Отчет по пятому этапу индивидуального проекта

Информационная безопасность

Кармацкий Никита Сергеевич

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. [**parasram?**].

# 3 Выполнение лабораторной работыё

Запускаем локальный сервер Apache (рис. 1).

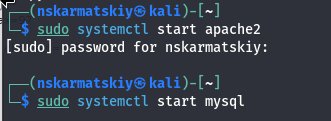


Рис. 1: Запуск локального сервера

Запускаем инструмент Burp Suite (рис. 2).

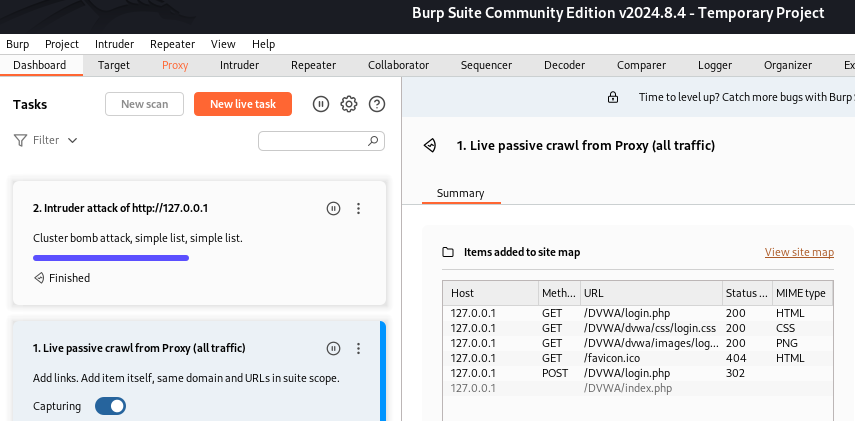


Рис. 2: Запуск приложения

Измененяем настроек сервера для работы с proxy и захватом данных с помощью Burp Suite (рис. 3).

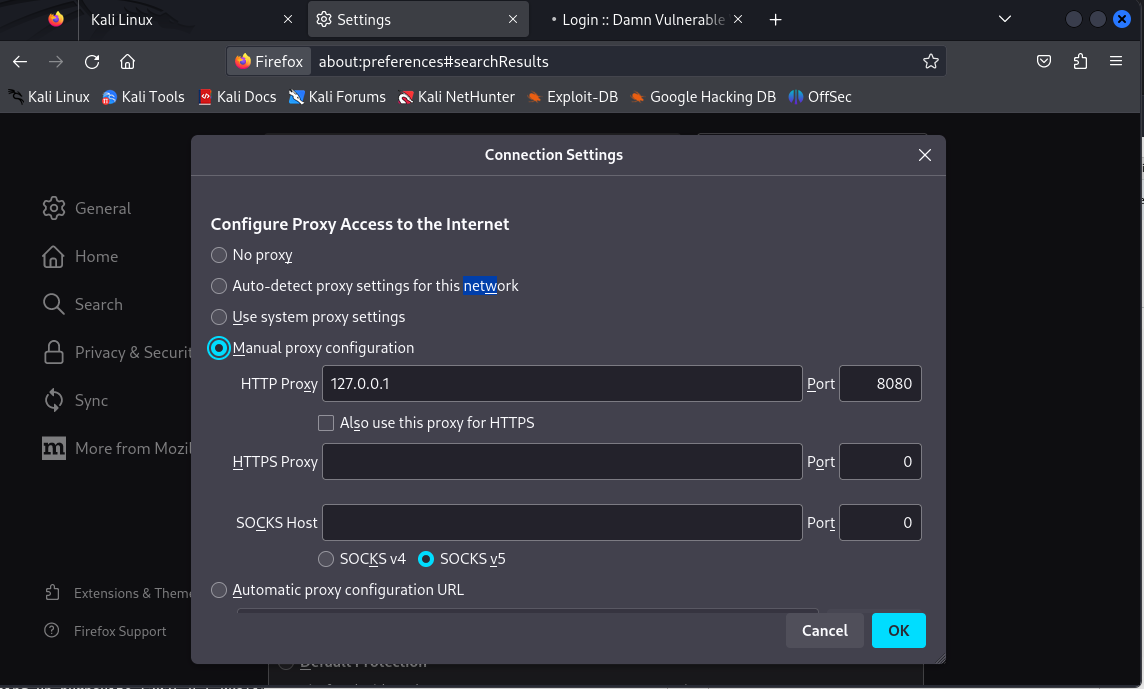


Рис. 3: Настройки сервера

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

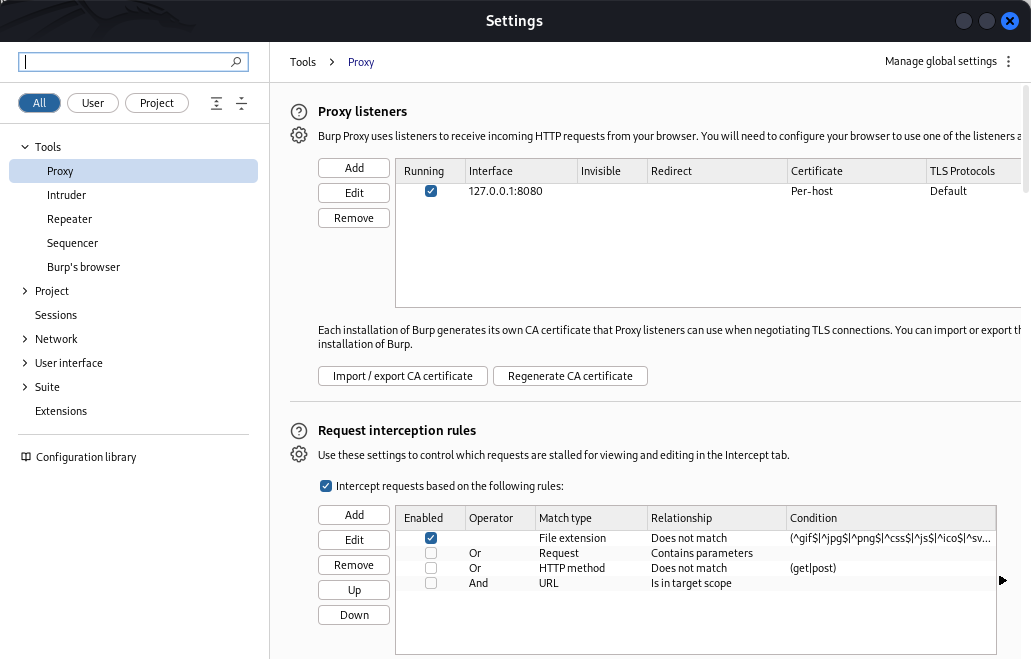


Рис. 4: Настройки Burp Suite

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

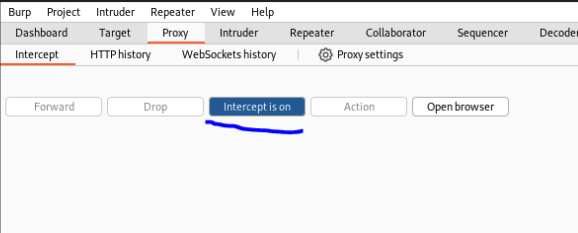


Рис. 5: Настройки Proxy

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

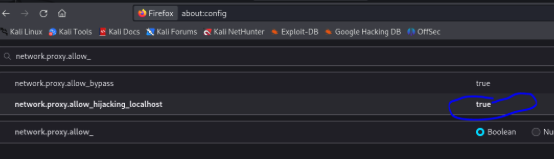


Рис. 6: Настройки параметров

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

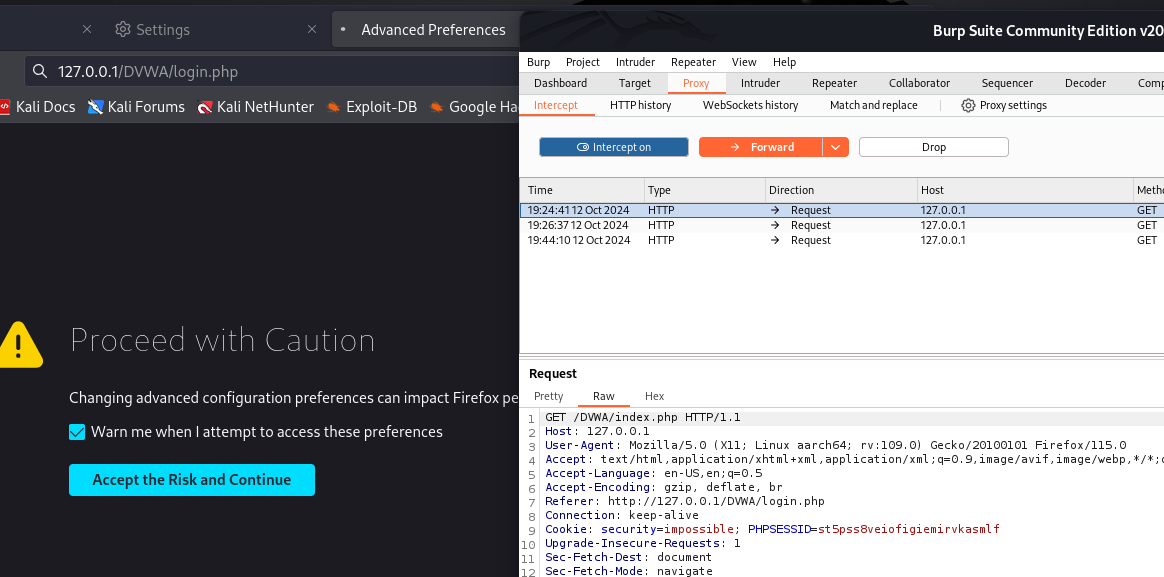


Рис. 7: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. 8).

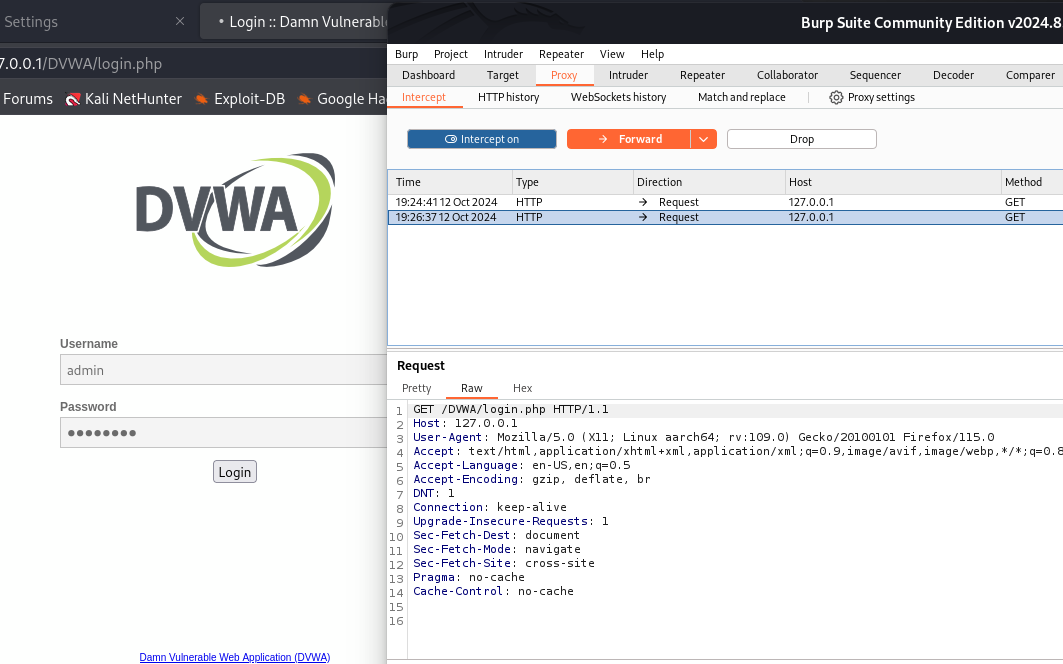


Рис. 8: Страница авторизации

История запросов хранится во вкладке Target (рис. 9).

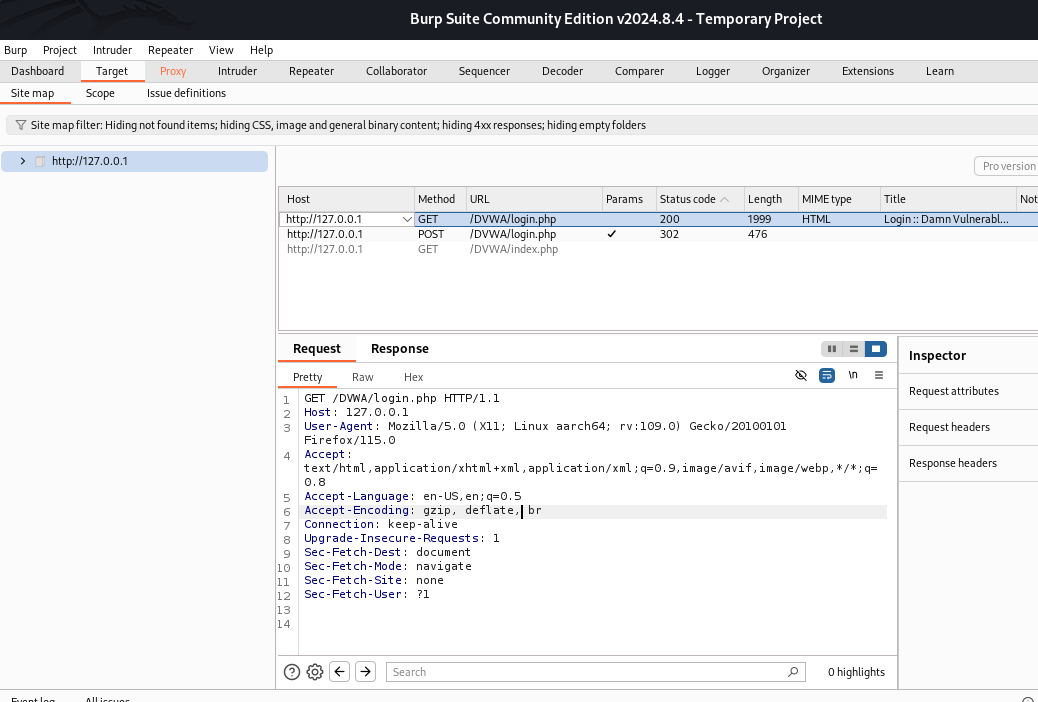


Рис. 9: История запросов

Попробуем ввести данные в веб-приложении и нажмем Login. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода (рис. 10).

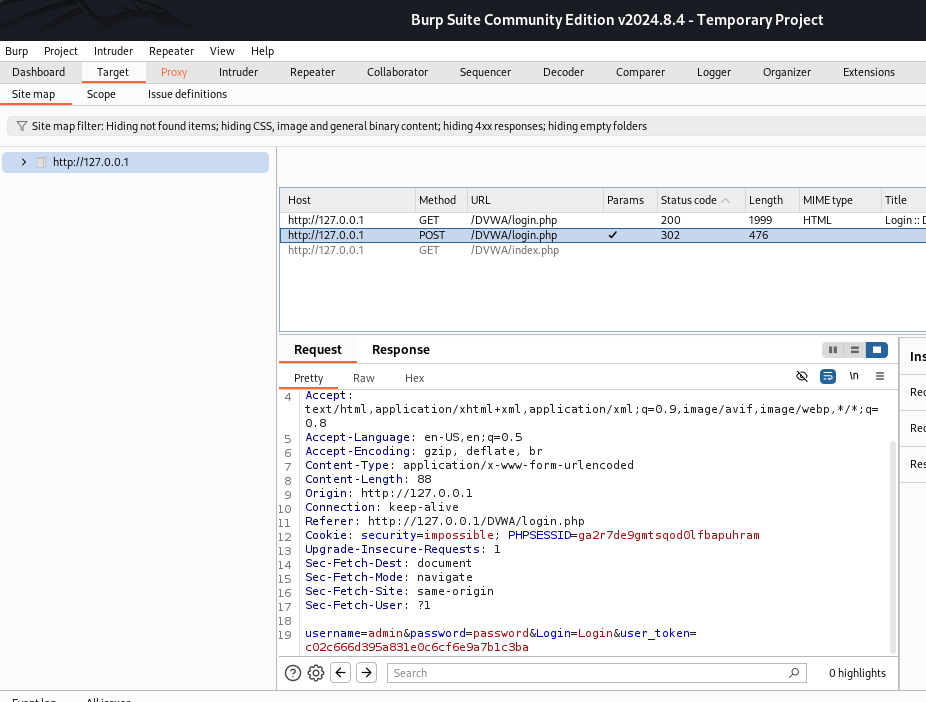


Рис. 10: Ввод случайных данных

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. 11).

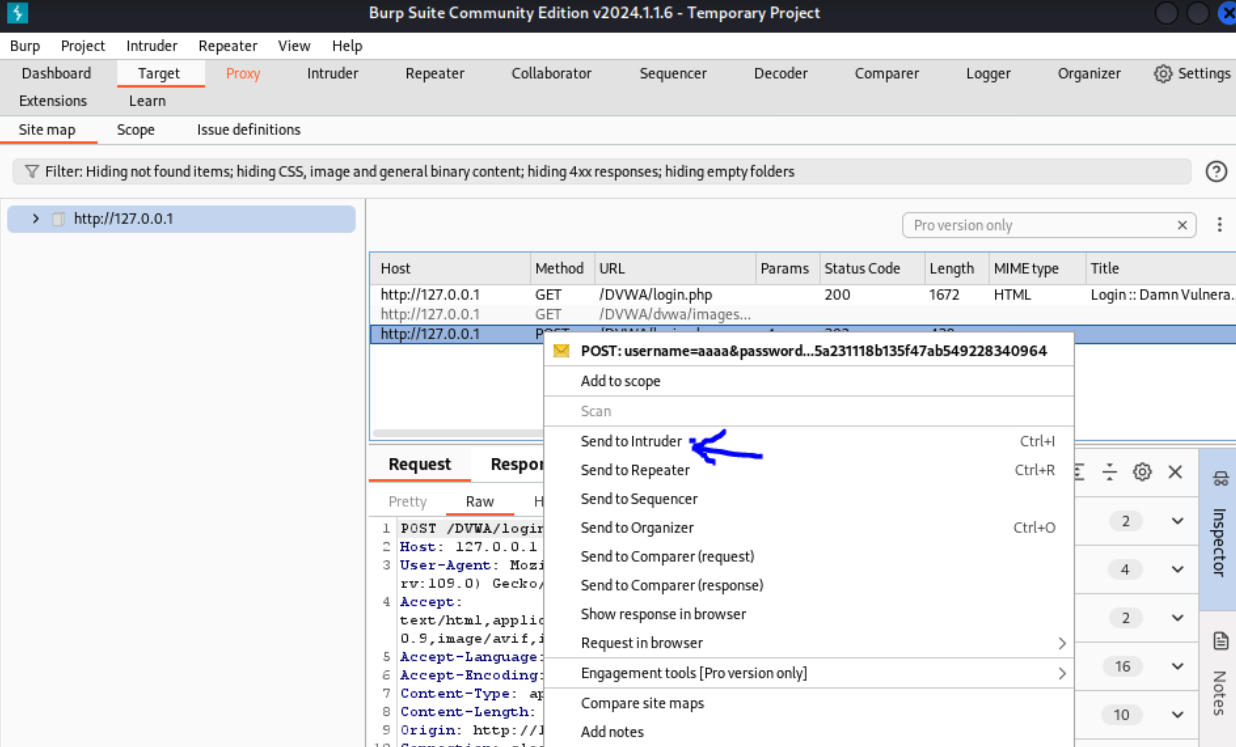


Рис. 11: POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. 12).

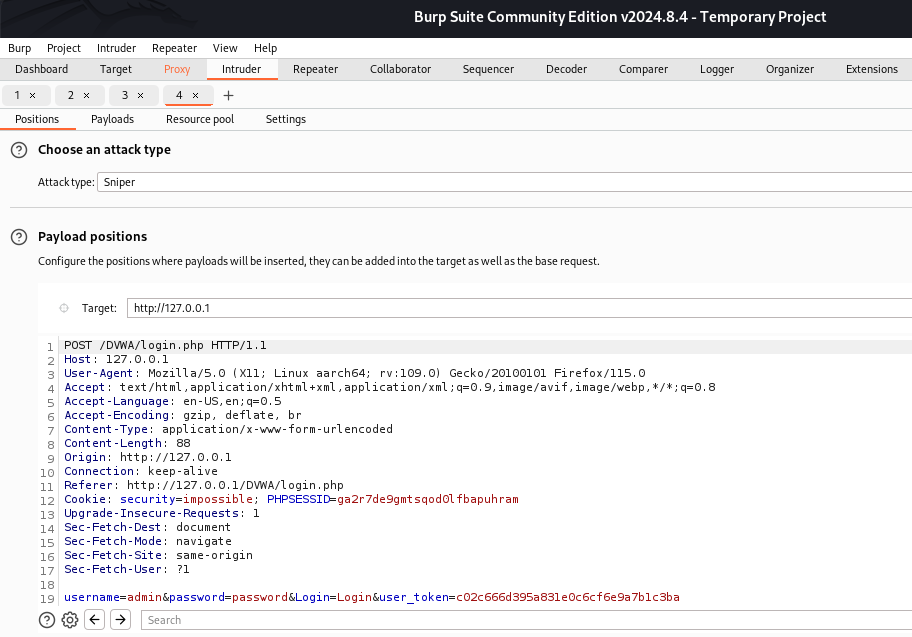


Рис. 12: Вкладка Intruder

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. 13).

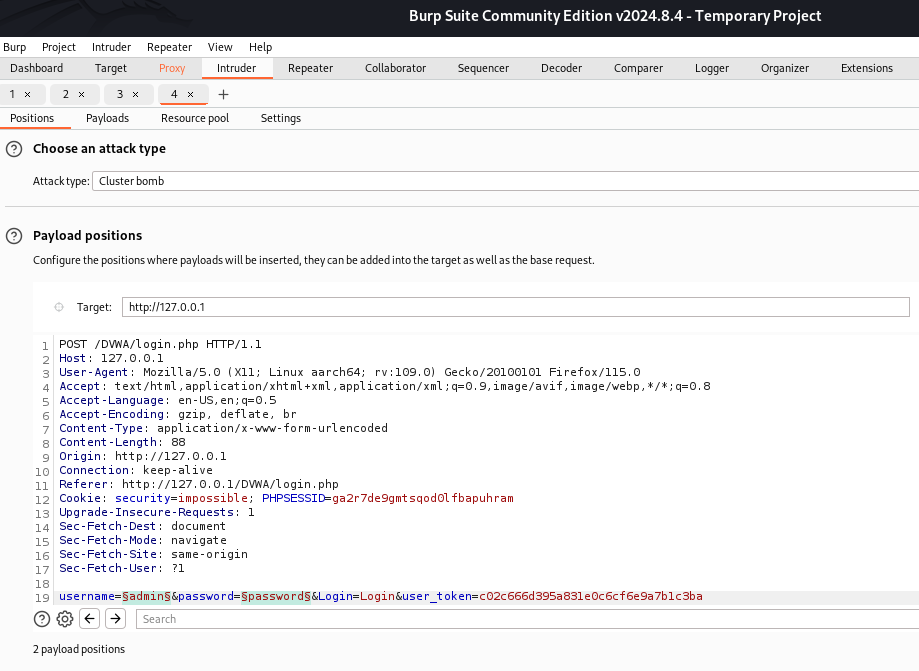


Рис. 13: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. 14).

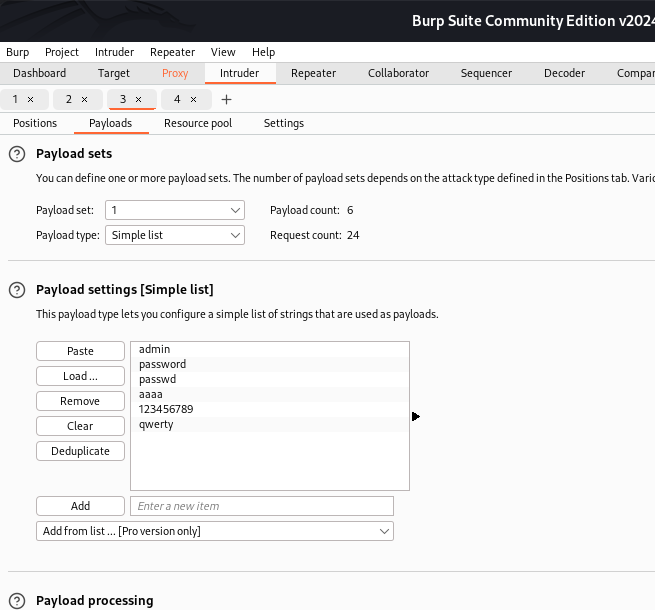


Рис. 14: Первый Simple list

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. 15).

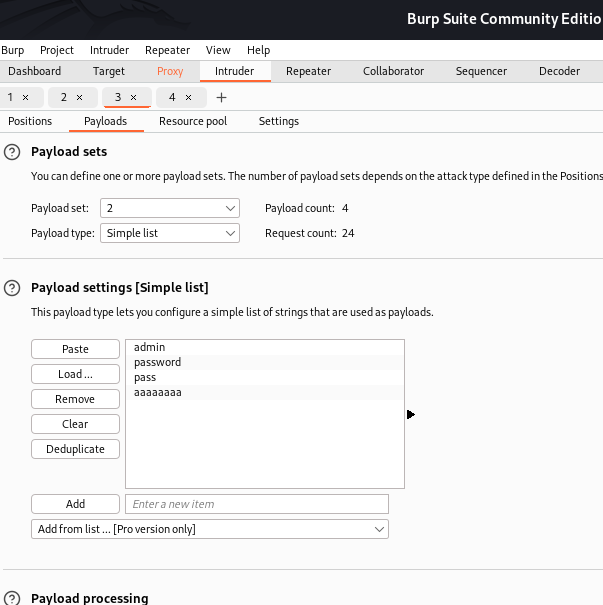


Рис. 15: Второй Simple list

Запускаем атаку и начинаем подбор (рис. 16).

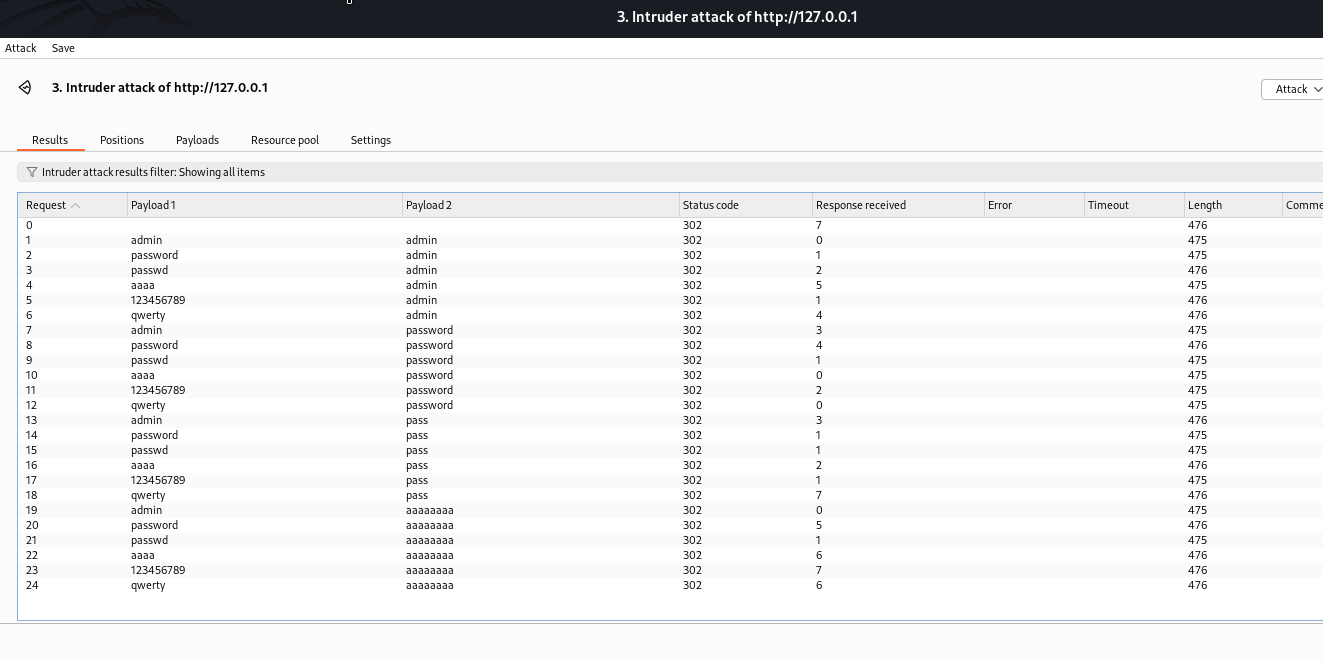


Рис. 16: Запуск атаки

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. 17).

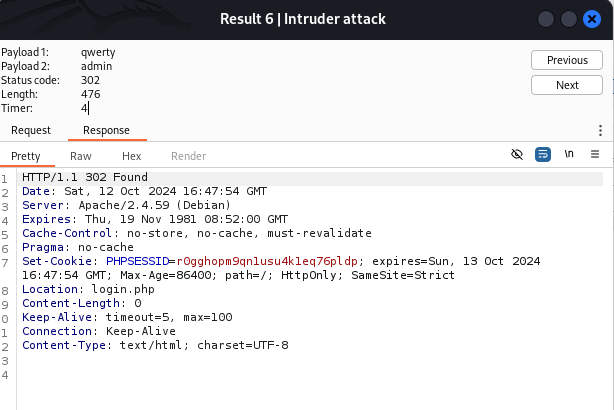


Рис. 17: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. 18).

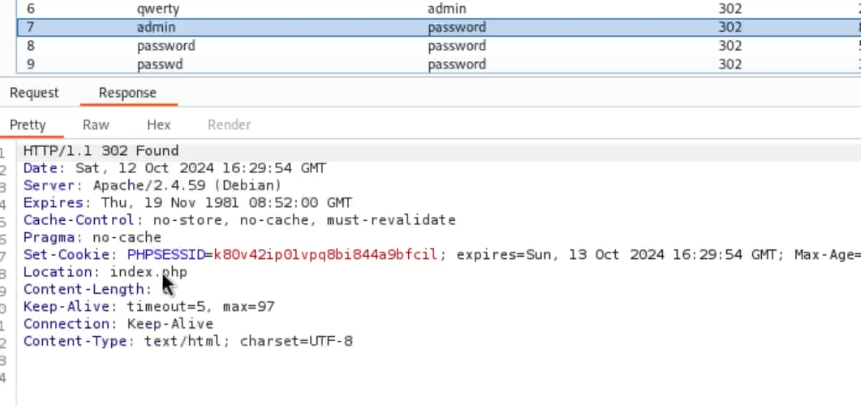


Рис. 18: Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater” (рис. 19).

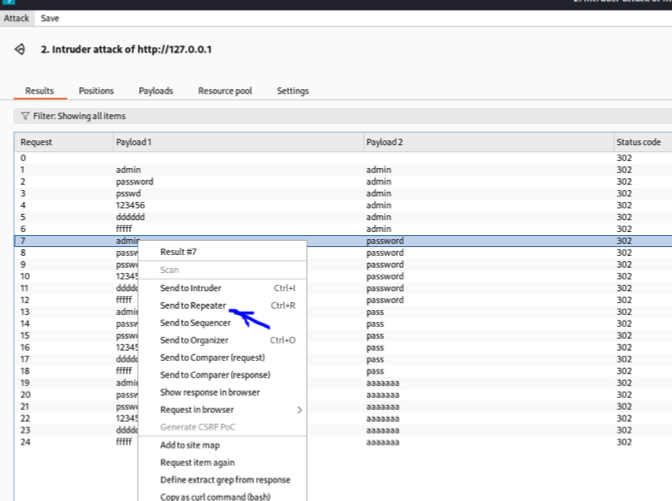


Рис. 19: Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. 20).

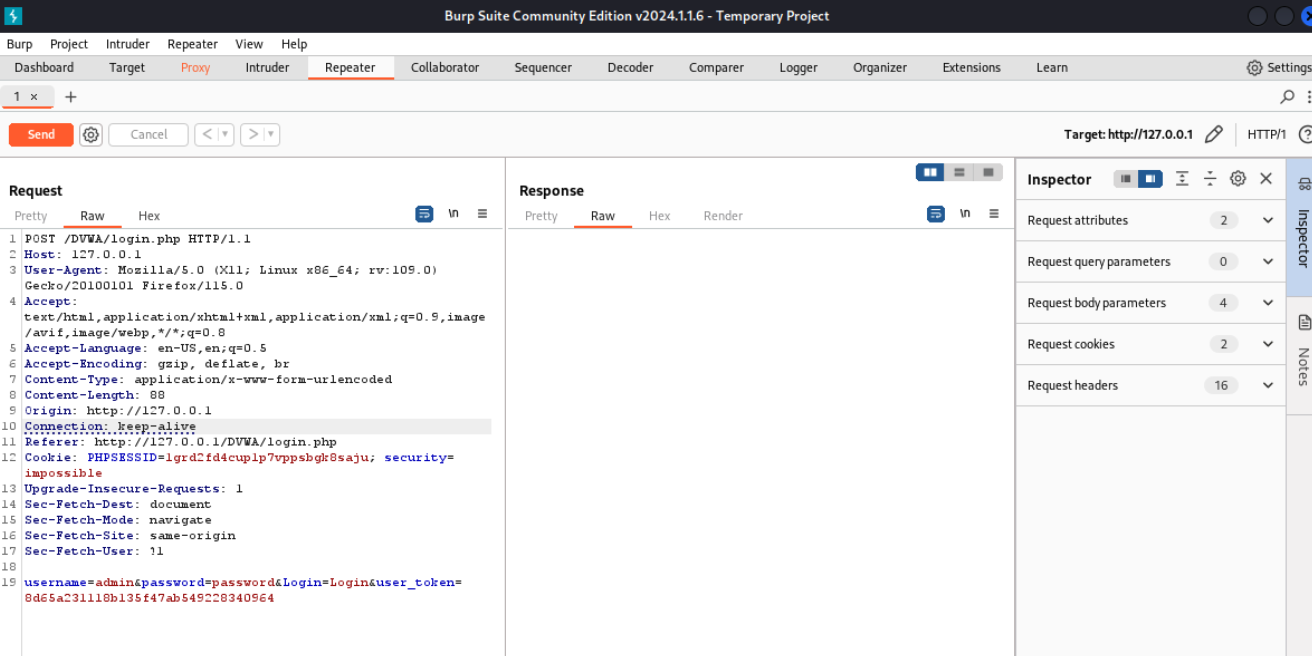


Рис. 20: Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. 21).

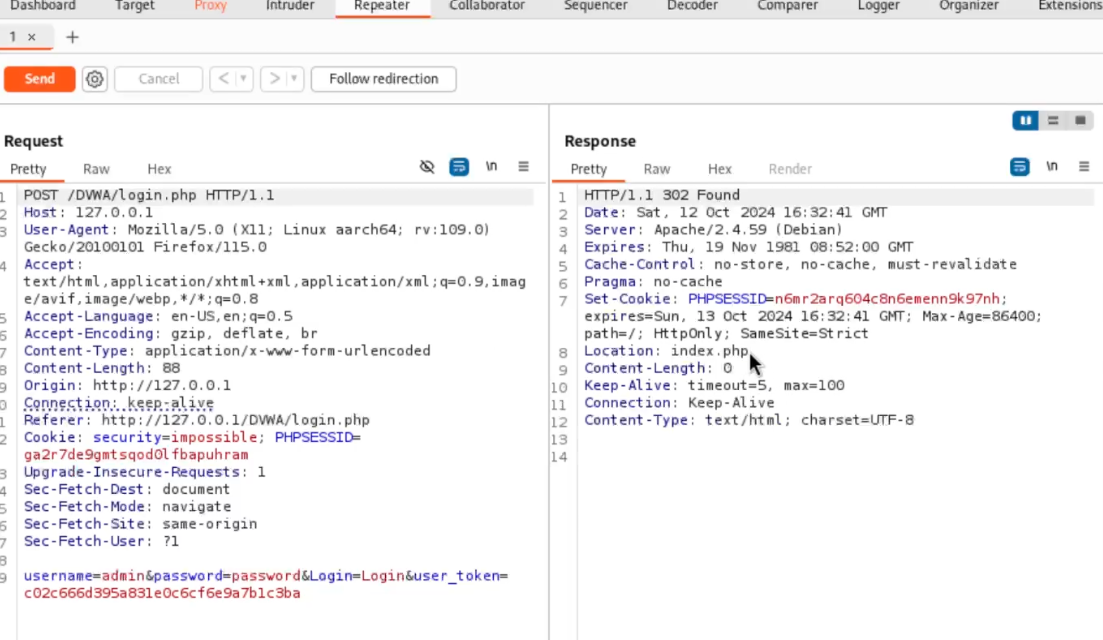


Рис. 21: Окно Response

После нажатия на Follow redirection, получим нескомпилированный html код в окне Response (рис. 22).

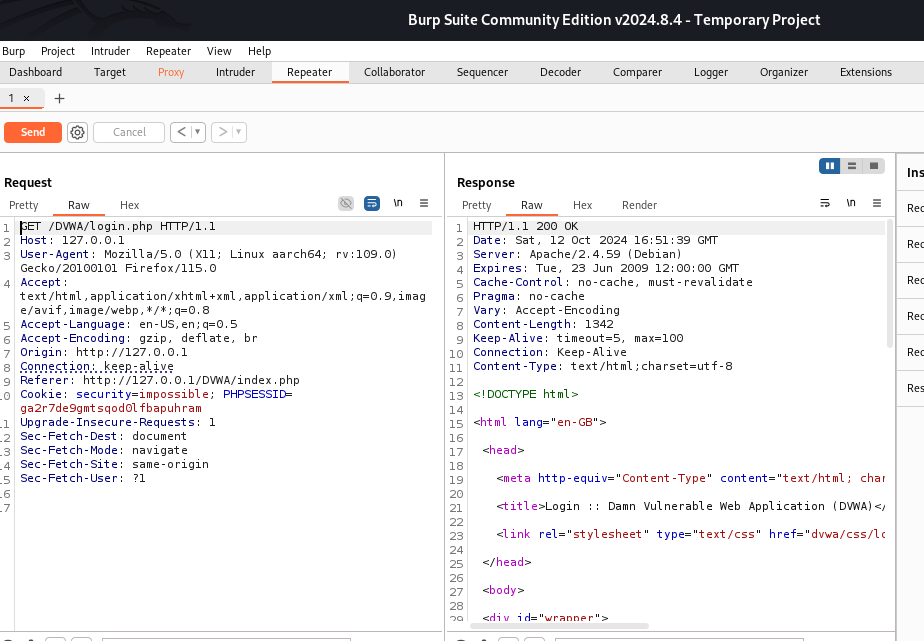
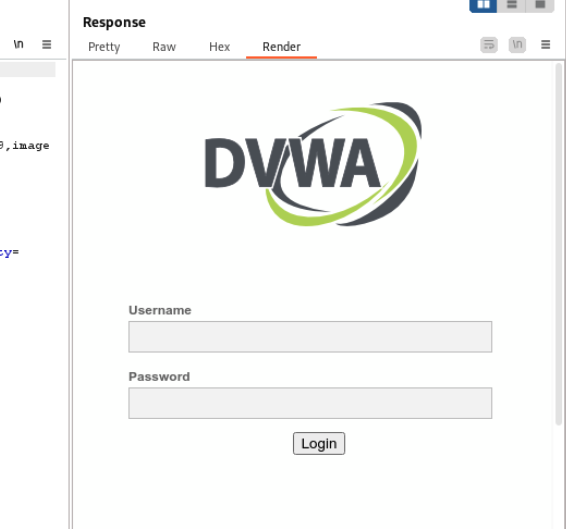


Рис. 22: Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. **¿fig:023?**).

 # Вывод

Научились использовть инструмент Burp Suite

# 4 Список литературы