

# Основы информационной безопасности. Индивидуальный проект

## Этап № 5. Использование Burp Suite

---

Демидова Е.А.

09.09.2023

Российский Университет дружбы народов

## Информация

---

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/eademidova>



## Вводная часть

---

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

### **Задачи:**

- Перехватить HTTP запрос и ответ
- Проанализировать HTTP запрос и ответ

**Инструмент:** DVWA, Burp Suit

## Выполнение лабораторной работы

---

```
(root@eademidova)-[/home/eademidova]  
# chmod +x burpsuite_community_linux_v2024_5_5.sh
```

```
(root@eademidova)-[/home/eademidova]  
# ./burpsuite_community_linux_v2024_5_5.sh  
Unpacking JRE ...  
Starting Installer ...
```

Рис. 1: Установка ПО

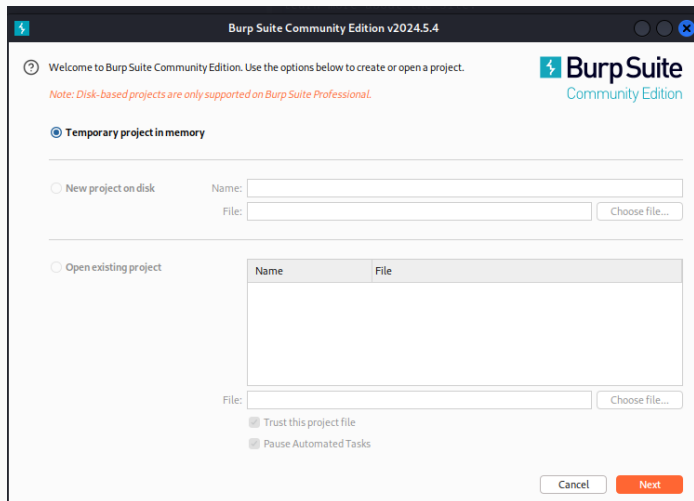


Рис. 2: Создание проекта



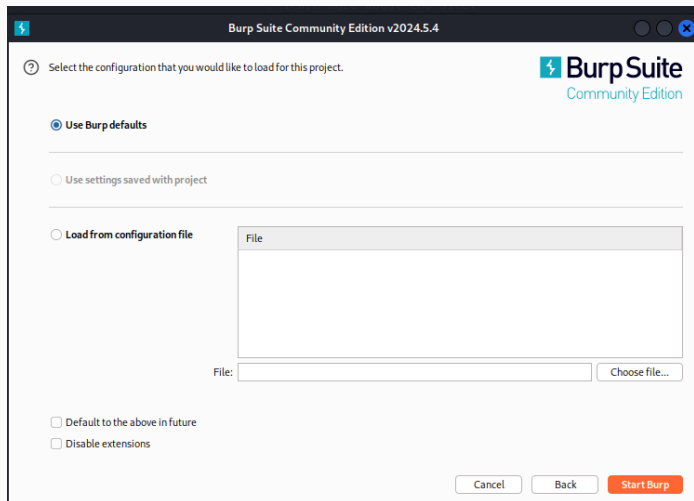


Рис. 3: Установка параметров

# Настройка перехвата трафика

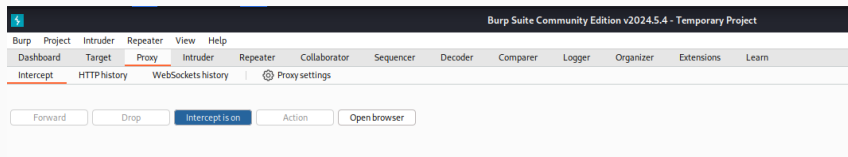


Рис. 4: Включение Burp Proxy

# Настройка перехвата трафика

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

127.0.0.1

Port

8080

☐ Also use this proxy for HTTPS

HTTPS Proxy

Port

0

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

Cancel

OK

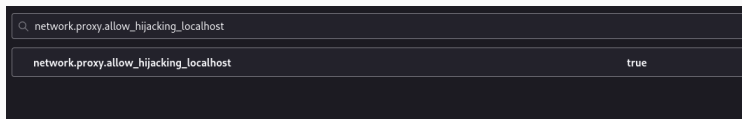


Рис. 6: Установка флага allow\_hijacking\_localhost

# Перехват запросов

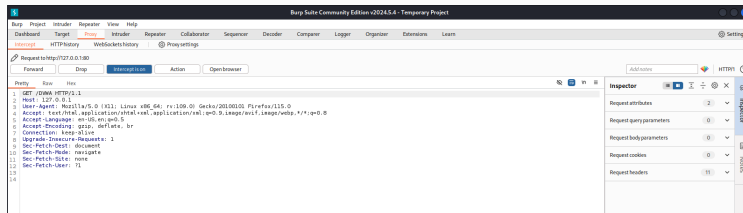


Рис. 7: Перехват запроса на вход на сайт

The screenshot displays the Burp Suite interface. The top menu bar includes Dashboard, Project, Intruder, Repeater, View, and Help. The main toolbar contains various tools like Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'HTTP history' tab is active, showing a list of intercepted requests. The selected request is a POST to /OWA/login.php. The 'Inspector' tab on the right shows the raw request and response data.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response...
9	http://127.0.0.1	GET	/OWA			301	564	HTML		301 Moved Permanently			127.0.0.1		06:17:35.2	8080	35
10	http://127.0.0.1	GET	/OWA			302	605	HTML					127.0.0.1	securityimposib...	06:20:53.2	8080	141
11	http://127.0.0.1	GET	/OWA/login.php			200	1669	HTML	php	Login: Damn Vulnerab...			127.0.0.1	06:21:04.2	8080	80	
14	http://127.0.0.1	GET	/favicon.ico			404	487	HTML	ico	404 Not Found			127.0.0.1	06:21:06.2	8080	13	
15	http://127.0.0.1	POST	/OWA/login.php			302	476	HTML	php	Login: Damn Vulnerab...			127.0.0.1	PHPSESSID=87ec...	06:23:53.2	8080	114
16	http://127.0.0.1	GET	/OWA/login.php			200	1706	HTML	php				127.0.0.1	06:24:57.2	8080	12	
17	http://127.0.0.1	POST	/OWA/login.php			302	476	HTML	php				127.0.0.1	PHPSESSID=87ec...	06:25:22.2	8080	41
18	http://127.0.0.1	GET	/OWA/index.php			200	6432	HTML	php	Welcome: Damn Vulner...			127.0.0.1	06:25:36.2	8080	6	
20	http://127.0.0.1	GET	/OWA/js/jquery.js			200	1366	script	js				127.0.0.1	06:25:36.2	8080	9	
21	http://127.0.0.1	GET	/OWA/js/jquery.event.listeners.js			200	912	script	js				127.0.0.1	06:25:36.2	8080	8	

**Request**

```
1 POST /OWA/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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/OWA/login.php
12 Cookie: security=asposable; PHPSESSID=87ec5315qo3ko0k0qkv1c1
13 Upgrade-Insecure-Requests: 1
14 Sec-Patch-Des: document
15 Sec-Patch-Mode: navigate
16 Sec-Patch-Site: same-origin
17 Sec-Patch-User: TL
18
19 username=admin&password=password&login=Login&user_token=
20 231d70bf45a2fc27fe40e9bb167b7f1
```

**Response**

```
1 HTTP/1.1 302 Found
2 Date: Fri, 02 Aug 2024 10:25:35 GMT
3 Server: Apache/2.4.61 (Ubuntu)
4 Expires: Thu, 19 Nov 2003 08:12:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=87ec5315qo3ko0k0qkv1c1; expires=Sat, 09 Aug 2024 10:25:35 GMT; Max-Age=64800; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

**Inspector**

Request attributes: 2

Request body parameters: 4

Request cookies: 2

Request headers: 16

Response headers: 11

Рис. 8: Запрос на аутентификацию

[illegible]

Рис. 9: Функция повторения запроса

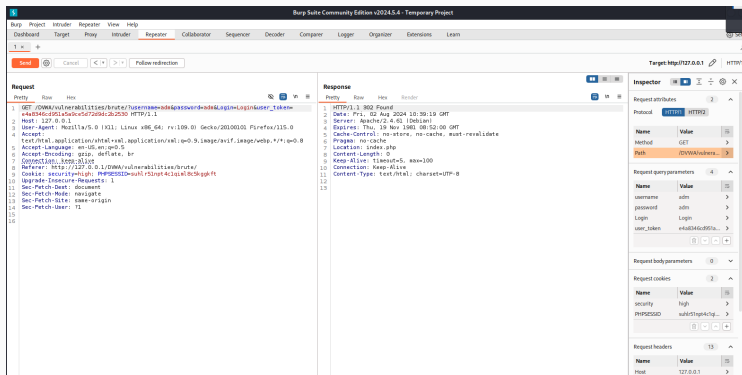


Рис. 10: Изучение ответа на запрос с функцией повторения запроса



## Заключение

---

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

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: <https://github.com/digininja/DVWA>.
2. Burp Suit [Электронный ресурс]. PortSwigger Ltd., 2024. URL: <https://portswigger.net/burp>.