Отчёт по индивидуальному проекту №5

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

1 Цель работы **5**

2 Выполнение лабораторной работы **6**

3 Выводы **12**

Список иллюстраций

2.1 Перехват http-запросов 6
2.2 Настройка прокси-сервера 7
2.3 Перехват трафика 7
2.4 Запрос на авторизацию 8
2.5 Создание атаки Cluster bomb 8
2.6 Задание нескольких значений для переменных 9
2.7 Посылание запросов на авторизацию 10
2.8 Верные логин и пароль 11

Список таблиц

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. 2.1)

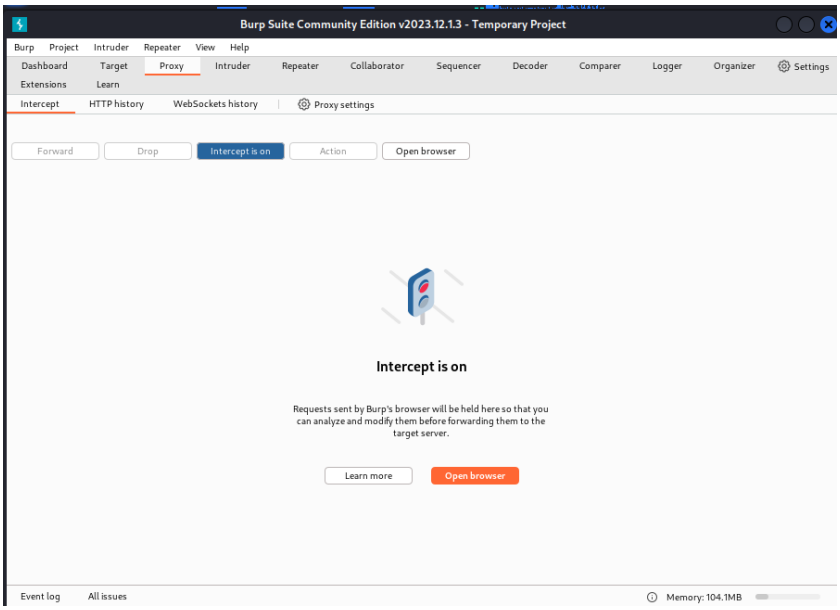

Рис. 2.1: Перехват http-запросов

2. В настройках браузера настраиваю прокси-сервер (рис. 2.2)

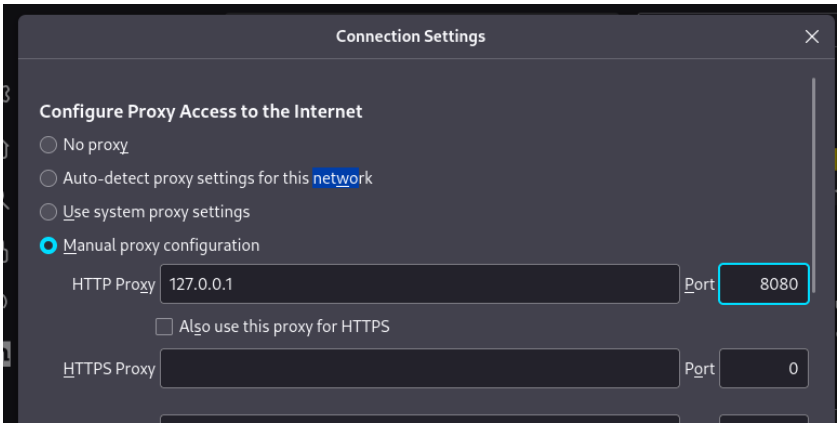

Рис. 2.2: Настройка прокси-сервера

3. Теперь, трафик браузера перехватывается в программе Burp Suite. Например, при открытии веб-страницы мы видим GET-запрос к ней (рис. 2.3)

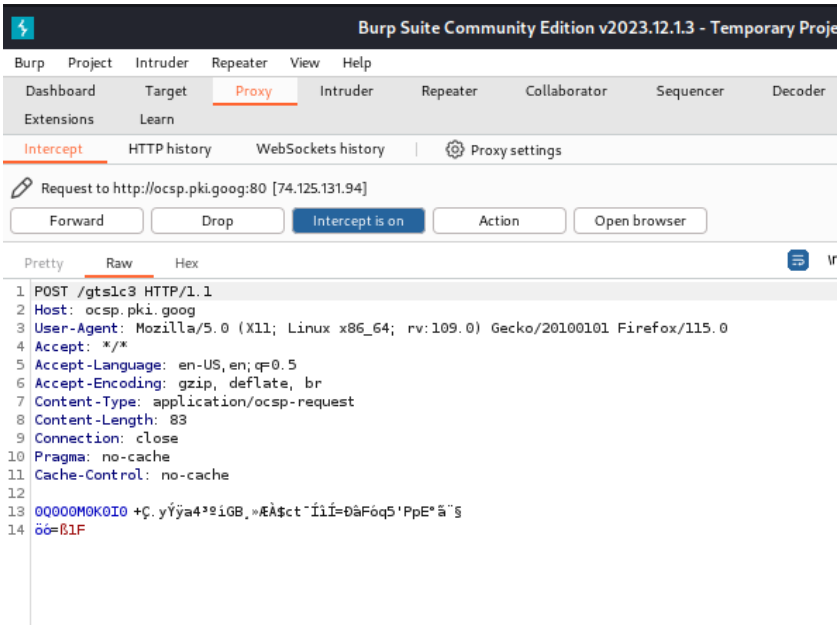

Рис. 2.3: Перехват трафика

4. Отправляю POST-запрос к DVWA на авторизацию с логином *usrname* и паролем *passw*. (рис. 2.4)

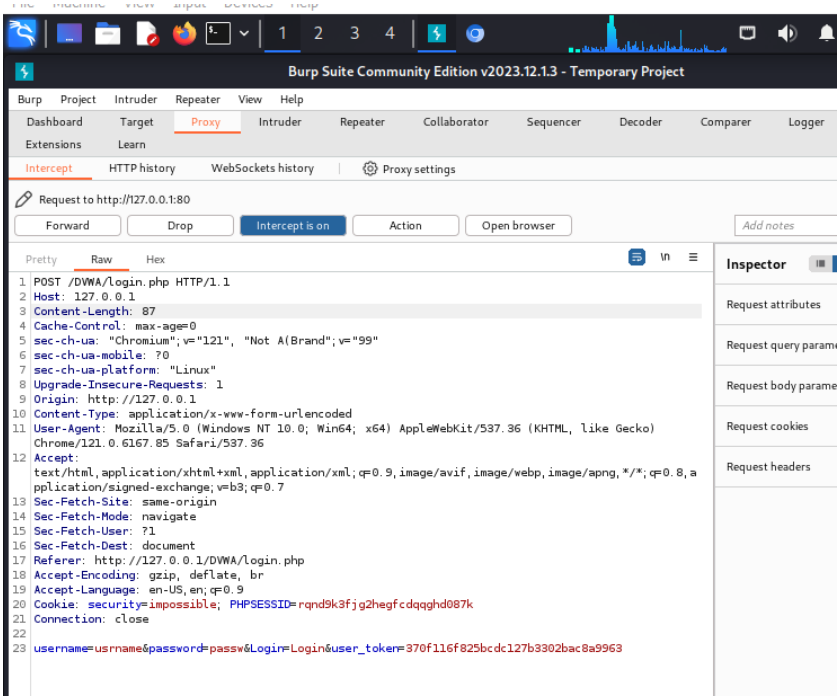

Рис. 2.4: Запрос на авторизацию

5. 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. 2.5)

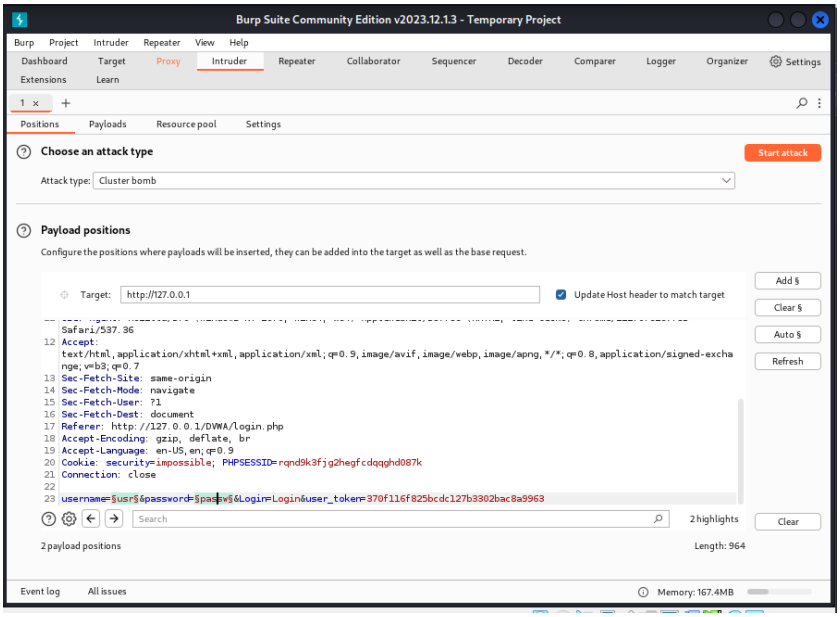

Рис. 2.5: Создание атаки Cluster bomb

6. Перехожу во вкладку Payloads, и для переменной 1 (username) добавляю несколько значений. Аналогично делаю для переменной 2 (login) (рис. 2.6)

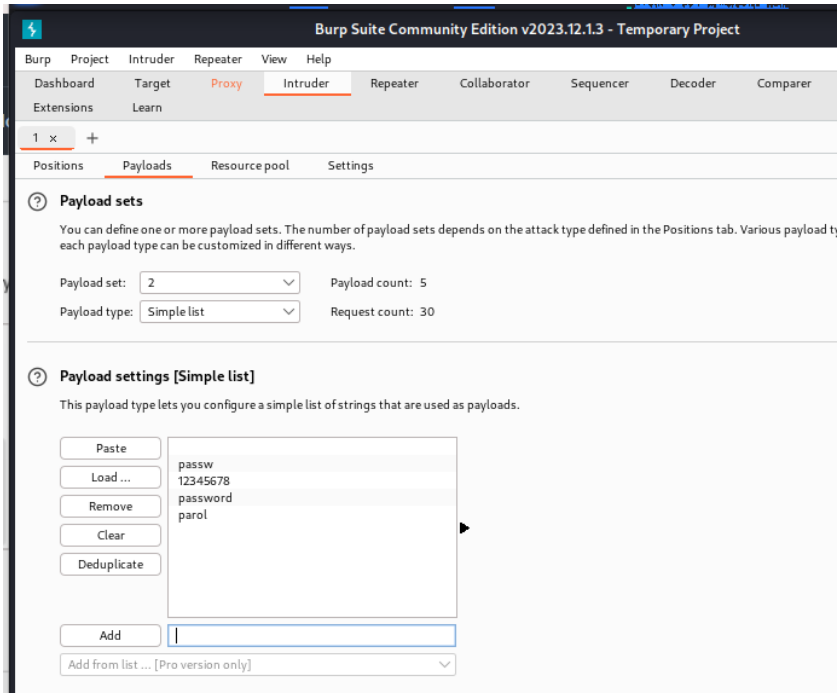

Рис. 2.6: Задание нескольких значений для переменных

7. 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. 2.7)

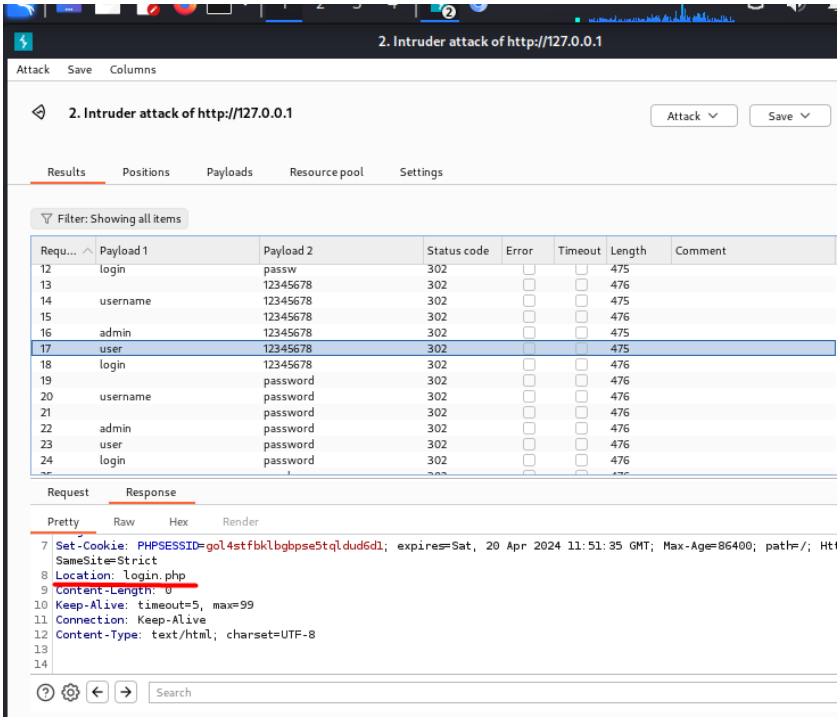

Рис. 2.7: Посылание запросов на авторизацию

8. Все комбинации, кроме admin:password, перенаправляются на /login.php. Комбинация admin:password перенаправляет на страницу /index.php - значит, комбинация admin:password верная (рис. 2.8)

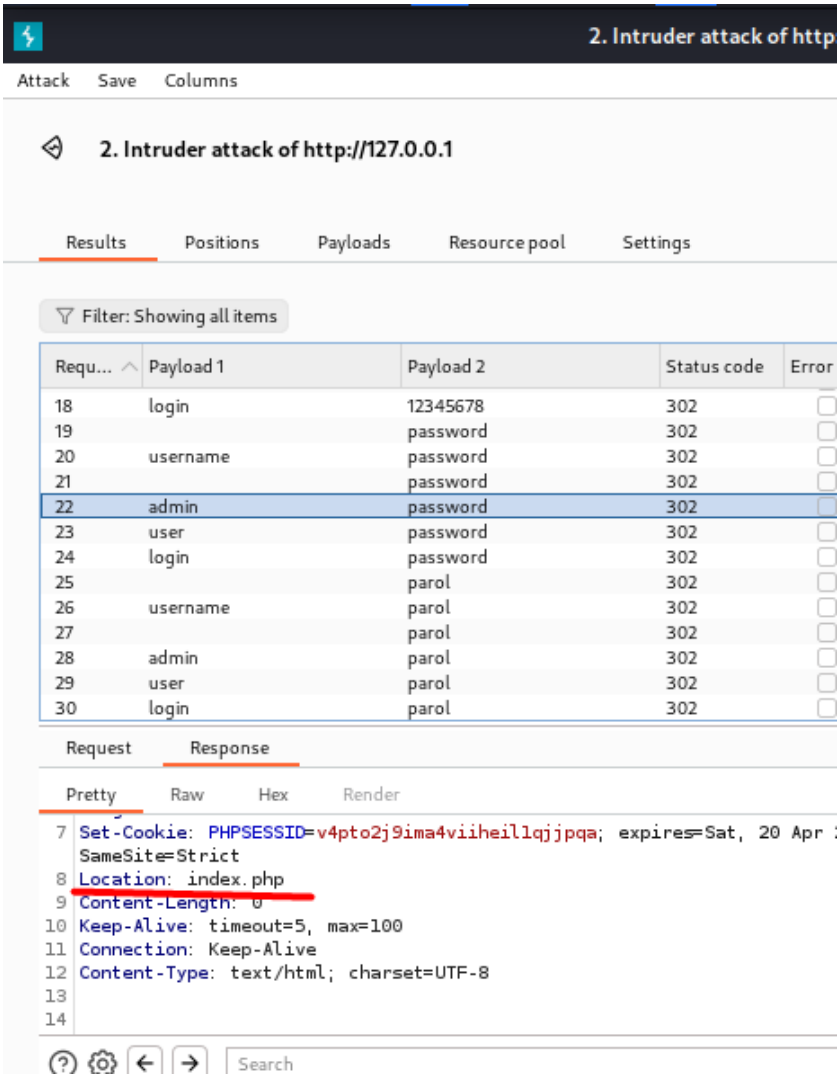

Рис. 2.8: Верные логин и пароль

3 Выводы

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