

Отчёт по этапу №5 индивидуального проекта

Использование Burp Suite

Хусаинова Динара Айратовна, НПИбд-02-21, 1032212283

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Выводы	12
Список литературы. Библиография	13

Список иллюстраций

1	Запуск локального сервера	7
2	Запуск приложения	8
3	Сетевые настройки браузера	8
4	Настройки сервера	9
5	Настройки Burp Suite	9
6	Настройки Proxu	10
7	Настройки параметров	10
8	Получаемые запросы сервера	10
9	Страница авторизации	11

Цель работы

Научиться использовать Burp Suite.

Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений. [[@parasram](#)].

Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. [-@fig:001]).

```
dash
(dakhusainova@kali)-[~]
$ sudo systemctl start apache2
[sudo] password for dakhusainova:

(dakhusainova@kali)-[~]
$ sudo systemctl start apache2
Completing external command
1password2john
2to3-2.7
7z
7z2john
7za
7zr
411toppm
DPAPImk2john
FileCheck-16
FileCheck-17
GET
GenPat
HEAD
JxrDecApp
JxrEncApp
ModemManager
NetworkManager
POST
SIPdump
Thunar
UnicodeNameMappingGenerator-16
UnicodeNameMappingGenerator-17
VBoxClient
VBoxControl
VBoxService
X
(dakhusainova@kali)-[~]
$ sudo systemctl start mysql

(dakhusainova@kali)-[~]
$
```

Рис. 1: Запуск локального сервера

Запускаю инструмент Burp Suite (рис. [-@fig:002]).

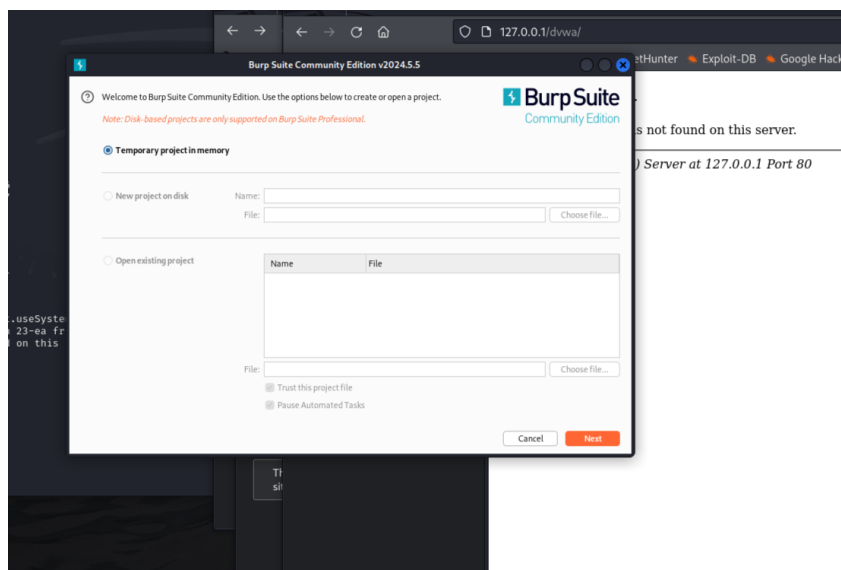


Рис. 2: Запуск приложения

Открываю сетевые настройки браузера, для подготовке к работе (рис. [-@fig:003]).

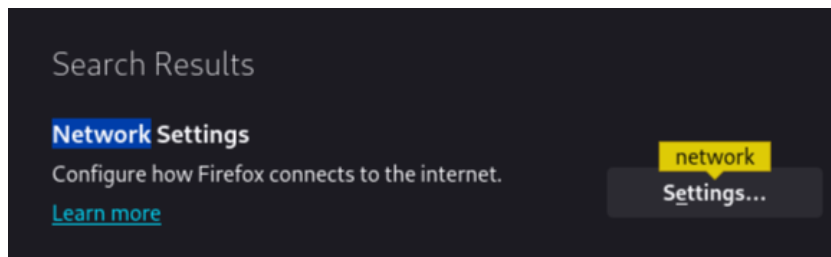


Рис. 3: Сетевые настройки браузера

Изменение настроек сервера для работы с проху и захватом данных с помощью Burp Suite (рис. [-@fig:004]).

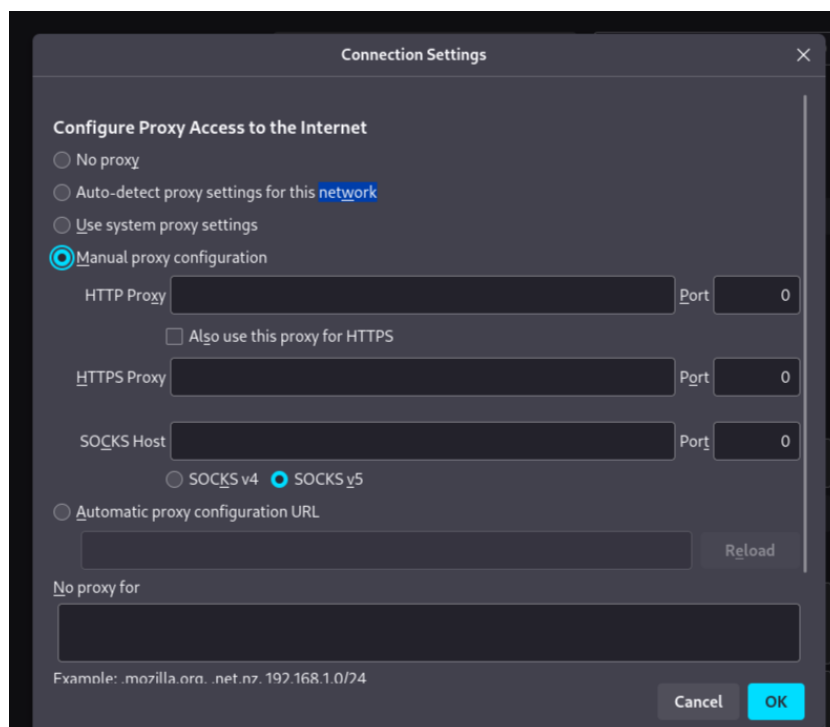


Рис. 4: Настройки сервера

Изменяю настройки Прoxy инструмента Burp Suite для дальнейшей работы (рис. [-@fig:005]).

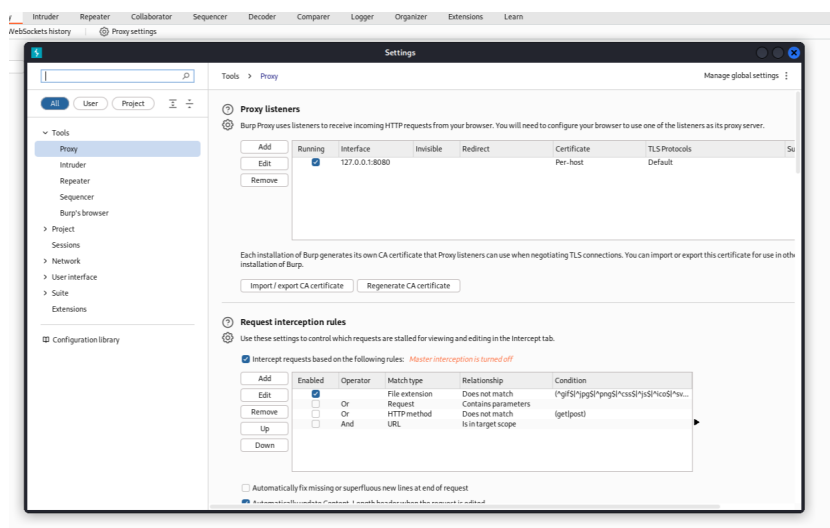


Рис. 5: Настройки Burp Suite

Во вкладке Proxy устанавливаю “Intercept is on” (рис. [-@fig:006]).

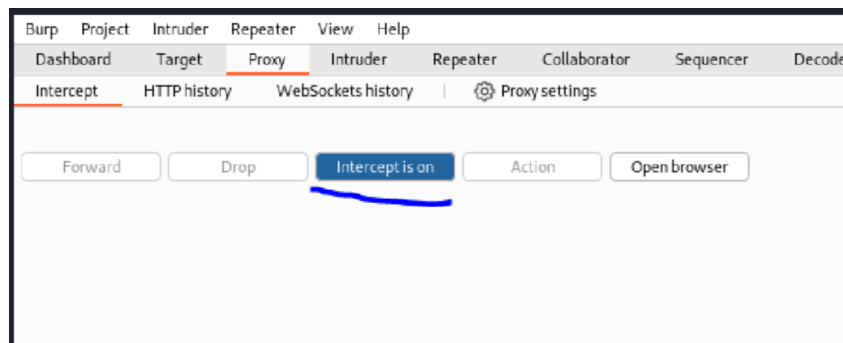


Рис. 6: Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network.proxy.allow_hijacking_localhost` на `true` (рис. [-@fig:007]).

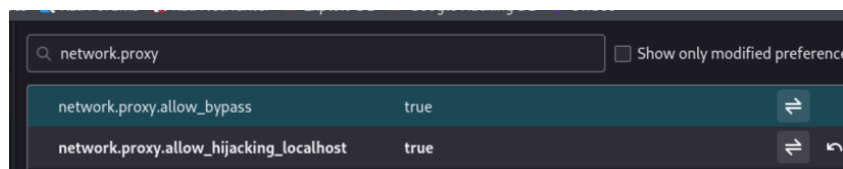


Рис. 7: Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:008]).

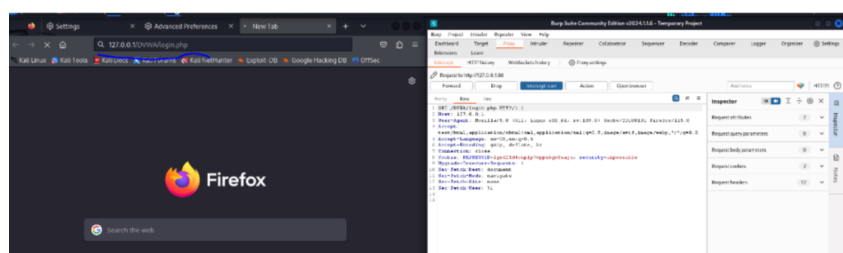


Рис. 8: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:009]).

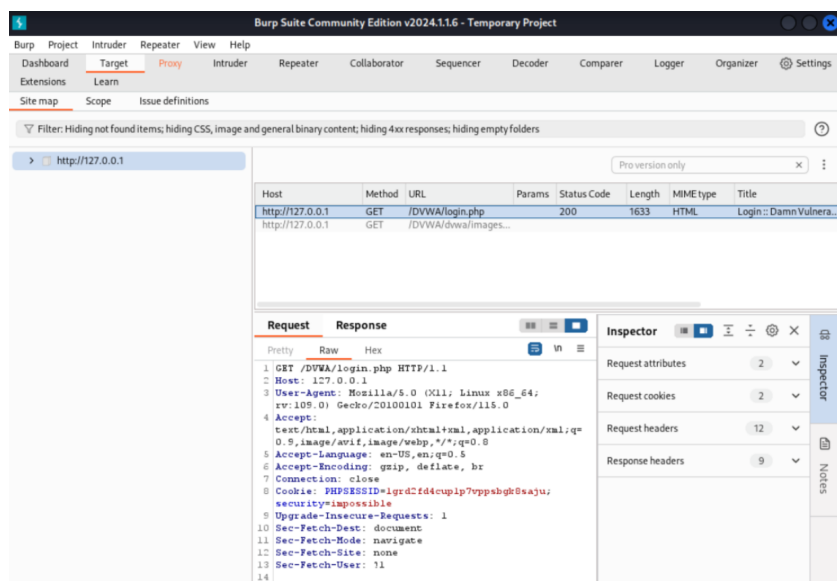


Рис. 9: Страница авторизации

История запросов хранится во вкладке Target.

Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

Список литературы. Библиография

[1] Документация по DVWA: <https://kali.tools/?p=1820>