Основы информационной безопасности

Индивидуальный проект. Этап № 5. Использование Burp Suite

Подлесный Иван Сергеевич

Содержание

Список иллюстраций

Постановка задачи

Целью данной работы является использование Burp Suit для перехвата, изменения и изучения HTTP запросов и ответов.

Выполнение лабораторной работы

Intercept HTTP traffic with Burp Proxy

Burp Suite был установлен за кадром заранее, так что необходимо просто настроить ПО и создать проект

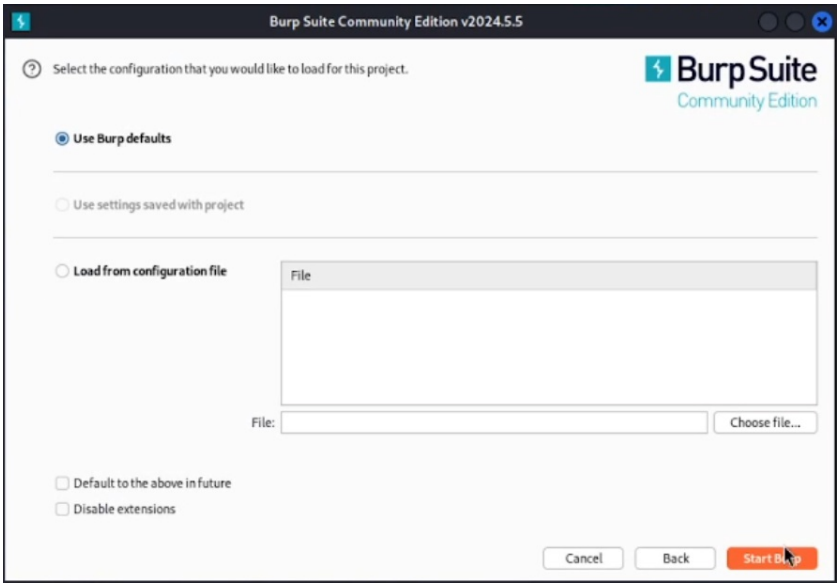

Рис. 1: Настройка ПО

Теперь попробуем перехватить http запрос с помощью Burp Proxy. Включим перехват, а в браузере включим прокси и укажем для него адрес локального хоста, а также установим параметр, разрешающий перехват запросов локального хоста(рис. fig. 2 - fig. 4).

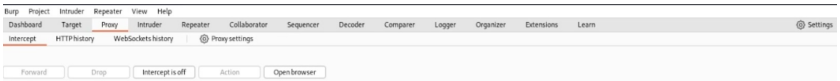

Рис. 2: Включение Burp Proxy

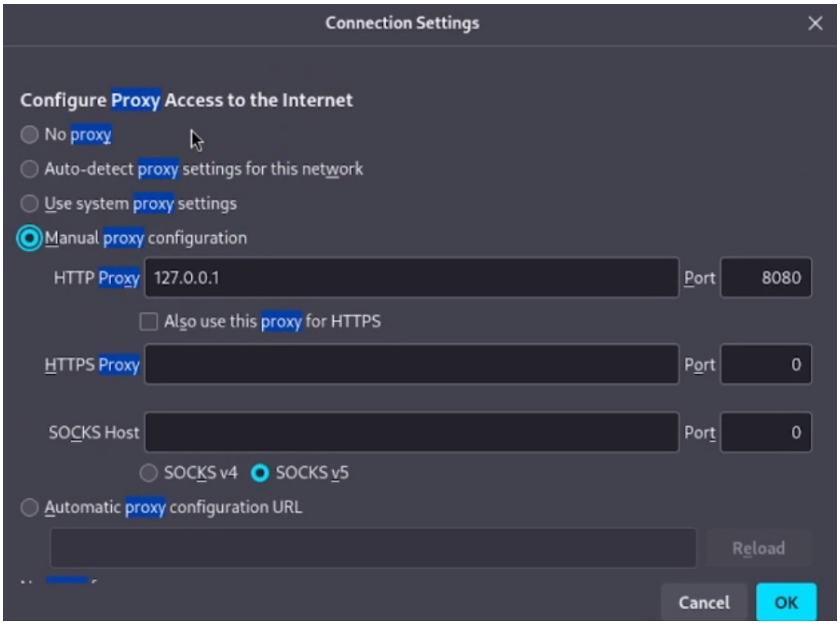

Рис. 3: Настройка HTTP Proxy браузера

Рис. 4: Установка флага allow_hijacking_localhost

Можем увидеть первый перехваченный запрос: вход на сайт DVWA. Указаны адрес локального хоста, версия браузера, ОС устройства и другая информация(рис. fig. 5):

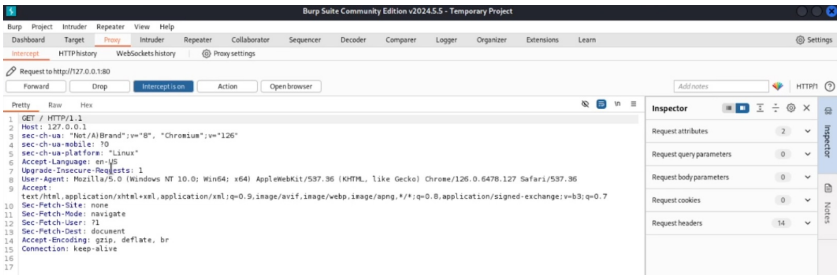

Рис. 5: Перехват запроса на вход на сайт

Рассмотрим перехват запроса аутентификации(рис. fig. 6):

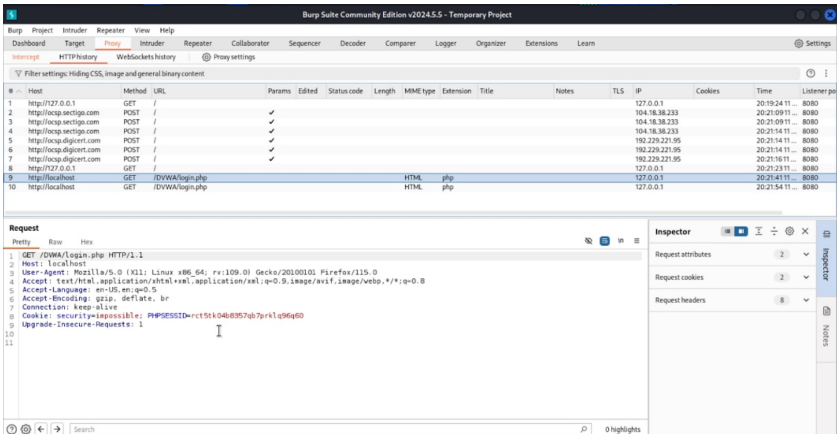

Рис. 6: Запрос на аутентификацию

Здесь дополнительно указываются куки запроса, а также выдается сам запрос с указанием введенного имени пользователя и пароля.

Кроме того уже совершенный запрос можно отпправить на повтор для того чтобы изучить ответы(рис. fig. 7):

В запросах можно изменять вводимую нформацию и сравнивать ответы(рис. fig. 7):

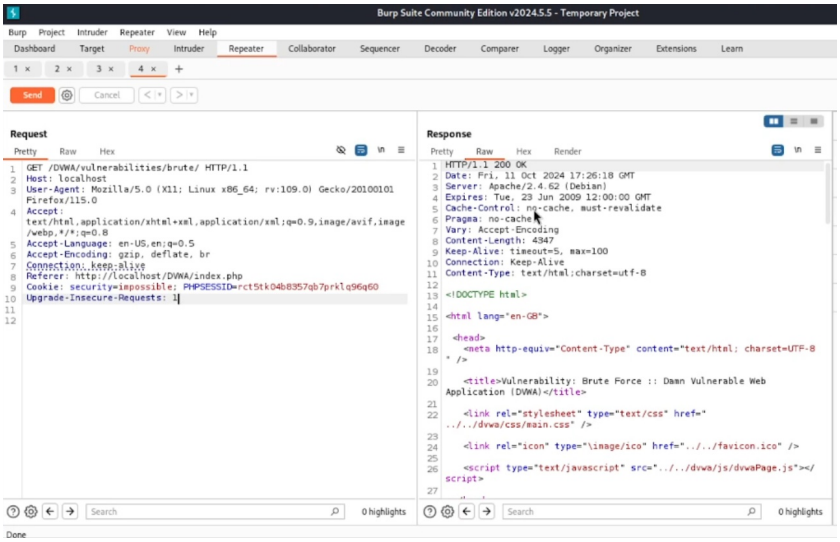

Рис. 7: Изучение ответа на запрос с функцией повторения запроса

Выводы

В результате выполнения работы научились на практике использовать ПО Burp Suite для перехвата, изменения и изучения HTTP запросов и ответов.