Отчёт по индивидуальному проекту

Этап 4

Надежда Александровна Рогожина

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Познакомиться с утилитой Burp Suite.

2 Теоретическое введение

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

3 Выполнение лабораторной работы

В первую очередь, я запустила `burp suite` через команду `# burpsuite` в терминале. На вкладке `Proxy - Intercept` необходимо было включить перехват (рис. [3.1]).

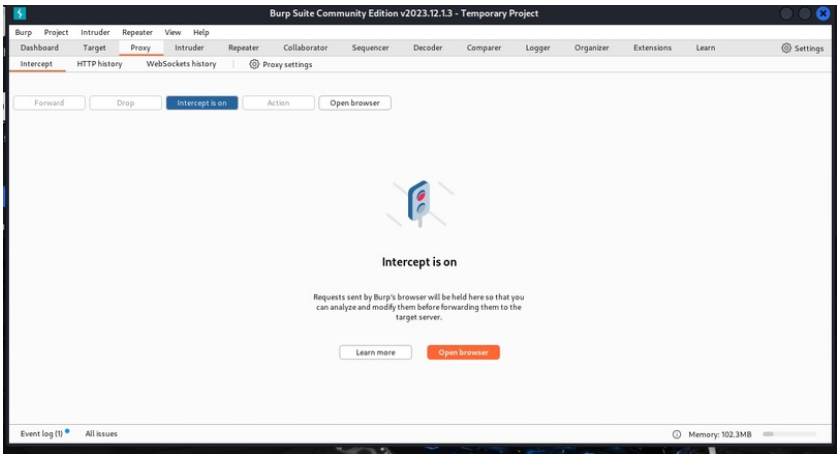

Рис. 3.1: Intercept is on

Также необходимо было настроить `proxy` (рис. [3.2]).

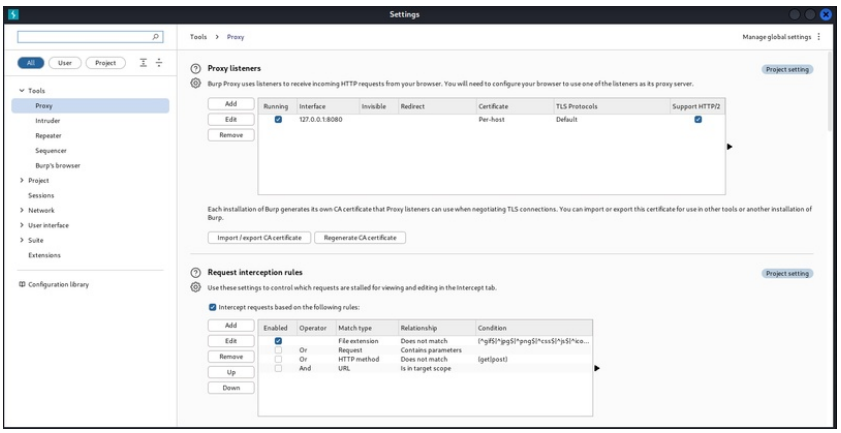

Рис. 3.2: 127.0.0.1:8080

После этого настроить сеть в браузере (рис. [3.3]).

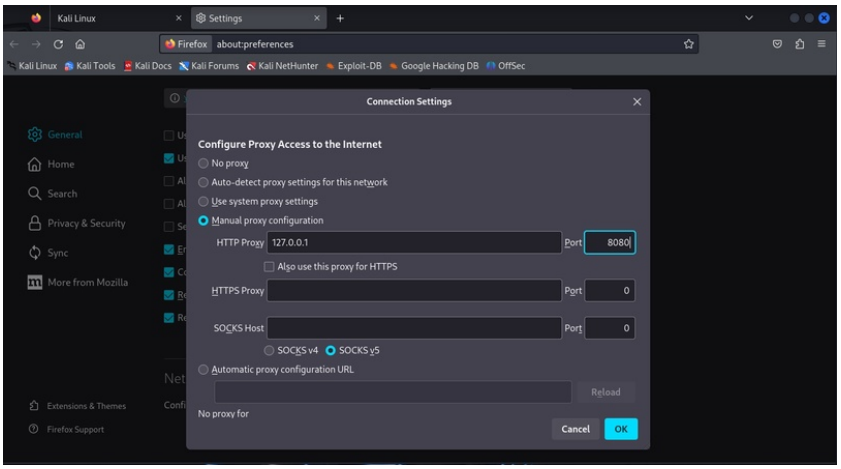

Рис. 3.3: Connection Settings

Попытаемся подключиться к порту `192.168.0.32/dvwa` (рис. [3.4]).

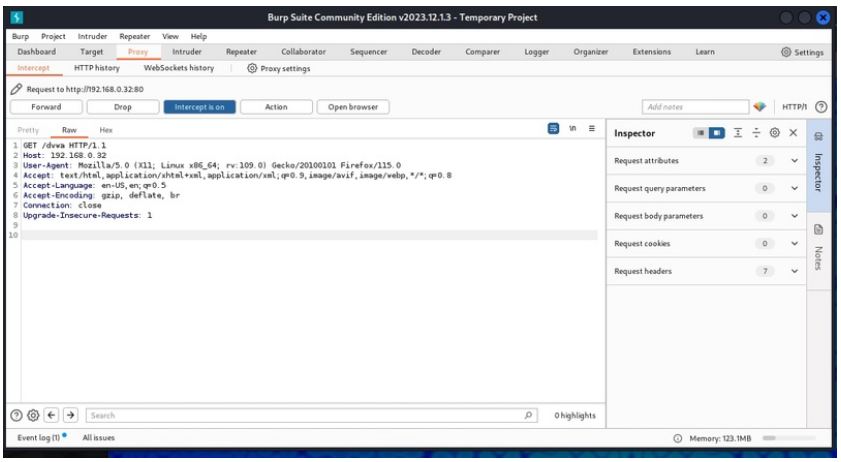

Рис. 3.4: 192.168.0.32/dvwa

Здесь мы получили первую информацию о ресурсе, к которому пытаемся подключиться. Нажимаем `Forward`. В этот момент, страница браузера продолжает загружаться (рис. [3.5]).

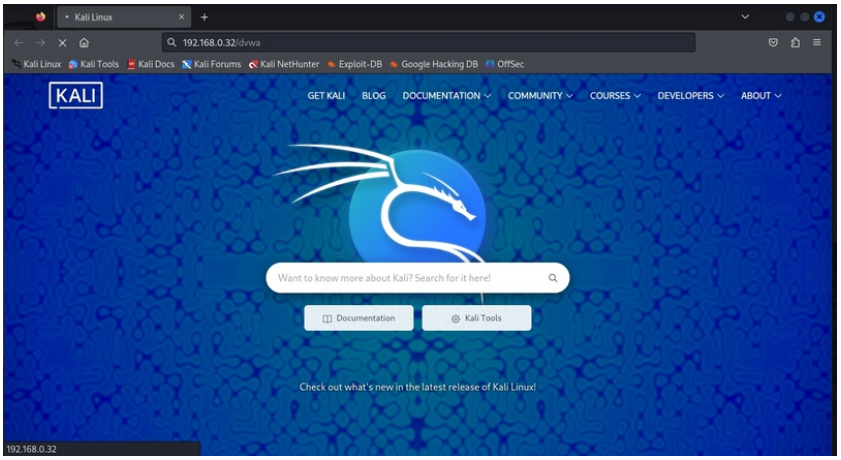

Рис. 3.5: Браузер

Однако, в `target` мы видим нашу цель и первые данные, полученные через `burp suite` (рис. [3.6]).

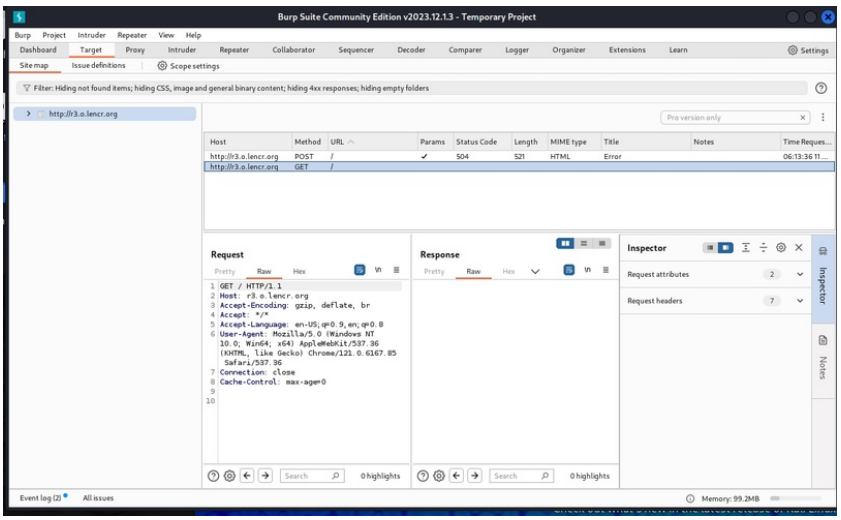

Рис. 3.6: Target

4 Выводы

В ходе лабораторной работы мы познакомились с инструментом сканирования сайтов `Burp Suite`.

Список литературы