Отчёт по индивидуальному проекту №5

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

# 1 Цель работы

Знакомство с программой Burp Suite и изучение ее функционала.

# 2 Выполнение лабораторной работы

1. Открываю Burp Suite и во вкладке Proxy включаю перехват http-запросов (рис. 1)

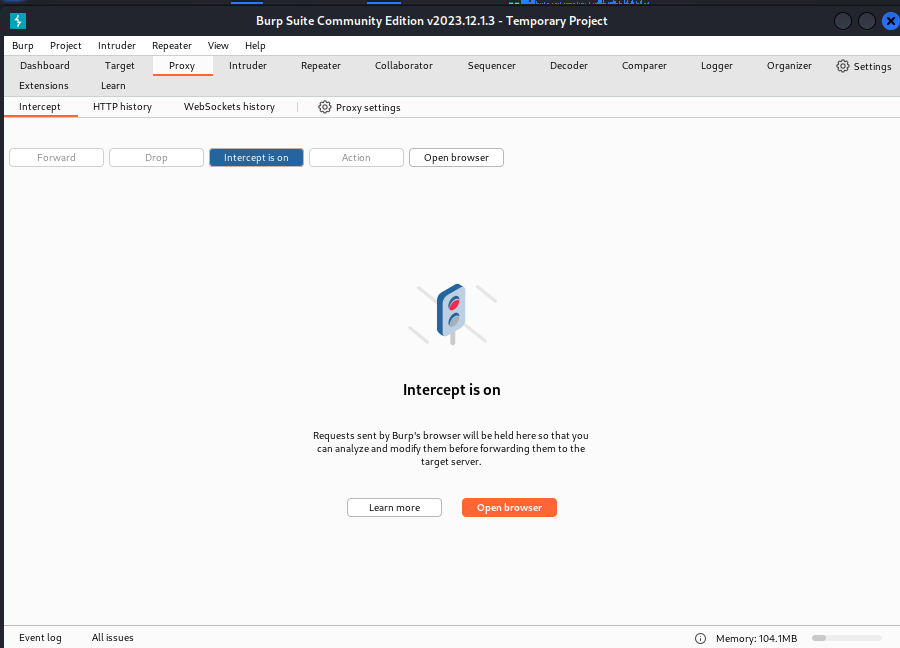


Рис. 1: Перехват http-запросов

1. В настройках браузера настраиваю прокси-сервер (рис. 2)

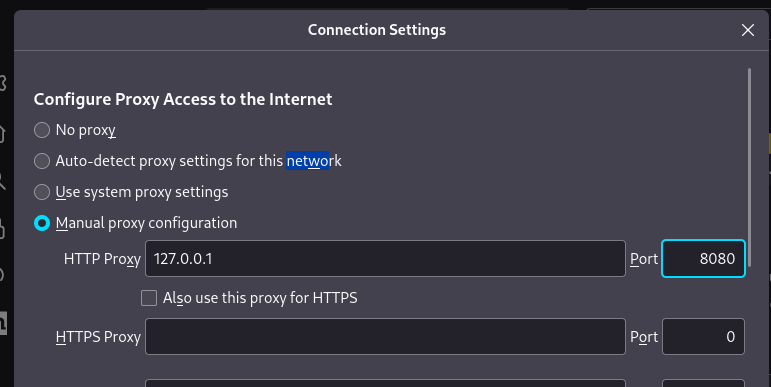


Рис. 2: Настройка прокси-сервера

1. Теперь, трафик браузера перехватывается в программе Burp Suite. Например, при открытии веб-страницы мы видим GET-запрос к ней (рис. 3)

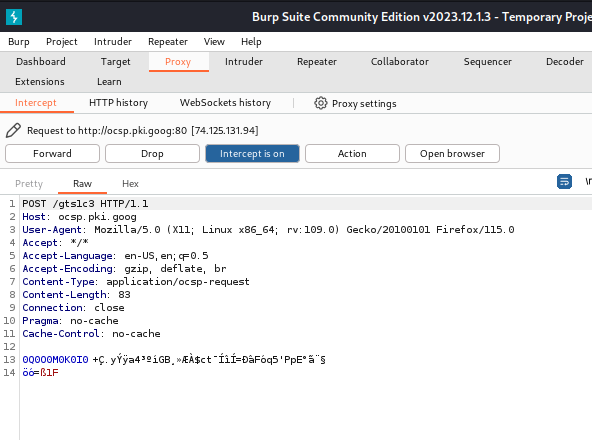


Рис. 3: Перехват трафика

1. Отправляю POST-запрос к DVWA на авторизацию с логином *usrname* и паролем *passw*. (рис. 4)

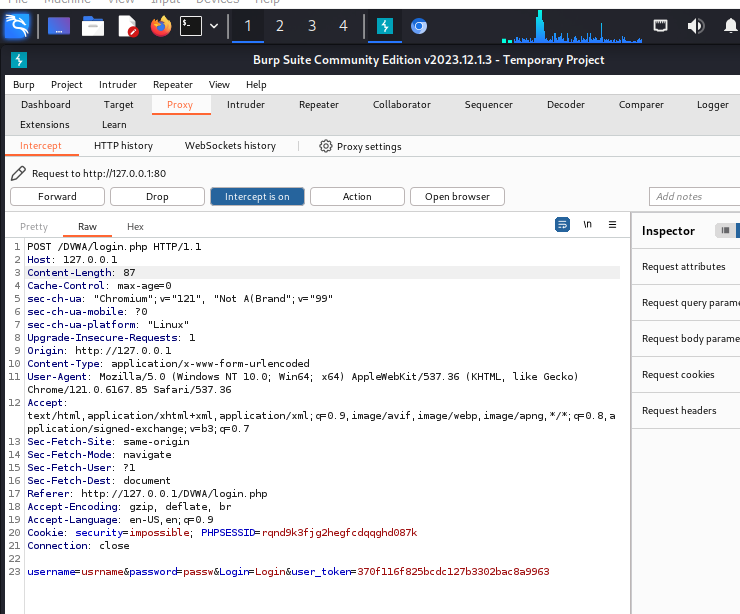


Рис. 4: Запрос на авторизацию

1. Перехожу во вкладку intruder, выбираю тип атаки Cluster bomb. Копирую POST-запрос к DVWA из прошлого пункта и параметры username и password оборачиваю в переменные (рис. 5)

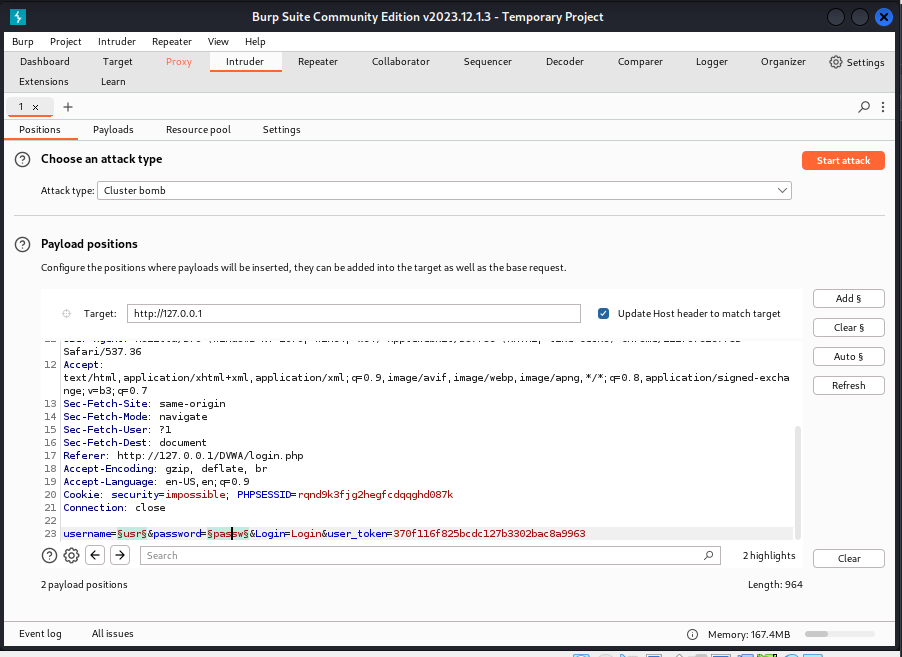


Рис. 5: Создание атаки Cluster bomb

1. Перехожу во вкладку Payloads, и для переменной 1 (username) добавляю несколько значений. Аналогично делаю для переменной 2 (login) (рис. 6)

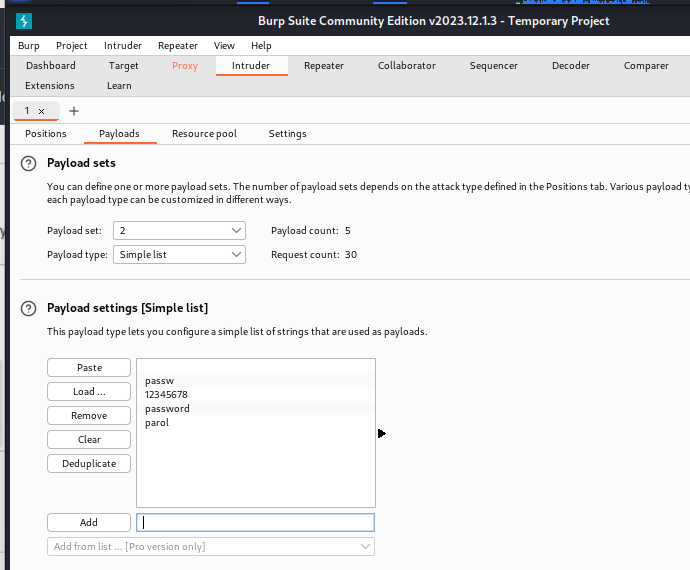


Рис. 6: Задание нескольких значений для переменных

1. Нажимаю на кнопку *Start attack*, после чего посылаются POST-запросы со всеми комбинациями переменных username и password. Например, для комбинации логина и пароля user:12345678 запрос перенаправляется на страницу /login.php - значит, данная комбинация неверная (рис. 7)

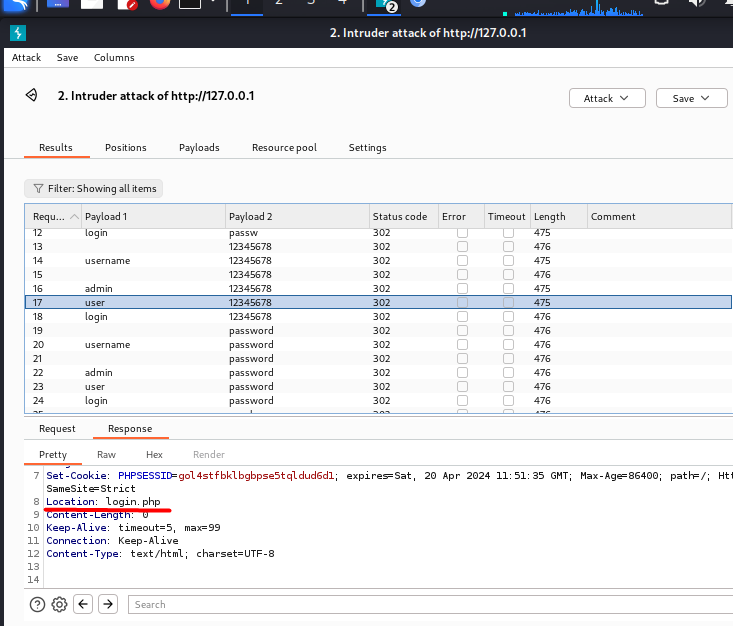


Рис. 7: Посылание запросов на авторизацию

1. Все комбинации, кроме admin:password, перенаправляются на /login.php. Комбинация admin:password перенаправляет на страницу /index.php - значит, комбинация admin:password верная (рис. 8)

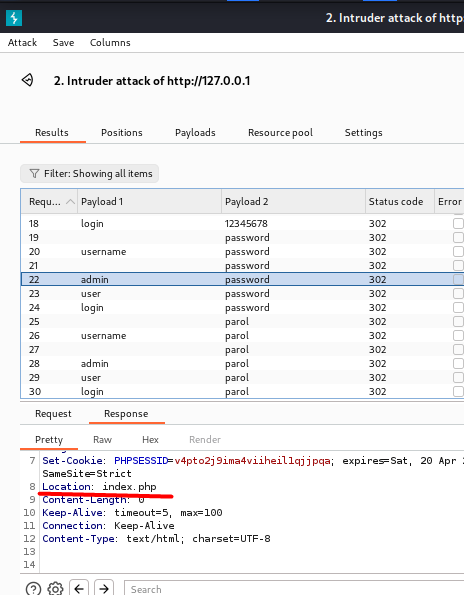


Рис. 8: Верные логин и пароль

# 3 Выводы

Я познакомился с Burp SUite и научился его применять на практике.