

Пятый этап индивидуального проекта

Использование Burp Suite

Беличева Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- <https://dmbelicheva.github.io/ru/>



Освоить навыки использования Burp Suite.

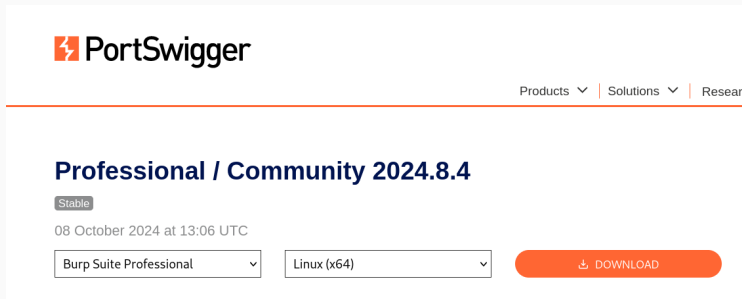
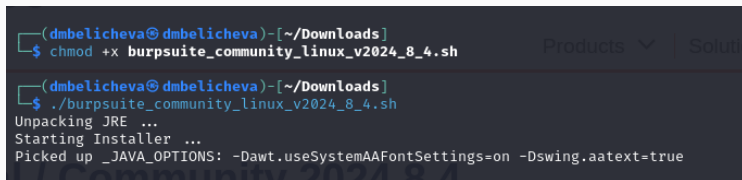


Рис. 1: Скачивание Burp Suite



```
(dmbelicheva@dmbelicheva) - [~/Downloads]
$ chmod +x burpsuite_community_linux_v2024_8_4.sh

(dmbelicheva@dmbelicheva) - [~/Downloads]
$ ./burpsuite_community_linux_v2024_8_4.sh
Unpacking JRE ...
Starting Installer ...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```

Рис. 2: Установка ПО

Выполнение лабораторной работы

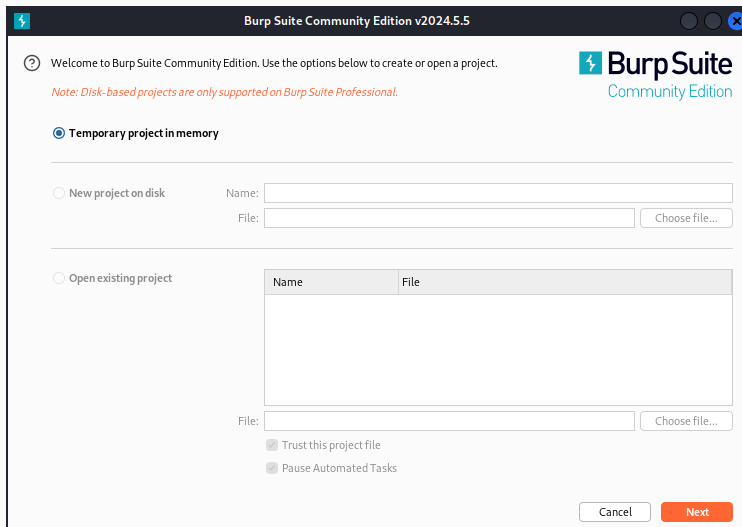


Рис. 3: Первоначальная настройка программы

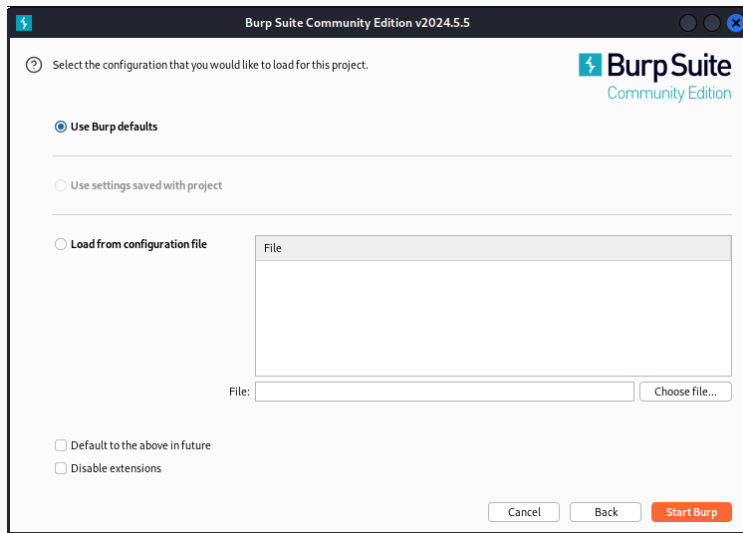


Рис. 4: Первоначальная настройка программы

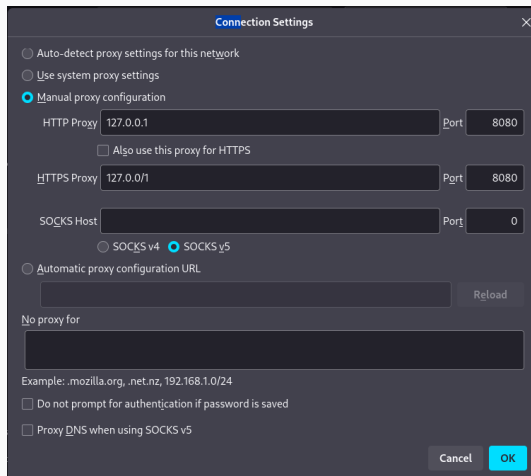


Рис. 5: Настройка прокси сервера

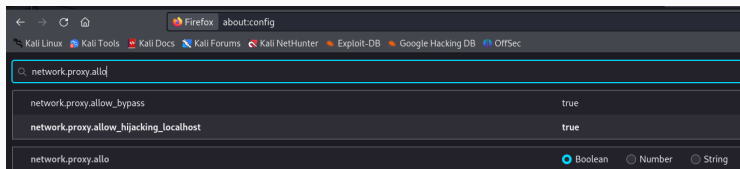


Рис. 6: Настройки параметров

Выполнение лабораторной работы

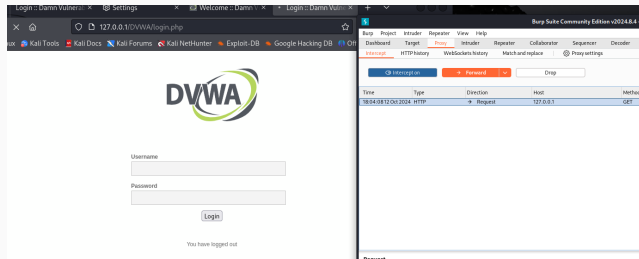


Рис. 7: Страница авторизации

Выполнение лабораторной работы

Burp Suite Community Edition v2024.8.4 - Temporary Project

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

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
6	http://127.0.0.1	GET	/DVWA/			302	337	HTML		
7	http://127.0.0.1	GET	/DVWA/login.php			200	1669	HTML	php	Login :: Damn Vu
8	http://127.0.0.1	POST	/DVWA/login.php	✓		302	449	HTML	php	
9	http://127.0.0.1	GET	/DVWA/login.php			200	1709	HTML	php	Login :: Damn Vu
11	http://127.0.0.1	POST	/DVWA/login.php	✓		302	449	HTML	php	
12	http://127.0.0.1	GET	/DVWA/index.php			200	6425	HTML	php	Welcome :: Dam
13	http://127.0.0.1	GET	/DVWA/setup.php			200	5632	HTML	php	Setup :: Damn Vu
14	http://127.0.0.1	GET	/DVWA/setup.php			200	5631	HTML	php	Setup :: Damn Vu
15	http://127.0.0.1	GET	/DVWA/			200	6339	HTML		Welcome :: Dam
16	http://127.0.0.1	GET	/DVWA/logout.php			302	337	HTML	php	
17	http://127.0.0.1	GET	/DVWA/login.php			200	1715	HTML	php	Login :: Damn Vu
18	http://127.0.0.1	GET	/DVWA/login.php					HTML	php	

Request

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 Referer: http://127.0.0.1/DVWA/
8 Connection: keep-alive
9 Cookie: security=low; PHPSESSID=6e0keiq5ieou9fos8g0tua8jbb
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
```

Inspecto

Request al

Request cc

Request hb

Рис. 8: http история запросов

Выполнение лабораторной работы

The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) login page. The page has a logo at the top and a login form with fields for "Username" (containing "test") and "Password" (containing "****"). A "Login" button is at the bottom. Below the form, a message states "CSRF token is incorrect".

Below the browser window is the Burp Suite Community Edition v2024.8.4 interface. The "HTTP history" tab is active, showing a list of requests. The selected request is a POST to /DVWA/login.php with a status code of 302. The "Request" pane shows the raw HTTP data, and the "Response" pane shows the raw HTTP data.

Request:

```
1 POST /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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 83
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: security=low; PHPSESSID=6e0keiq5ieus9foa8gtuabjbb
13 Upgrade-Insecure-Requests: 1
14 Sec-Patch-Dest: document
15 Sec-Patch-Mode: navigate
16 Sec-Patch-Site: same-origin
17 Sec-Patch-User: 71
18
19 username=test&password=test&login=Login&user_token=0cdcc76a2b7a98b509605bbb67ebbbea
```

Response:

```
1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 15:05:07 GMT
3 Server: Apache/2.4.62 (Debian)
4 Set-Cookie: PHPSESSID=6e0keiq5ieus9foa8gtuabjbb; expires=Sun, 13 Oct 2024 15:05:07 GMT; Max-Age=86400; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

Рис. 9: Попытка авторизации с неправильными данными, просмотр POST-запроса

Выполнение лабораторной работы

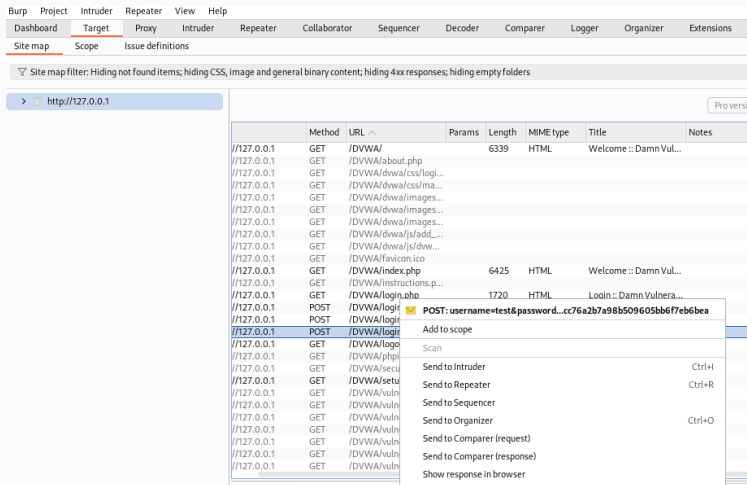


Рис. 10: Отправка запроса к Intruder

Выполнение лабораторной работы

?

Choose an attack type

Start attack

Attack type: Cluster bomb

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://127.0.0.1

☒ Update Host header to match target

Add §
Clear §
Auto §
Refresh

```
1 POST /DWWA/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: 89
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DWWA/login.php
12 Cookie: security=low; PHPSESSID=Ge0keiq5ieou9fos8g0tuaBjbb
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 username=Stest5&password=Stest5&Login=Login&user_token=0cdcc76a2b7a98b509605bb6f7eb6bea
```

Рис. 11: Задание параметров атаки

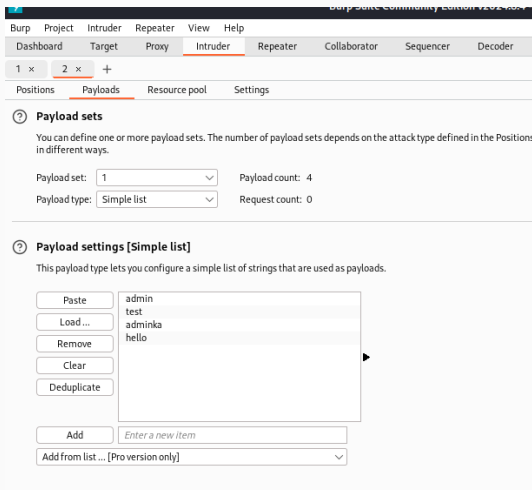


Рис. 12: Первый Simple list

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Payloads' sub-tab is active, displaying the 'Payload sets' configuration. Below this, the 'Payload settings [Simple list]' section is shown, which includes a list of payload strings and various management buttons.

Burp Suite Interface:

- Menu: Burp, Project, Intruder, Repeater, View, Help
- Sub-menu: Dashboard, Target, Proxy, **Intruder**, Repeater, Collaborator, Sequencer, D
- Tab bar: 1 x, **2 x**, +
- Sub-tab bar: Positions, **Payloads**, Resource pool, Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the target.

Payload set: Payload count: 4

Payload type: Request count: 16

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

password
12345
qwerty
bella

Рис. 13: Второй Simple list

Выполнение лабораторной работы

Attack Save

2. Intruder attack of http://127.0.0.1 Attack ▾

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	3			449	
1	admin	password	302	0			448	
2	test	password	302	2			448	
3	adminika	password	302	4			448	
4	hello	password	302	3			449	
5	admin	12345	302	9			448	
6	test	12345	302	4			449	
7	adminika	12345	302	6			448	
8	hello	12345	302	4			449	
9	admin	qwerty	302	3			448	
10	test	qwerty	302	4			449	
11	adminika	qwerty	302	6			448	
12	hello	qwerty	302	4			449	
13	admin	bella	302	5			448	
14	test	bella	302	4			449	
15	adminika	bella	302	8			448	
16	hello	bella	302	16			449	

Рис. 14: Результаты атаки

Выполнение лабораторной работы

Attack Save

11. Intruder attack of http://127.0.0.1

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received
0			302	6
1	admin	password	302	2
2	hello	password	302	4
3	adminka	password	302	6
4	testik	password	302	2
5	admin	12345	302	13
6	hello	12345	302	1
7	adminka	12345	302	4
8	testik	12345	302	3
9	admin	hello	302	2
10	hello	hello	302	3
11	adminka	hello	302	3
12	testik	hello	302	2
13	admin	password	302	14

Request Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 15:41:54 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=e6sm4o96m6jdpenn0u5ngqpgvb7; expires=Sun, 13 Oct 2024 15:41:54 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Lax
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=98
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13

Рис. 15: Результат неправильного запроса

11. Intruder attack of http://127.0.0.1

Attack Save

11. Intruder attack of http://127.0.0.1

Results Positions Payloads Resource pool Settings

▼ Intruder attack results filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received	Error
0			302	6	
1	admin	password	302	2	
2	hello	password	302	4	
3	adminka	password	302	6	
4	testik	password	302	2	
5	admin	12345	302	13	
6	hello	12345	302	1	
7	adminka	12345	302	4	
8	testik	12345	302	3	
9	admin	hello	302	2	
10	hello	hello	302	3	
11	adminka	hello	302	3	
12	testik	hello	302	2	
13	admin	nwerbu	302	14	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 15:41:54 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=npeqlgsq5pj2d4lfwe4s4b98ju; expires=Sun, 13 Oct 2024 15:41:54 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
```

Рис. 16: Результат правильного запроса

Выполнение лабораторной работы

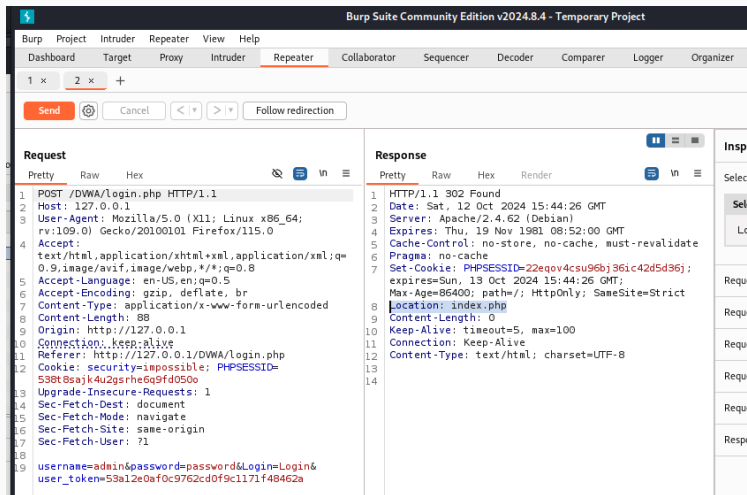


Рис. 17: Вкладка Repeater

В результате выполнения данного этапа проекта я освоила навыки использования Burp Suite.

1. Burp Suite Tips [Электронный ресурс]. 2020. URL: <https://habr.com/ru/articles/510612/>.