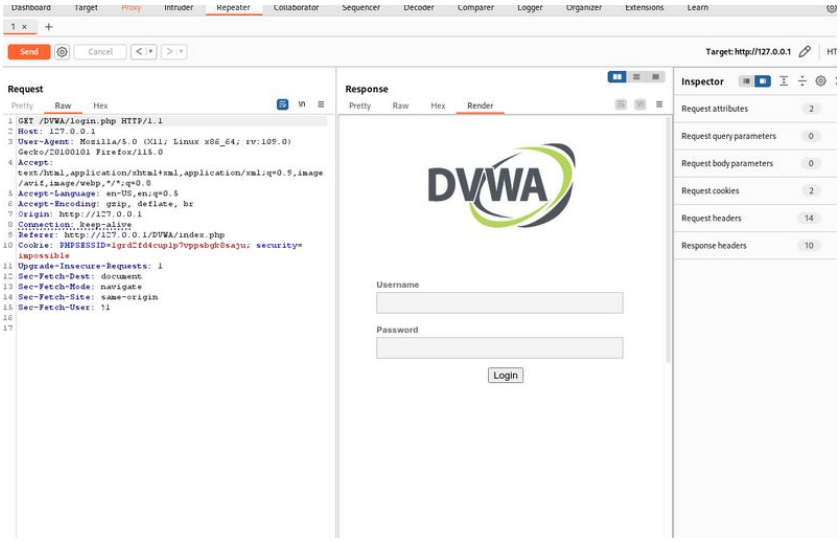

Рис. 24: Полученная страница

Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

Список литературы

[1] Документация по Virtual Box: https://www.virtualbox.org/wiki/Documentation

[2] 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