Отчёт по пятому этапу индивидуального проекта

Burp Suite

Вакутайпа Милдред

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Научиться использовть Burp Suite.

# 2 Выполнение лабораторной работы

Запускаю локальный серевер DVWA:

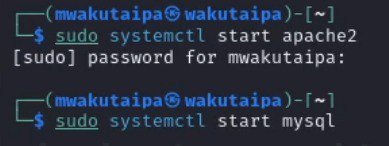


Рис. 1: Запуск сервера

Запускаю burp suite:



Рис. 2: Запуск Burp suite

Открываю сетевые настройки браузера и изменяю настройки сервера для работы с proxy и захватом данных с burp suite:

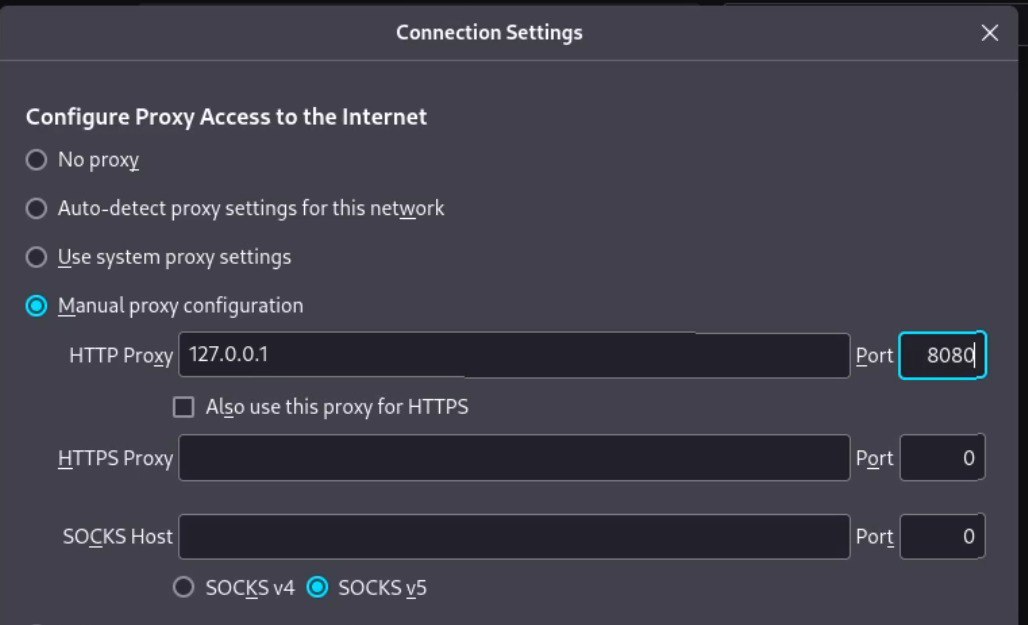


Рис. 3: сетевые настройки сервера

Изменяю настройки proxy инструмента burp suite:

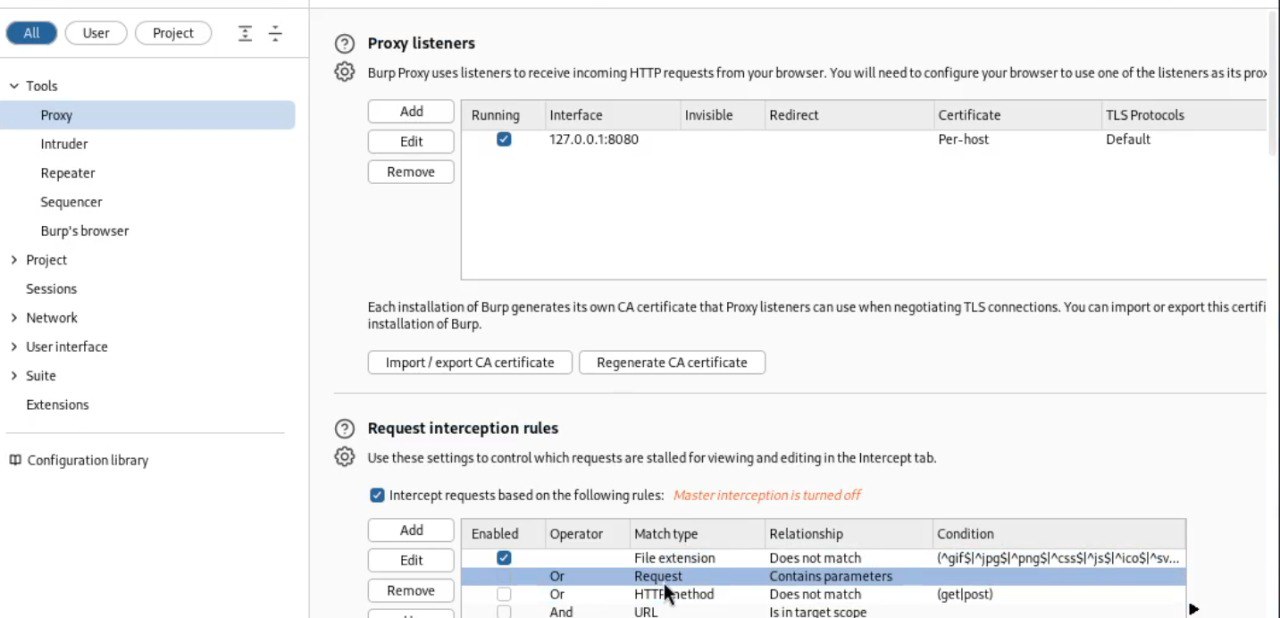


Рис. 4: настройки proxy

Включаю intercept во вкладе proxy:



Рис. 5: Включение intercept

Необходимо установить параметр network\_allow\_hijacking\_localhost на true ,чтобы burp suite работал с локальным сервером. Я это и делала:

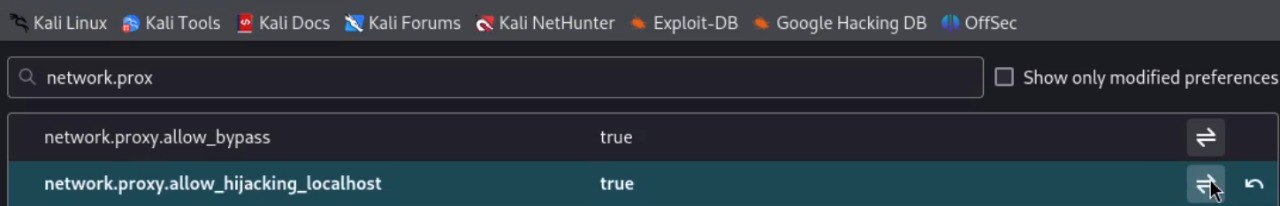


Рис. 6: Установка параметра локального хоста

Пытаюсь зайти на dvwa в браузаре и во вкладки proxy появляется запрос. Нажимаю forward, чтобы загрузить страницу:

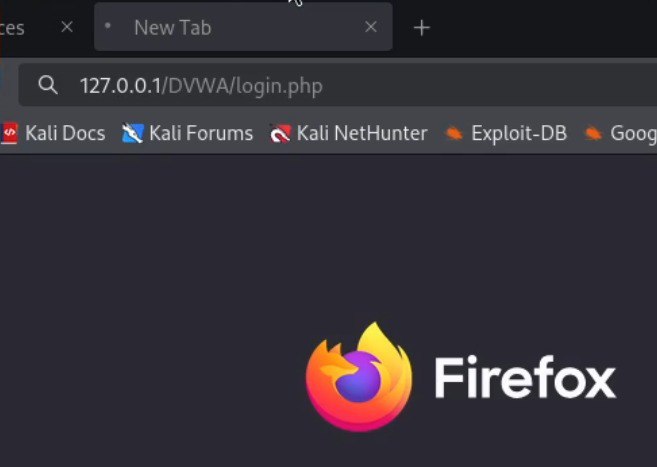


Рис. 7: Пытка зайти в dvwa

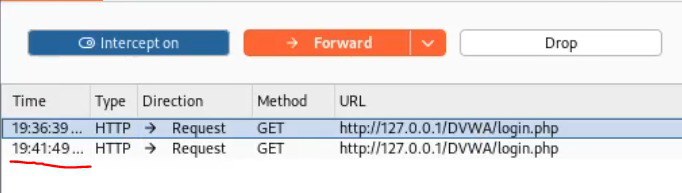


Рис. 8: вкладка proxy

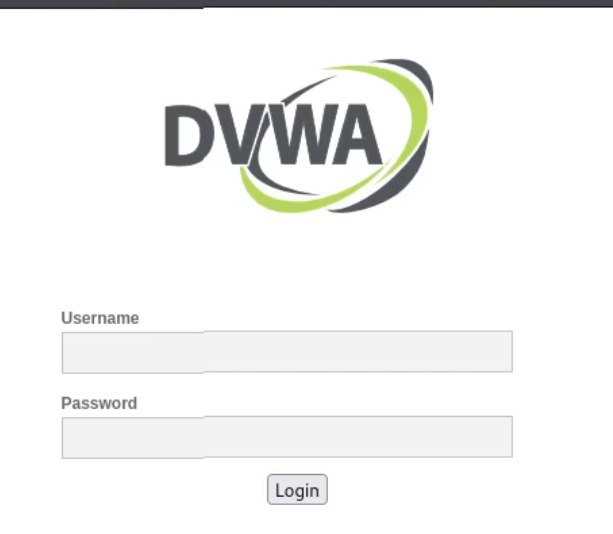


Рис. 9: окно dvwa

Когда пытаюсь ввести неправильные логин и пароль, в запросе появляется строка, в которой отображается введенные данные. Этот же запрос ,во вкладке target, отправила к злоумышленнику (send to intruder). Во вкладке intruder, изменяю тип атаки (на cluster bomb) и данные для входа.

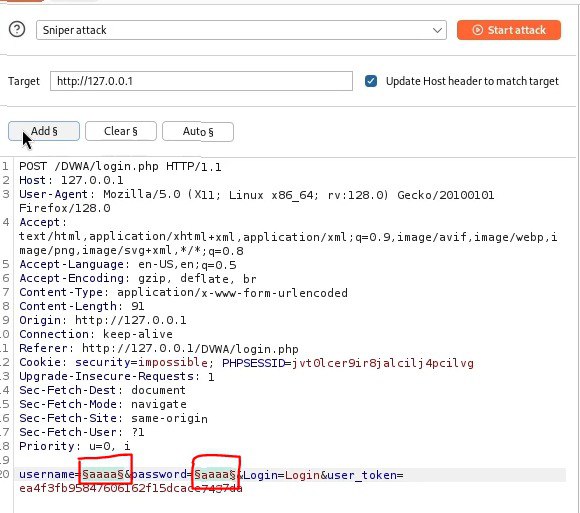


Рис. 10: Измененные данные

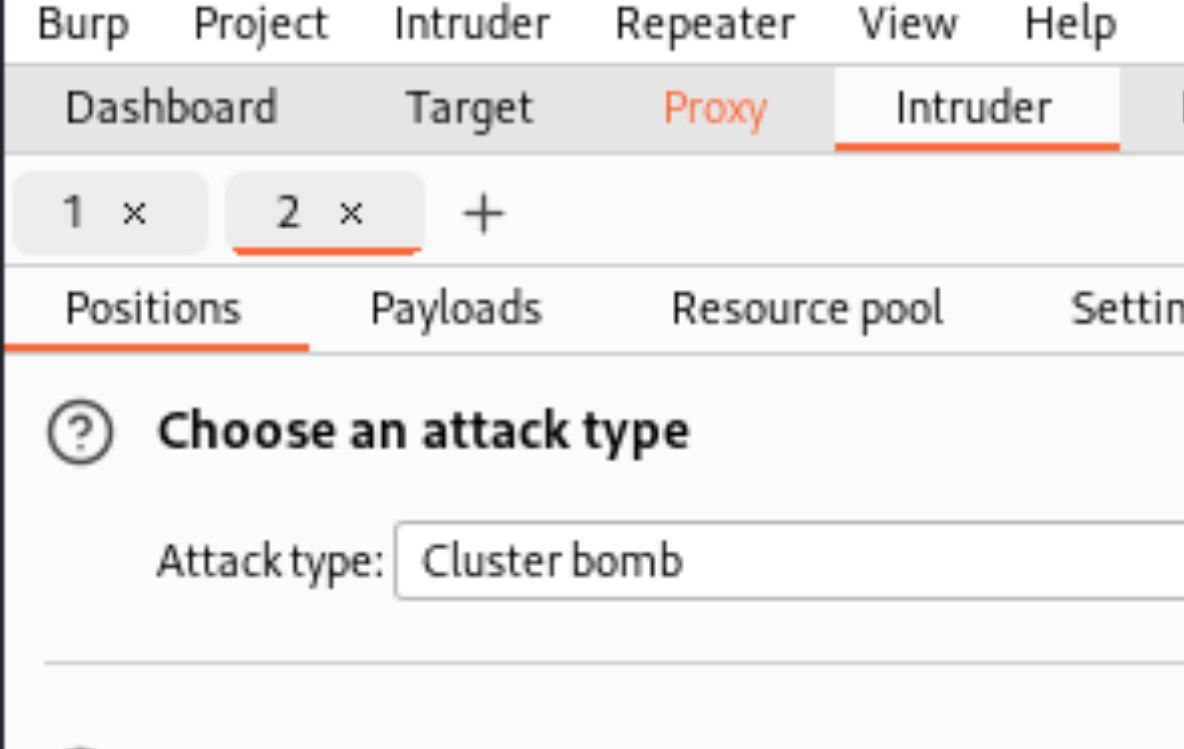


Рис. 11: Тип атака

Отметила два параметра для подбора, поэтому создала два списка со значениями для подбора в payload:

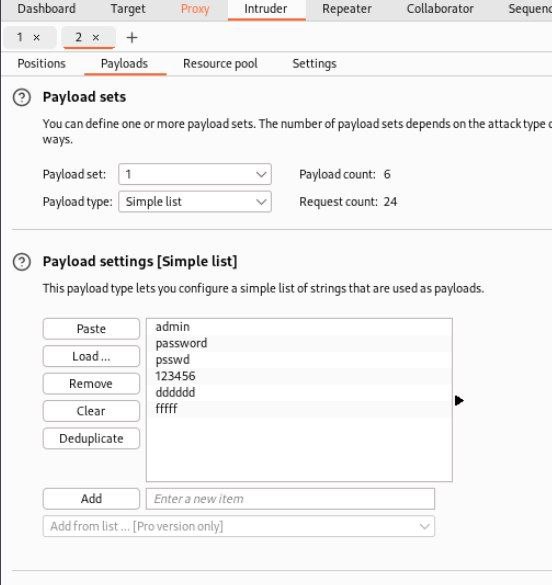


Рис. 12: Список 1

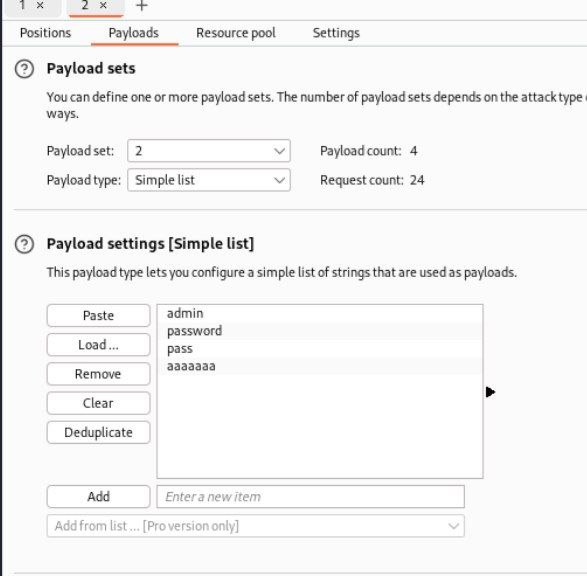


Рис. 13: Список 2

Далее запускаю атаку и начинаю подбор. При открытии каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В этом случае с подбором пары нас перенаправило на страницу index.php, значит пара должна быть верной:

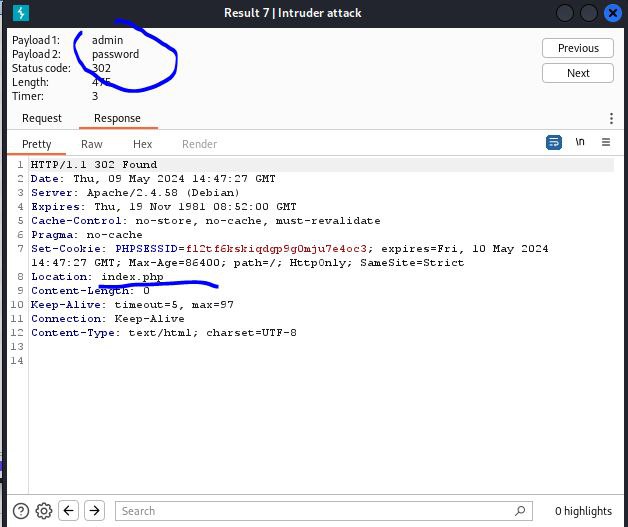


Рис. 14: Правильная пара

С использаванием repeater делаю доплнительную проверку. Нажимаю send и в response получаю результат перенаправление на index.php.

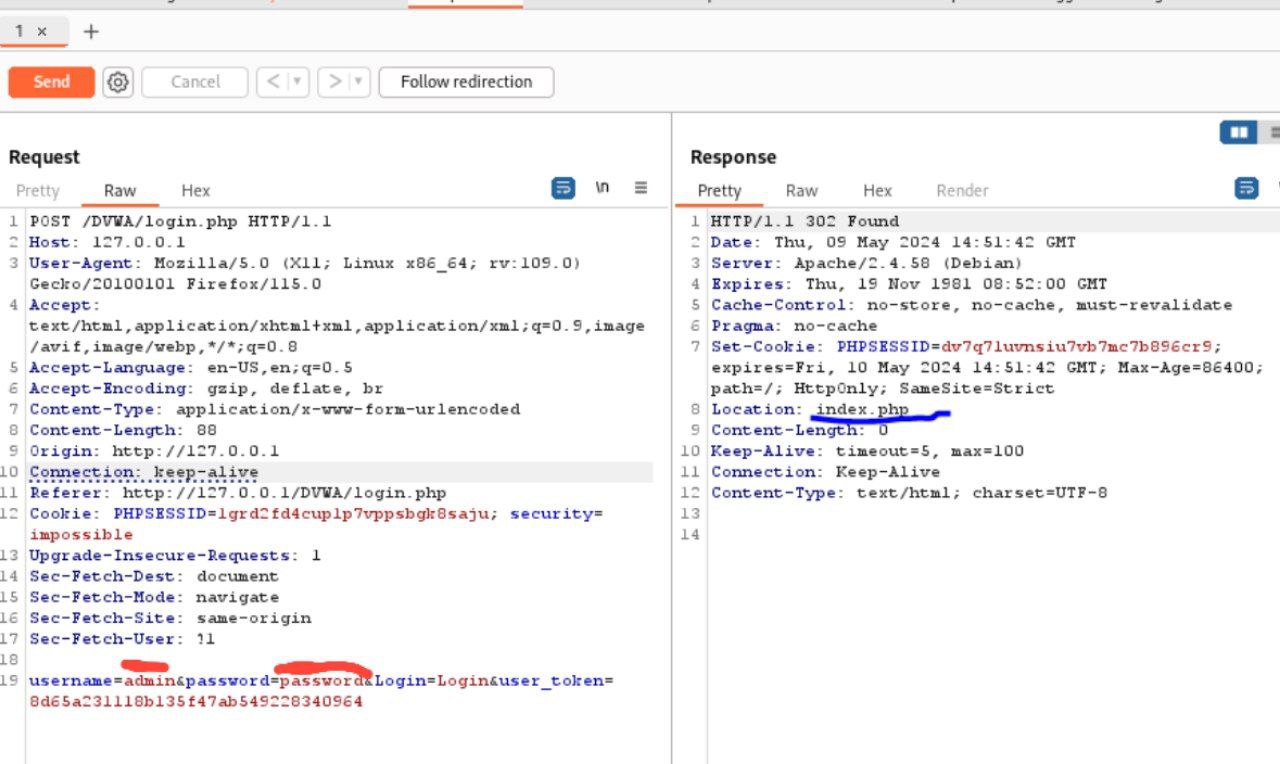


Рис. 15: Окна repeater и response

В подокне Render получаю то, как выглядит полученная страница:

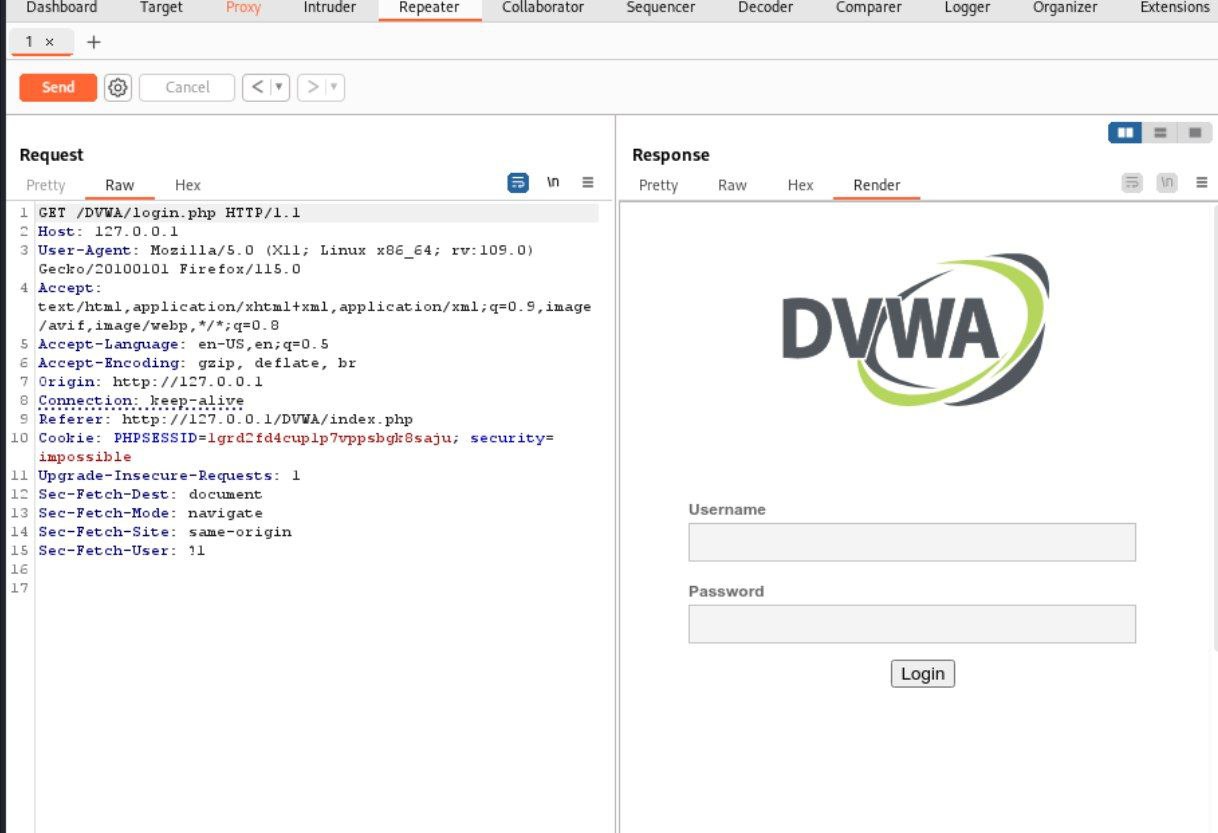


Рис. 16: Полученная страница

# 3 Выводы

Научилась использовать Burp Suite.

# Список литературы