

Этап №5 индивидуального проекта

Использование Burp Suite

Хусаинова Д.А. Группа НПИбд-02-21

Научиться использовать Burp Suite.

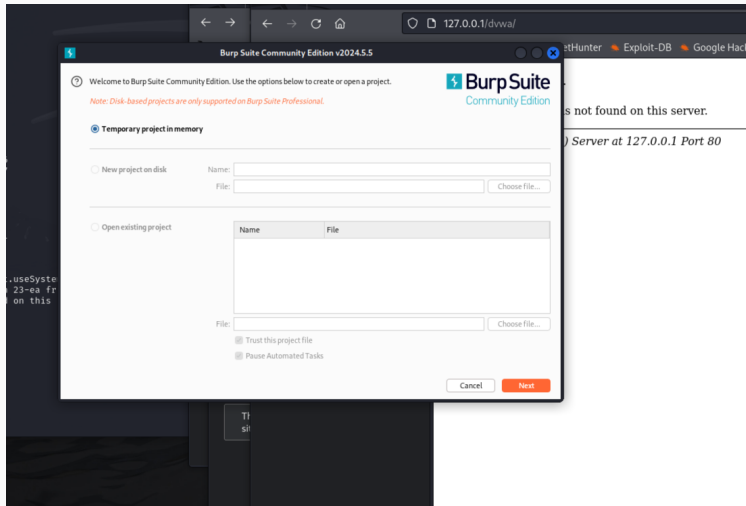
Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite

```
(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
```

Выполнение лабораторной работы

Запускаю инструмент Burp Suite



Выполнение лабораторной работы

Открываю сетевые настройки браузера, для подготовке к работе

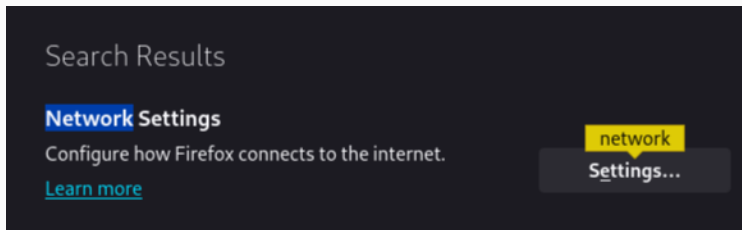
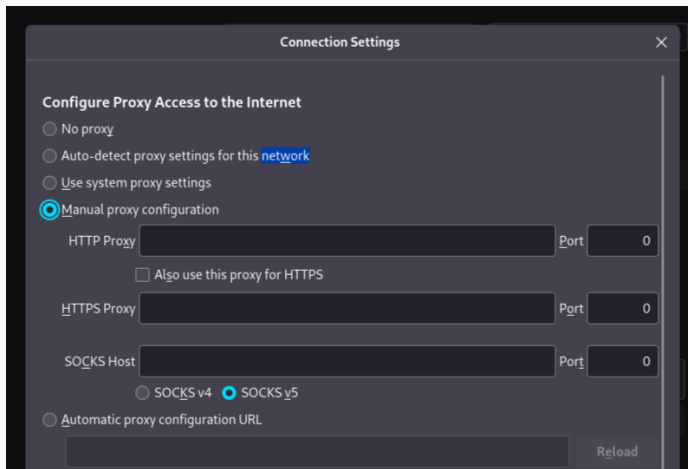


Рис. 3: Сетевые настройки браузера

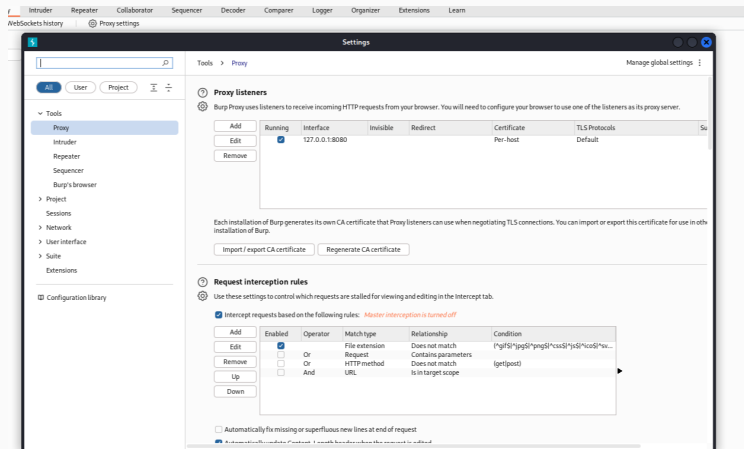
Выполнение лабораторной работы

Изменение настроек сервера для работы с прокси и захватом данных с помощью Burp Suite



Выполнение лабораторной работы

Изменяю настройки Прoxy инструмента Burp Suite для дальнейшей работы



Выполнение лабораторной работы

Во вкладке Proxy устанавливаю “Intercept is on”

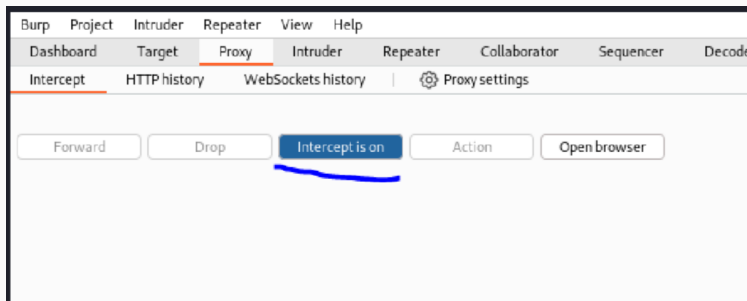


Рис. 6: Настройки Proxy

Выполнение лабораторной работы

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_loacalhost` на `true`

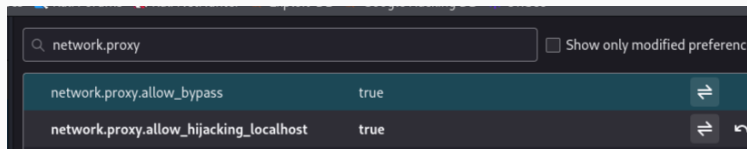


Рис. 7: Настройки параметров

Выполнение лабораторной работы

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxu появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу

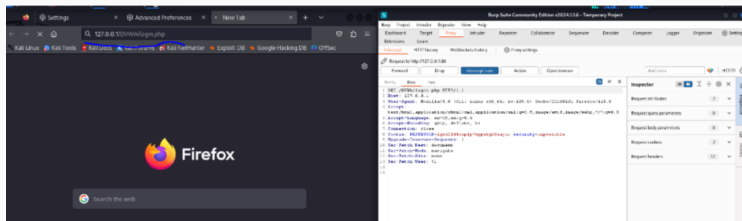


Рис. 8: Получаемые запросы сервера

Выполнение лабораторной работы

Загрузилась страница авторизации, текст запроса поменялся

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

> http://127.0.0.1

Host	Method	URL	Params	Status Code	Length	MIME type	Title
http://127.0.0.1	GET	/DVWA/login.php		200	1633	HTML	Login :: Damn Vulnerable...
http://127.0.0.1	GET	/DVWA/dvwa/images...					

Request Response

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Cookie: PHPSESSID=lgrd2fd4cupip7vppsbgk8saju; security=impossible
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14
```

Inspector

Request attributes 2

Request cookies 2

Request headers 12

Response headers 9

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

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