

# **5 этап индивидуального проекта**

**Основы информационной безопасности**

Серёгина Ирина Андреевна

# Содержание

|   |                                |    |
|---|--------------------------------|----|
| 1 | Цель работы                    | 3  |
| 2 | Задание                        | 4  |
| 3 | Теоретическое введение         | 5  |
| 4 | Выполнение лабораторной работы | 6  |
| 5 | Выводы                         | 9  |
|   | Список литературы              | 10 |

# 1 Цель работы

Ознакомление с Burp Suite.

## 2 Задание

Здесь приводится описание задания в соответствии с рекомендациями методического пособия и выданным вариантом.

## 3 Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения.

## 4 Выполнение лабораторной работы

1. С помощью `systemctl start apache2` и `systemctl start mysql` я запускаю локальный сервер, на котором после открою веб-приложение DVWA. Запускаю Burp Suite (рис. 4.1).

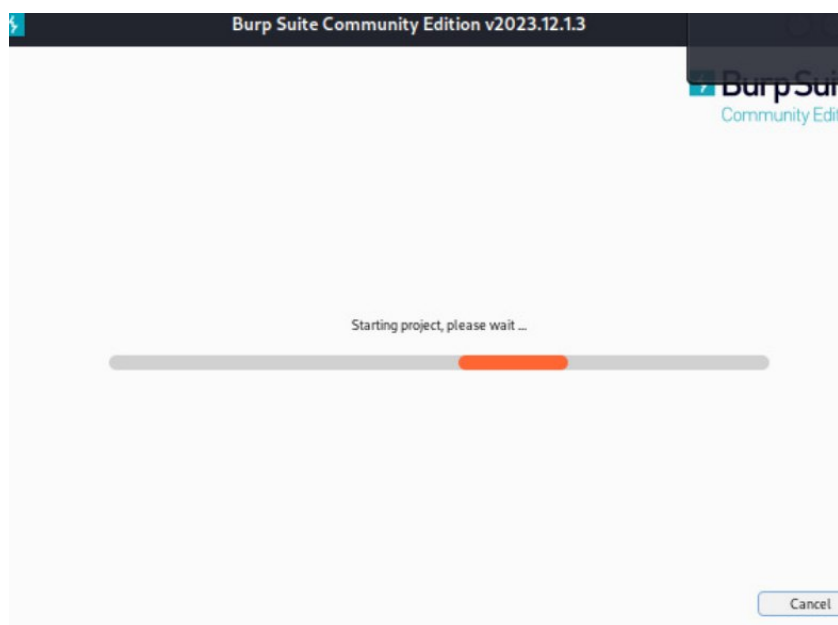


Рис. 4.1: запуск Burp Suite

2. Захожу в сетевые настройки браузера и меняю некоторые из них (рис. 4.2).

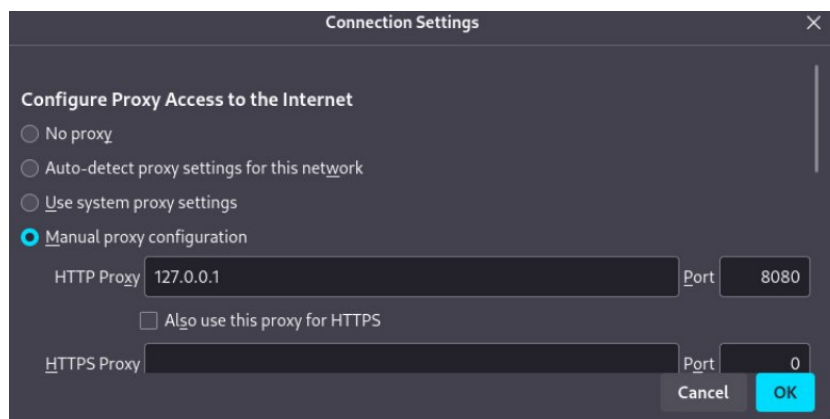


Рис. 4.2: изменение сетевых настроек браузера

3. Также меняю проху настройки самого инструмента. Во вкладке проху устанавливаю “intercept is on” (рис. 4.3).

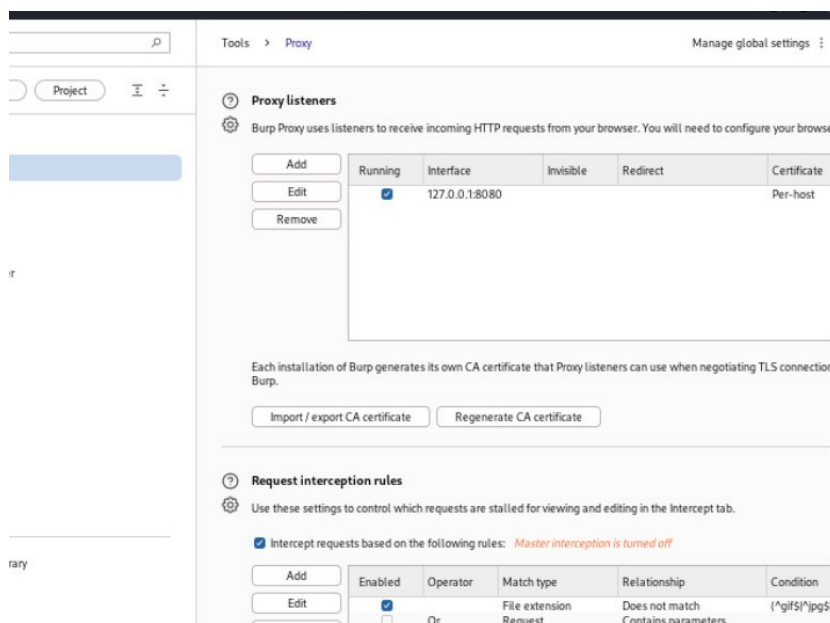


Рис. 4.3: настройки проху

4. В браузере устанавливаю данный параметр (рис. 4.4).

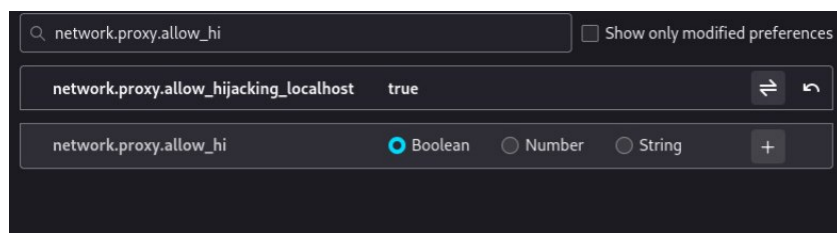


Рис. 4.4: настройка браузера

- После этого при попытке зайти на DVWA в браузере, во вкладке проху появляется запрос (рис. 4.5).

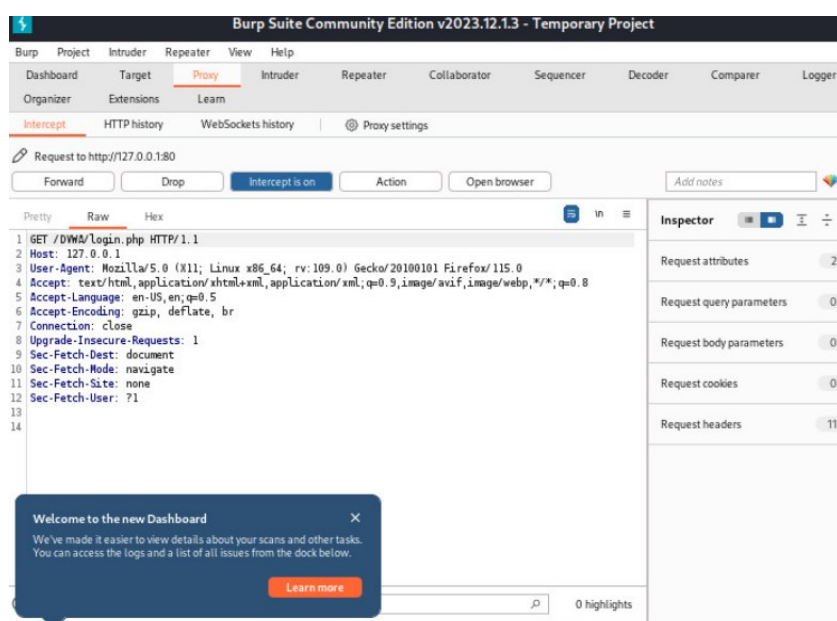


Рис. 4.5: запрос от сервера

- Во вкладке target находится история запросов, во вкладке intruder можно посмотреть тип атаки, котрый можно изменить, и запрос.



## 5 Выводы

Я ознакомилась с Burp Suite.

## **Список литературы**