Отчет по пятому этапу проекта

Основы информационной безопасности

Ищенко Ирина НПИьд-02-22

Содержание

# 1 Цель работы

Научиться использовать Burp Suite - набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения [1].

# 2 Выполнение лабораторной работы

Будем использовать для взлома учетных данных DVWA. Открываем Burp Suite через меню приложений, создаем проект и запускаем перехватчик (рис. 1).

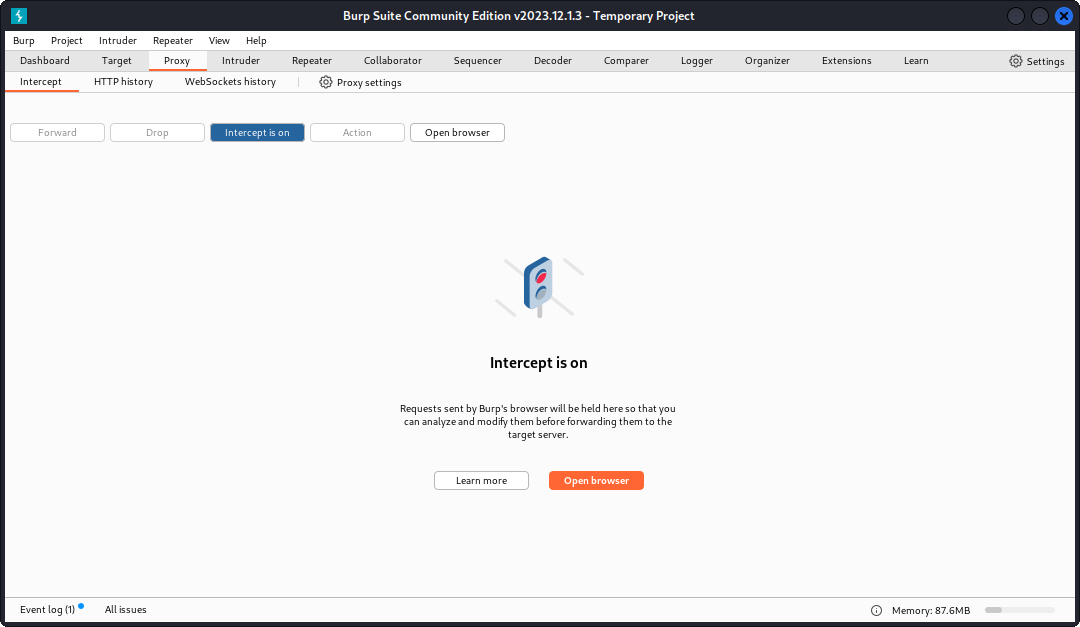


Рис. 1: Запуск перехватчика

Переходим в браузер по кнопке и открываем страницу аутетентификации в DVWA. В Burp Suite отображается актуальная информация (рис. 2).

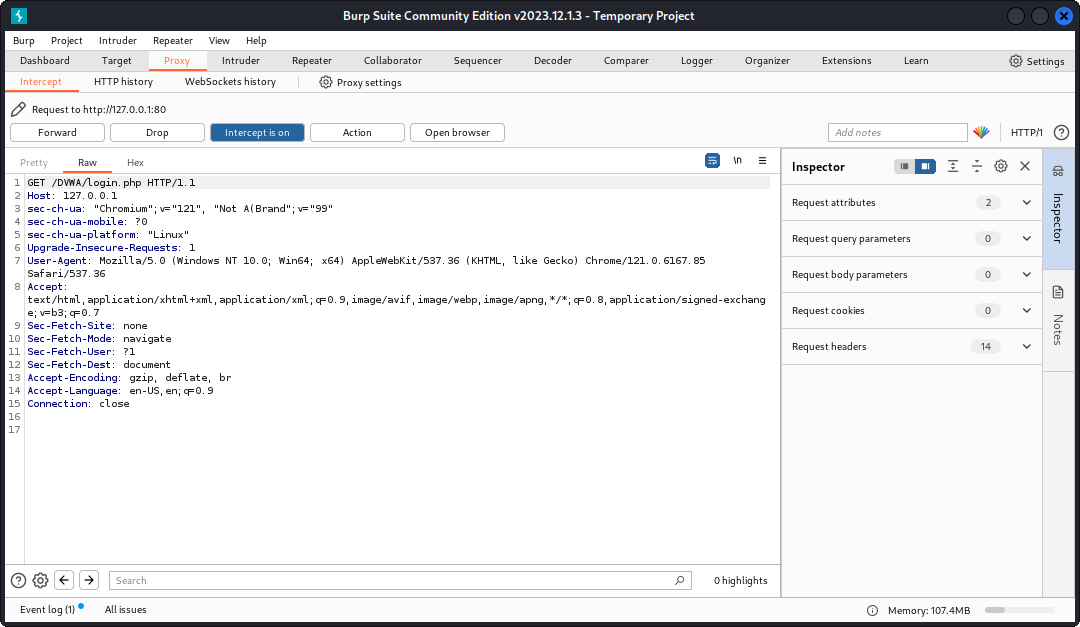


Рис. 2: Данные

С помощью кнопки forward на вкладке Target можно посмотреть карту сайта. Далее на сайте вводим случайные учетные данные. Burp Suite их перехватывает (рис. 3).

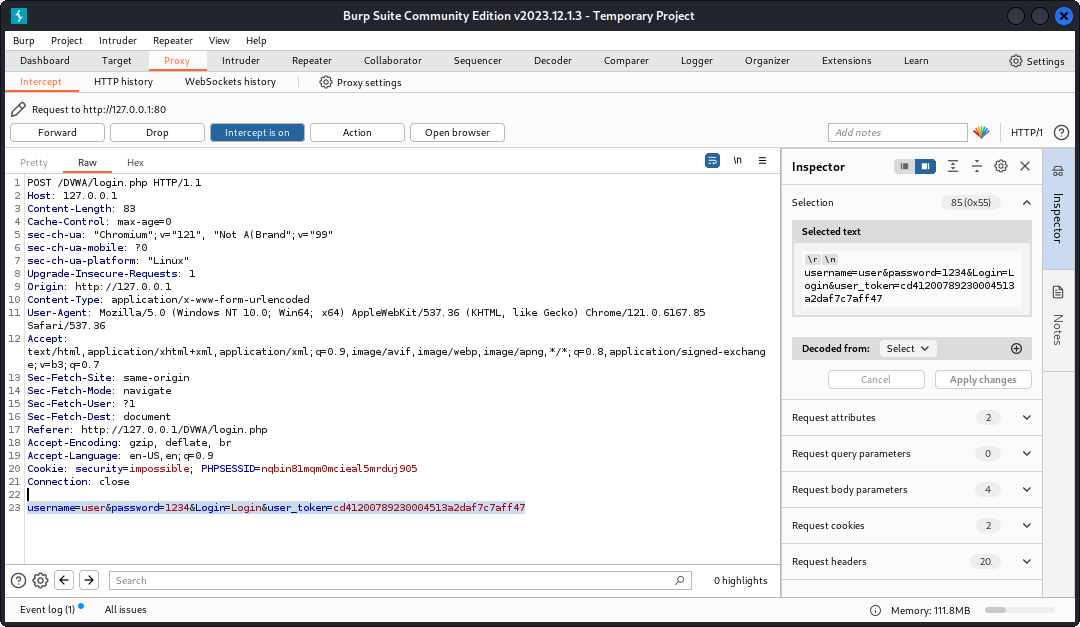


Рис. 3: Перехват данных

С вкладки HTTP-History отправляем строку с логином и паролем в Intruder. Добавляем поля логина и пароля, устанавливаем тип атаки Cluster Bomb (рис. 4).

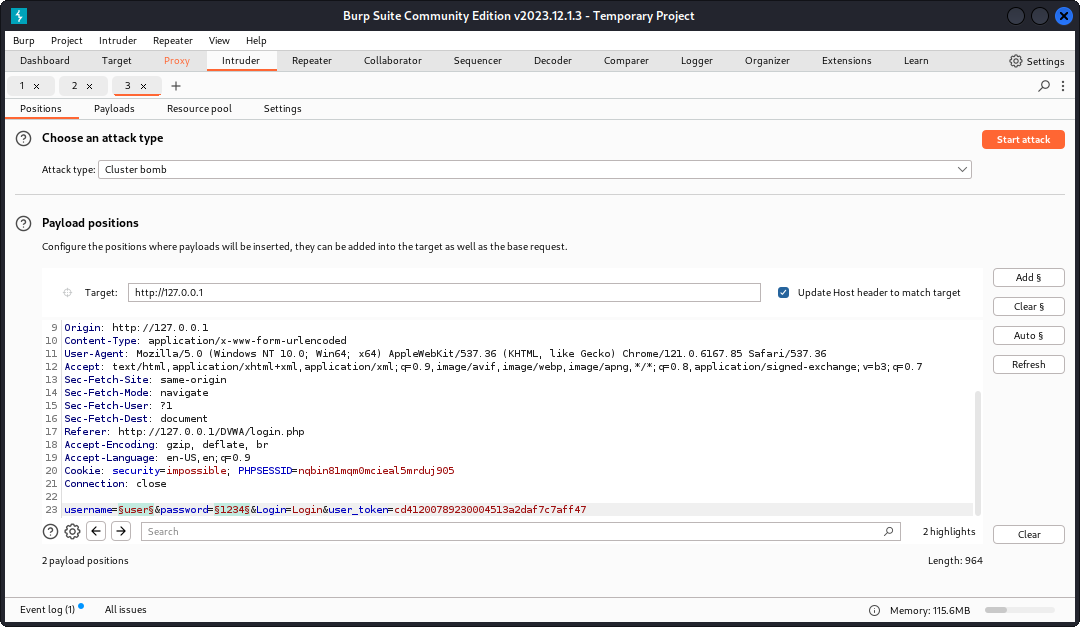


Рис. 4: Настройка атаки

Создаем списки возможных учетных данных (рис. 5) и (рис. 6).

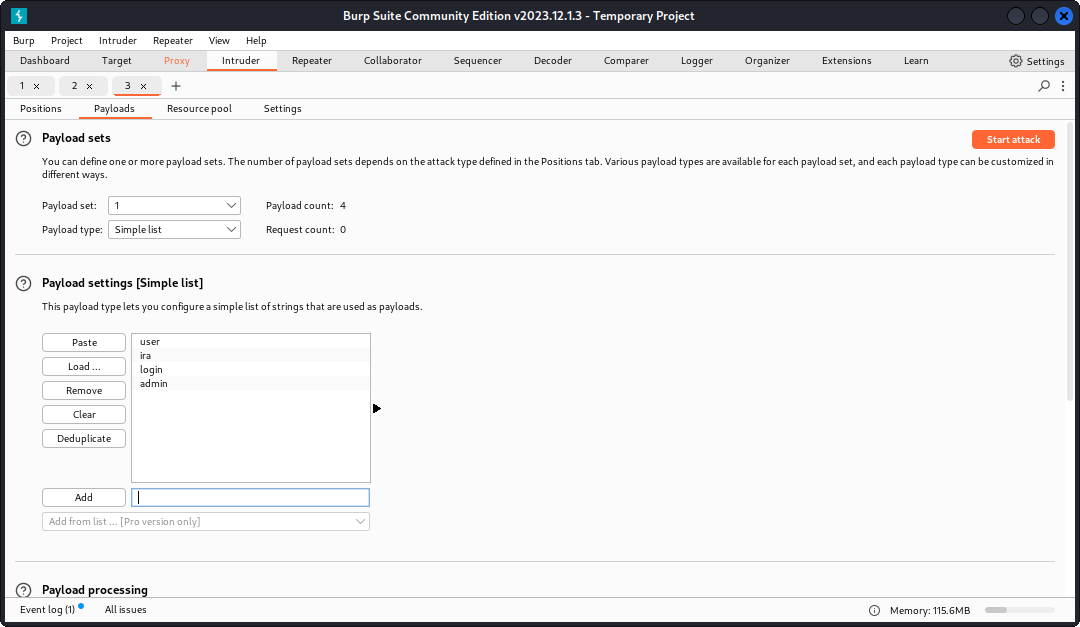


Рис. 5: Настройка Payloads

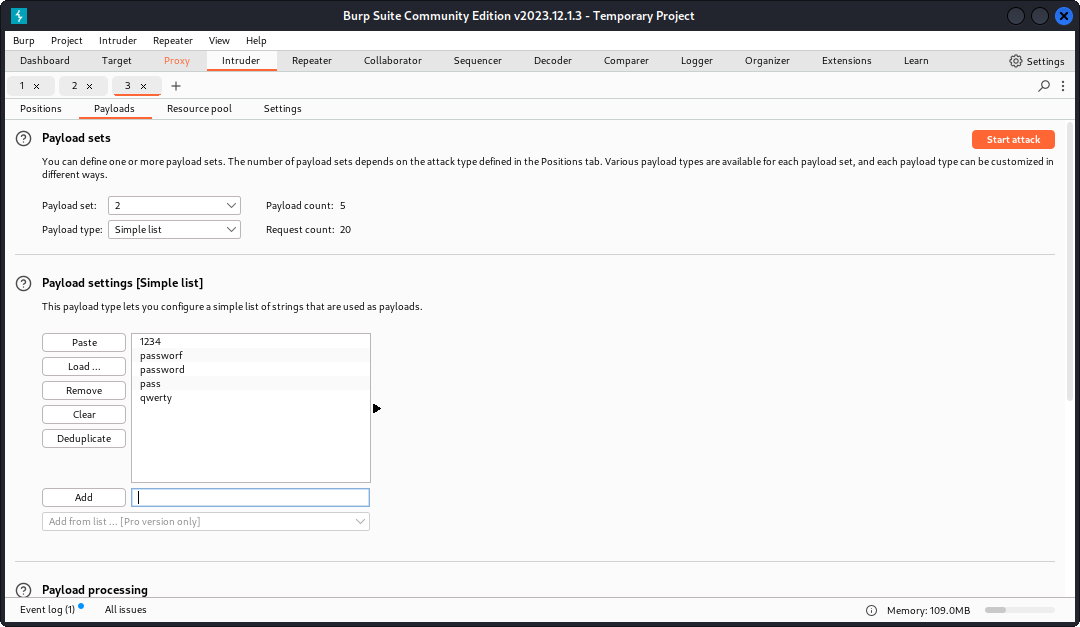


Рис. 6: Payloads

Запускаем атаку, по блоку Responce находим подходящие учетные данные (они перенаправляют на другую веб-страницу) (рис. 7).

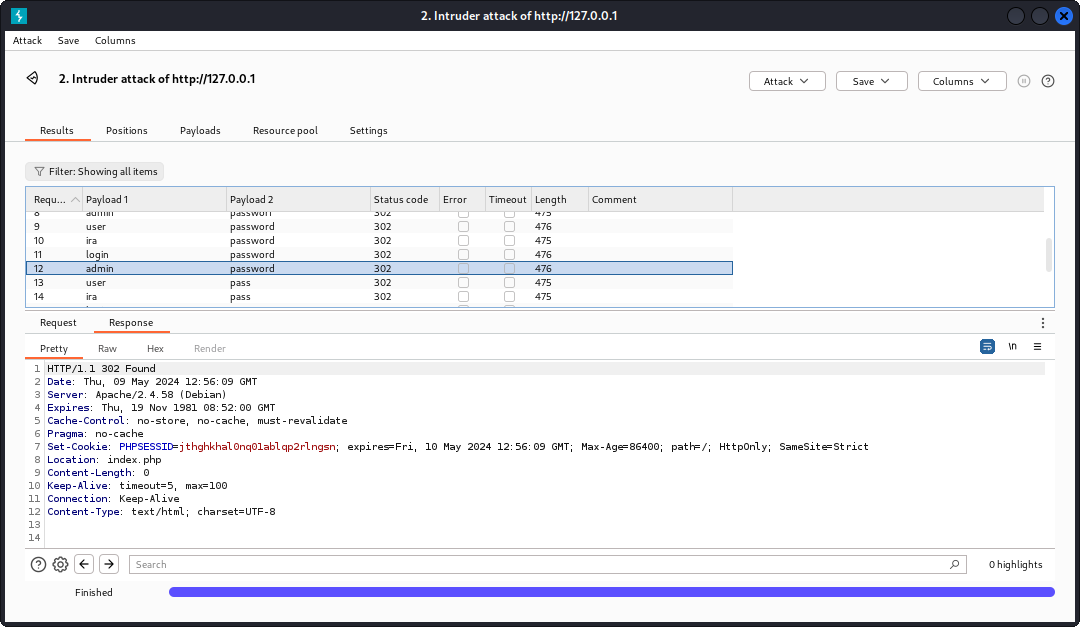


Рис. 7: Результат атаки

Чтобы вручную редактировать данные, строку можно отправить в Repeater (рис. 8).

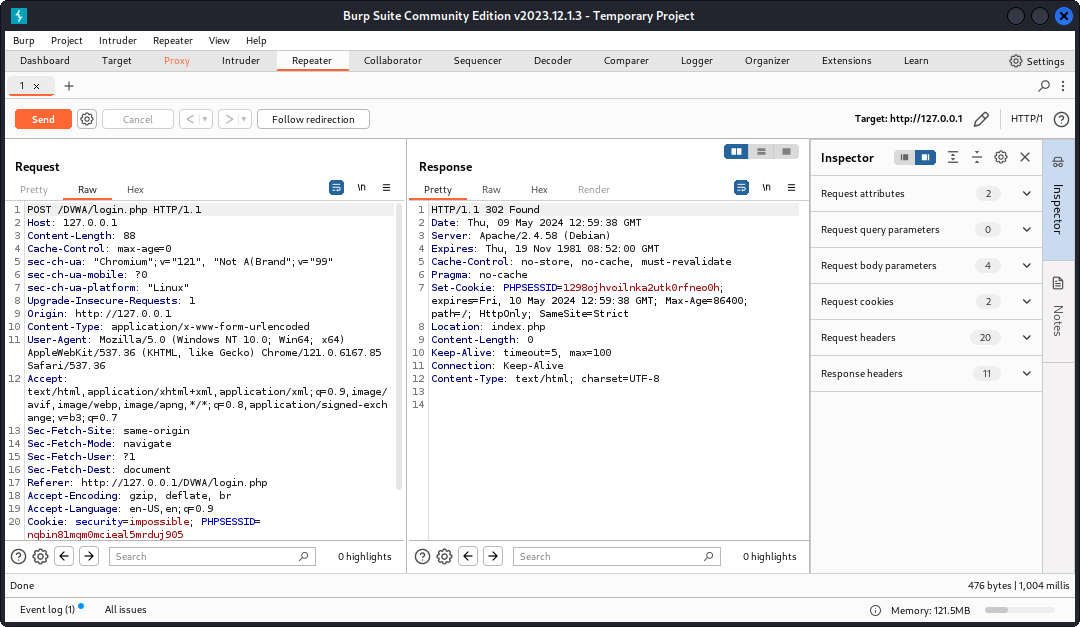


Рис. 8: Repeater

# 3 Выводы

В ходе этапа проекта я научилась использовать Burp Suite.

# Список литературы

1. Ш. Парасрам Т.Х. А. Замм. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.