Отчёт по этапу №5

Дисциплина: Основы информационной безопасности

Мишина Анастасия Алексеевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Научиться использовать Burp Suite для демонстрации реальных возможностей злоумышленников.

2 Выполнение лабораторной работы

Burp Suite представляет собой набор набор мощных инструментов безопасности веб-приложений. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов [1].

Запускаем Burp Suite. В нашем примере мы будем использовать его для взлома учетных данных, чтобы получить доступ к приложению DVWA. Для этого нам сначала потребуется настроить прокси-сервер и убедиться, что для IP установлено значение localhost IP, а номер порта - 8080. Открываем вкладку Proxy, ставим значение Intercept is on (рис. 2.1).

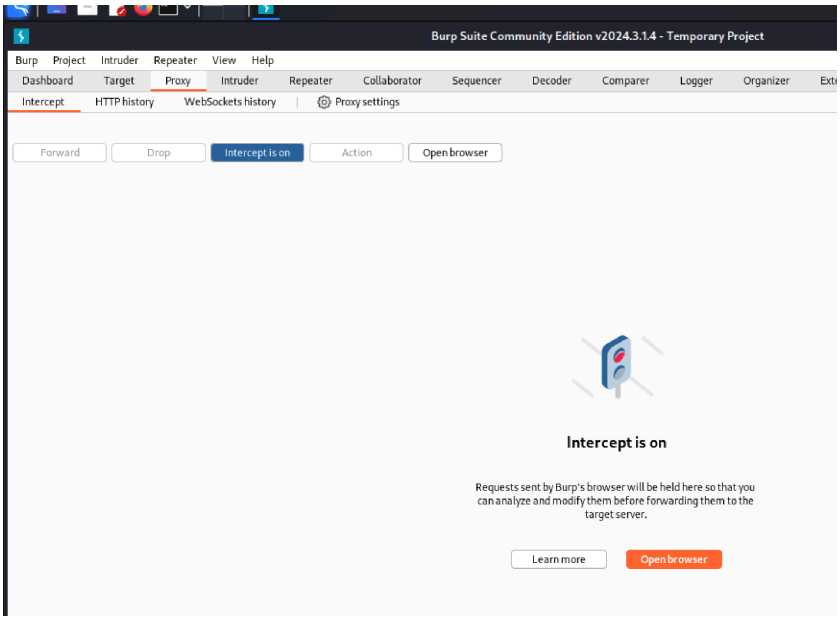

Рис. 2.1: Включение перехвата в прокси

Далее открываем браузер (firefox), заходим в настройки и ищем там network

settings. Настраиваем прокси сервер, после этого запускаем и открываем DVWA (рис. 2.2).

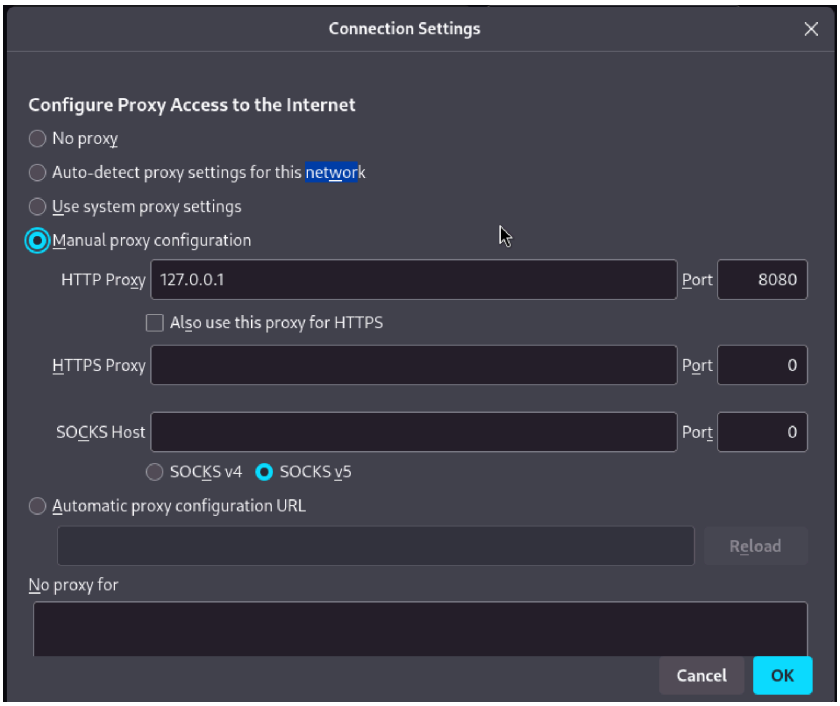

Рис. 2.2: Настройка прокси-сервера

Переходим в интерфейс Burp Suite, уже видим данные, которые программа смогла получить (рис. 2.3).

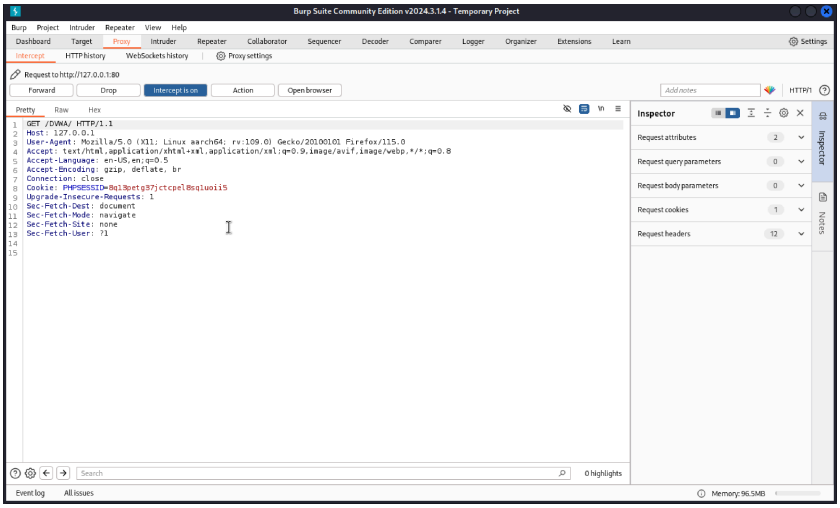

Рис. 2.3: Перехват данных веб-приложения

В браузере вводим любые логин и пароль для входа, в моем случае - login и password. Во вкладке Intercept видим перехваченный запрос, где на последней строке видны наши введенные логин и пароль (рис. 2.4).

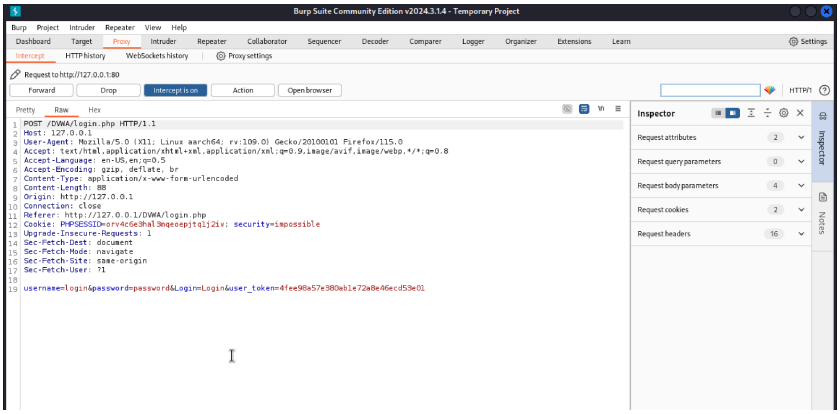

Рис. 2.4: Запрос для входа в веб-приложение

Во вкладке HTTP history так же можно увидеть попытку входа. Нажимаем на нее правой кнопкой мыши и выбираем send to Intruder (рис. 2.5).

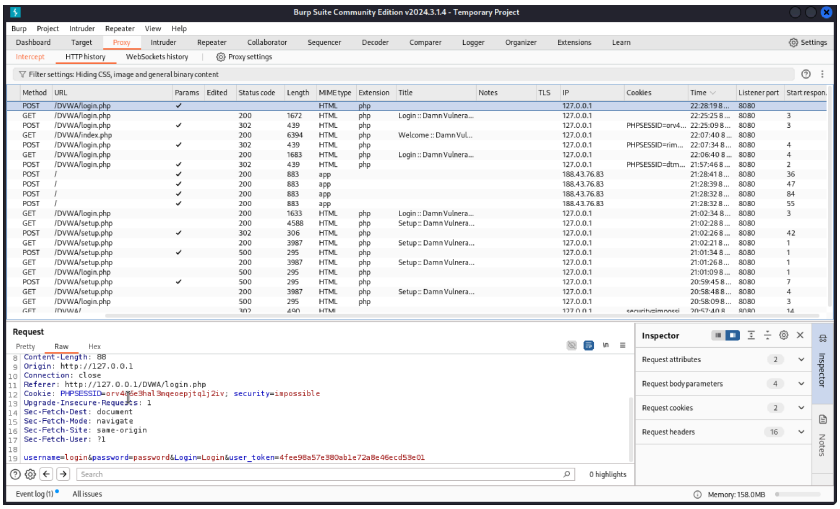

Рис. 2.5: HTTP history

В разделе Intruder выбираем вкладку Positions и выделяем поля со введенными логином и паролем на последней строке, нажимаем Add (рис. 2.6).

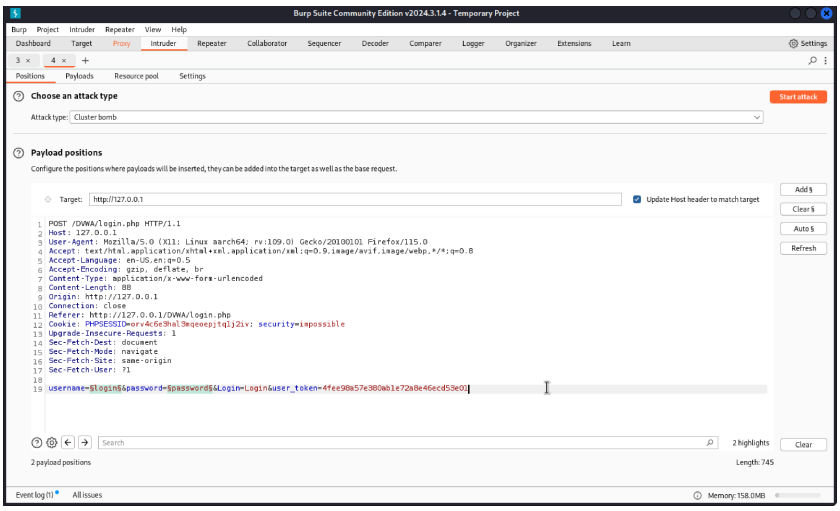

Рис. 2.6: Выбор позиций в Intruder

Указываем тип атаки Cluster bomb и переходим на вкладку Payloads. В Payload set выбираем 1 и заполняем Payload settings - вводим возможные логины для подбора (рис. 2.7).

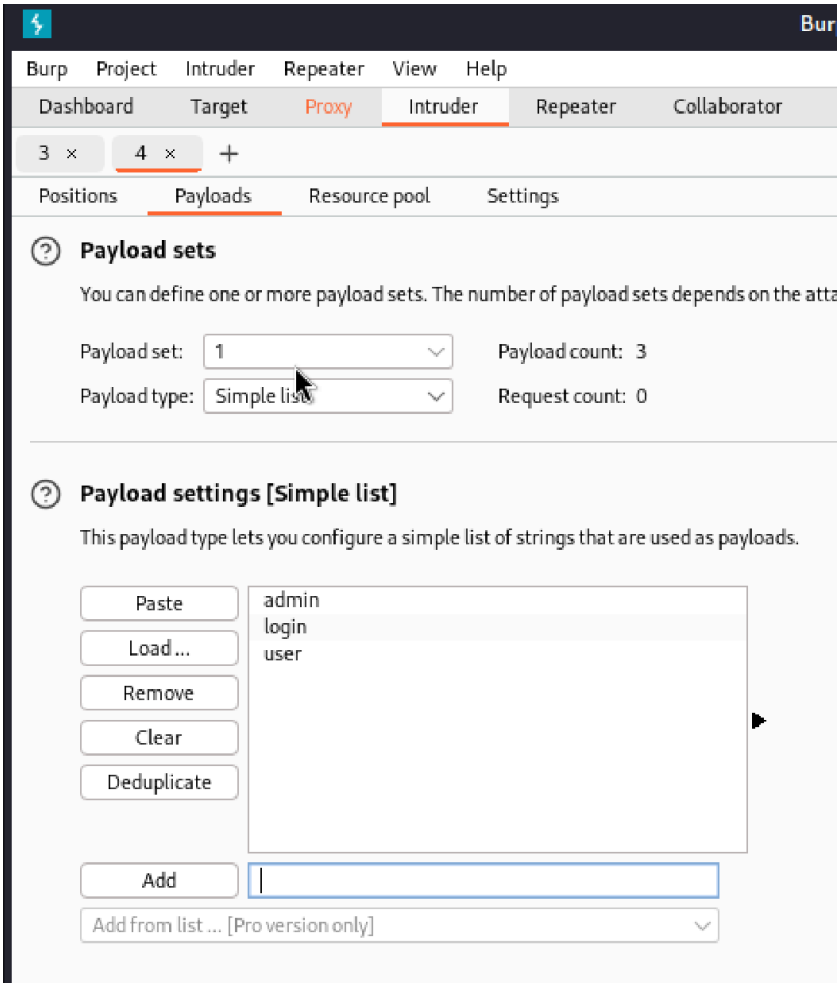

Рис. 2.7: Заполнение нагрузки username

В Payload set выбираем 2 и заполняем Payload settings - вводим возможные пароли (рис. 2.8).

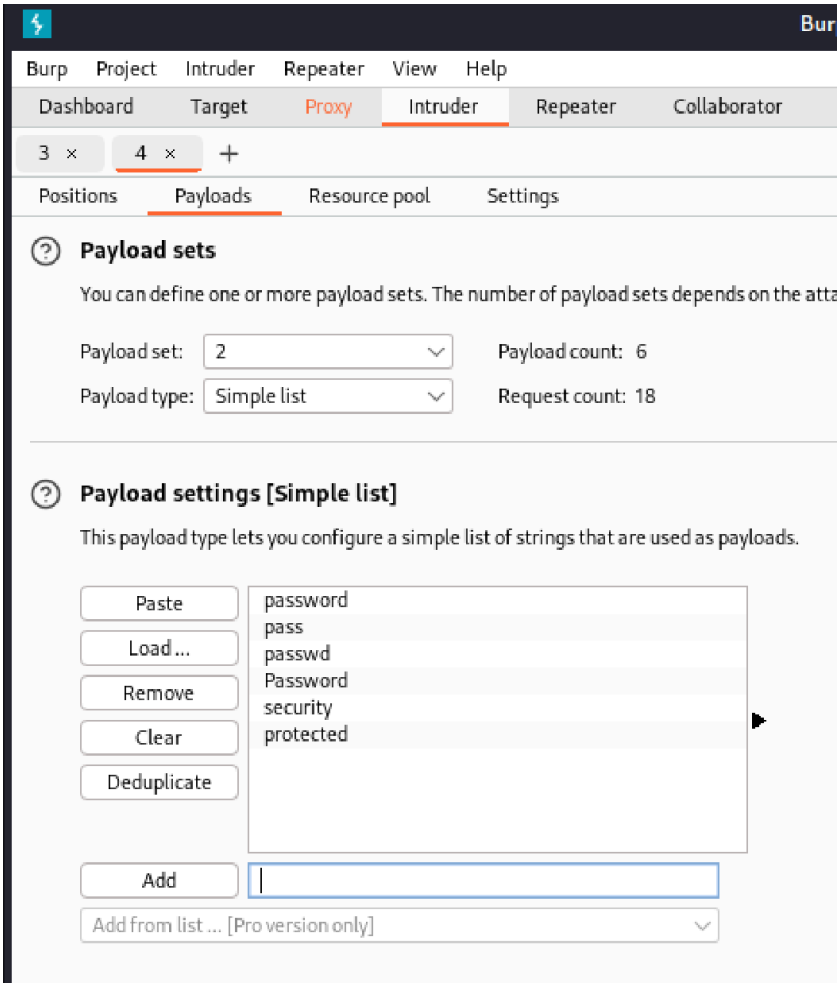

Рис. 2.8: Заполнение нагрузки password

Нажимаем Start attack и ждем результаты. Все попытки получили статус (код ответа HTTP) 302 - Перенаправление. Нажимаем правой кнопкой мыши на результат и во вкладке Response видим, куда перенаправляется запрос - в основом login.php. Находим комбинацию, когда запрос переправляется на index.php. Это и будет верная комбинация логина-пароля: admin password (рис. 2.9).

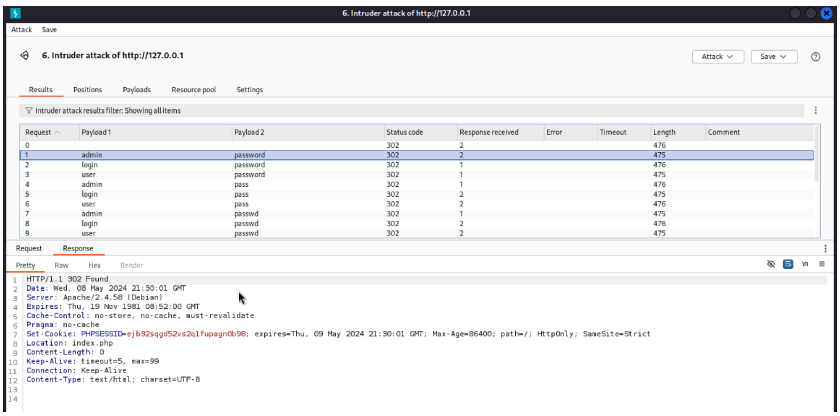

Рис. 2.9: Результаты атаки

Нажав на запрос и выбрав Send to Repeater, можно проверить эти результаты в Burp Suite (рис. 2.10). Ретранслятор предназначен для ручного изменения HTTP-запросов и данных, отправляемых в этих запросах. Во вкладке Repeater можно изменять данные в запросе, нажать Send и получить ответ [2] (рис. 2.11).

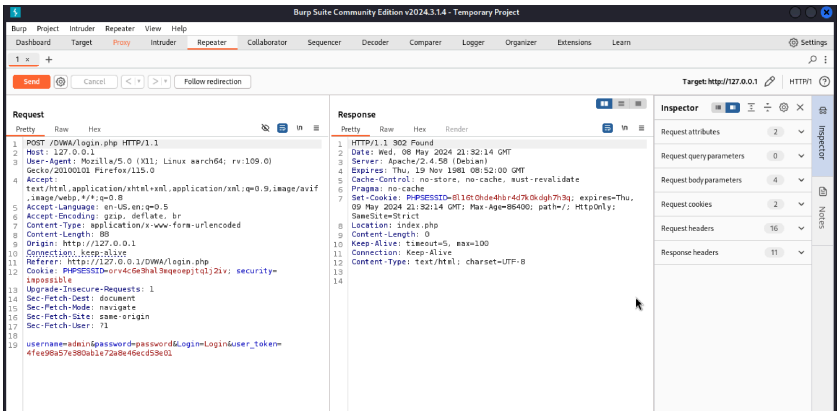

Рис. 2.10: Использование Repeater

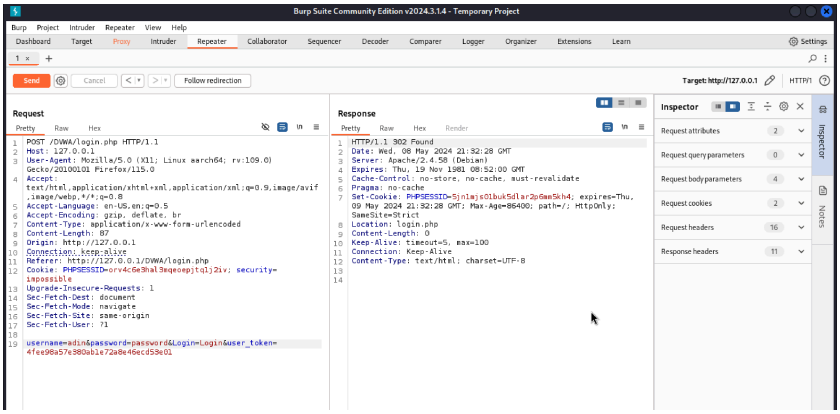

Рис. 2.11: Использование Repeater

3 Выводы

В ходе выполнения данной работы, я научилась использовать набор инструментов Burp Suite. Данный набор инструментов безопасности приложений является мощной платформой для атаки веб-приложений.

Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.
2. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.