

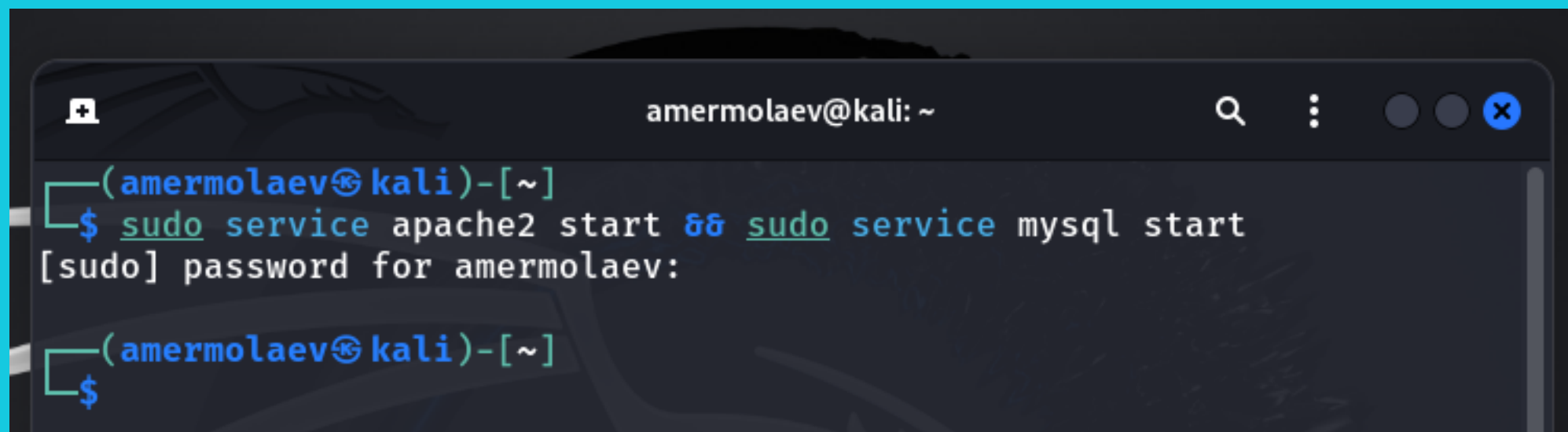
Презентация к 5 этапу индивидуального проекта

Цель работы: приобрести практический навык по использованию инструмента Burp Suite - набора мощных инструментов безопасности веб-приложений.



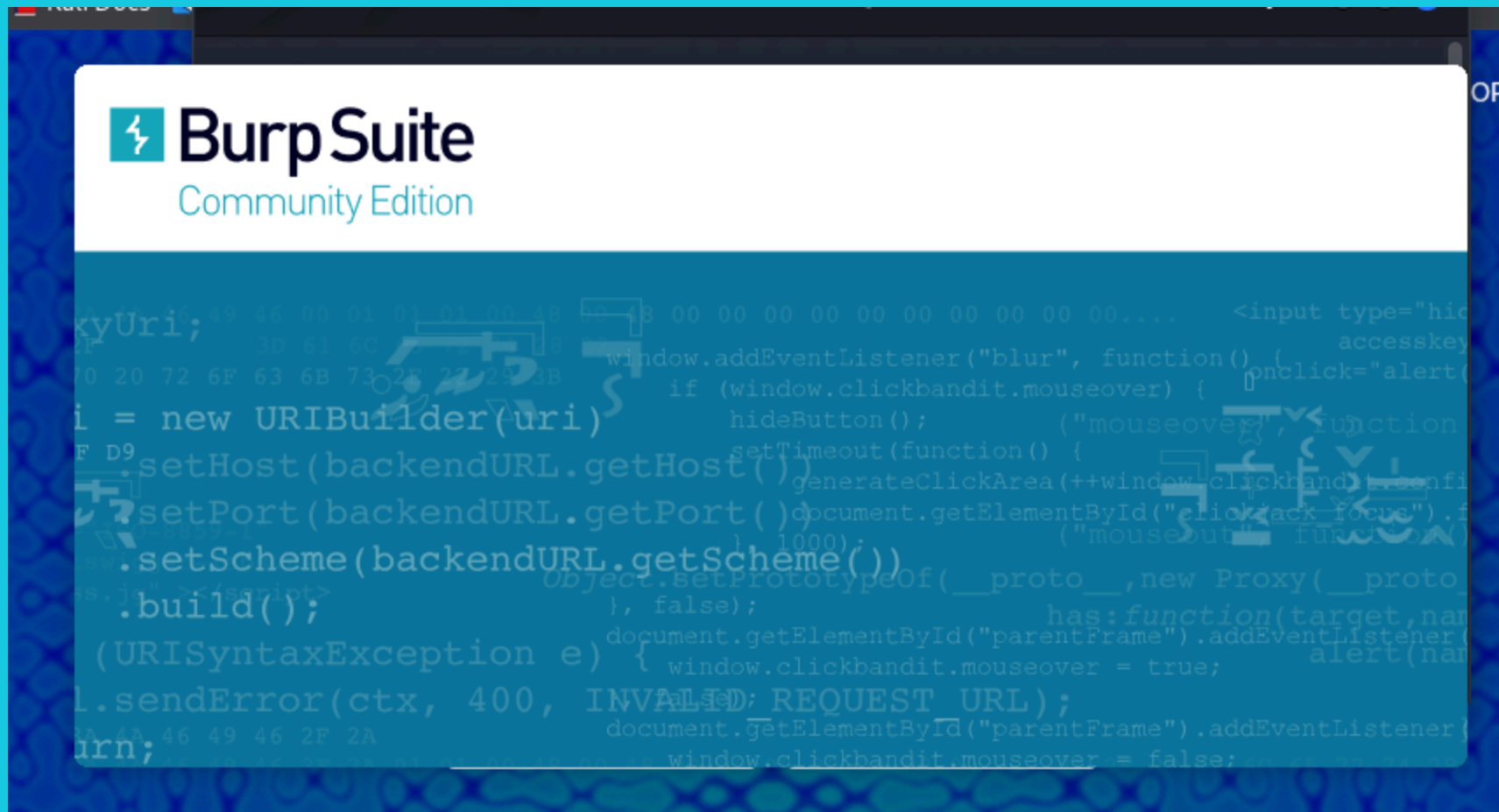
Выполнение работы

Запуск сервисов

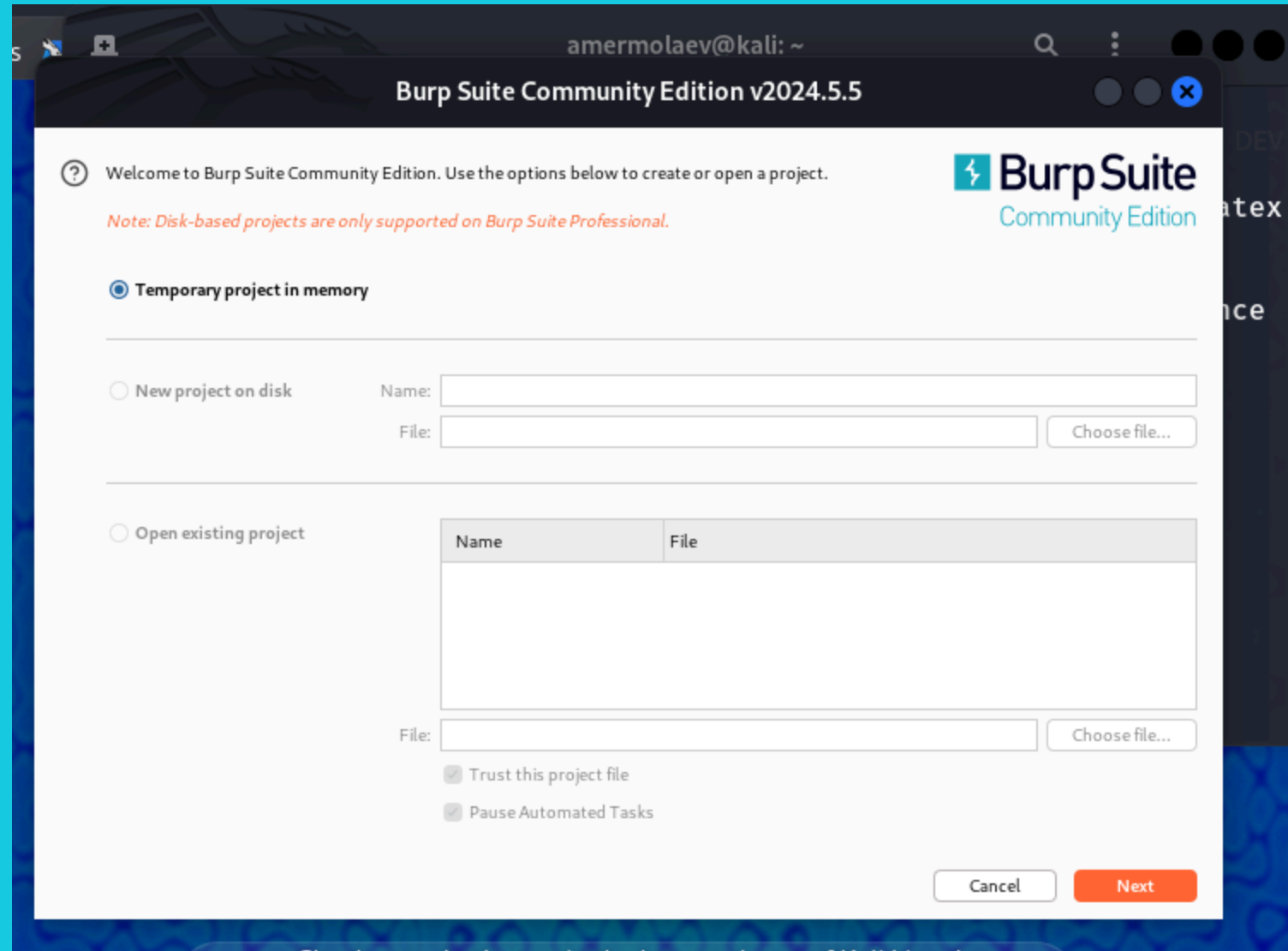


```
amermolaev@kali: ~  
└─(amermolaev@kali)-[~]  
└─$ sudo service apache2 start && sudo service mysql start  
[sudo] password for amermolaev:  
└─(amermolaev@kali)-[~]  
└─$
```

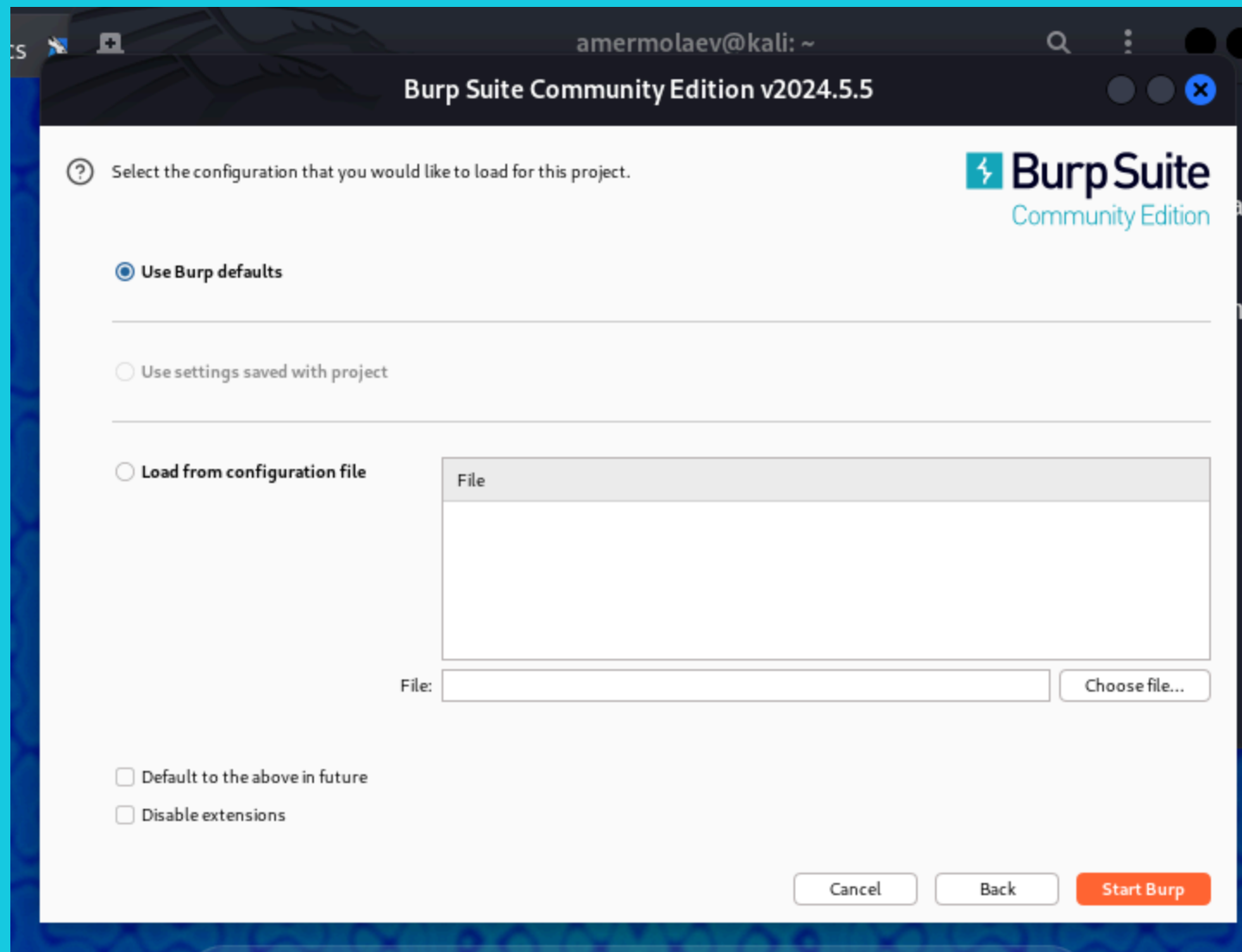
Запуск Burp Suite



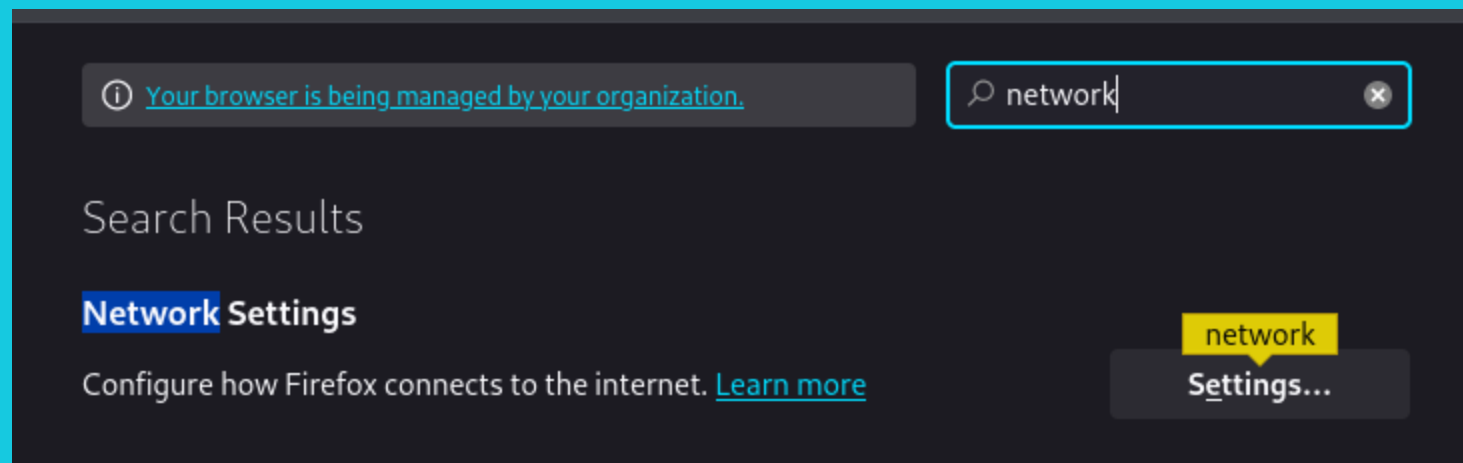
Настройки проекта



Настройки проекта



Настройка браузера



Настройка браузера

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

Cancel

OK

Настройки в Burp Suite

AllUserProject

Tools

Proxy

Intruder

Repeater

Sequencer

Burp's browser

Project

Sessions

Network

User interface

Suite

Extensions

Configuration library

Tools > Proxy

Manage global settings

Project setting

Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

AddEditRemove

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default	<input checked="" type="checkbox"/>

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificateRegenerate CA certificate

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules: Master interception is turned off

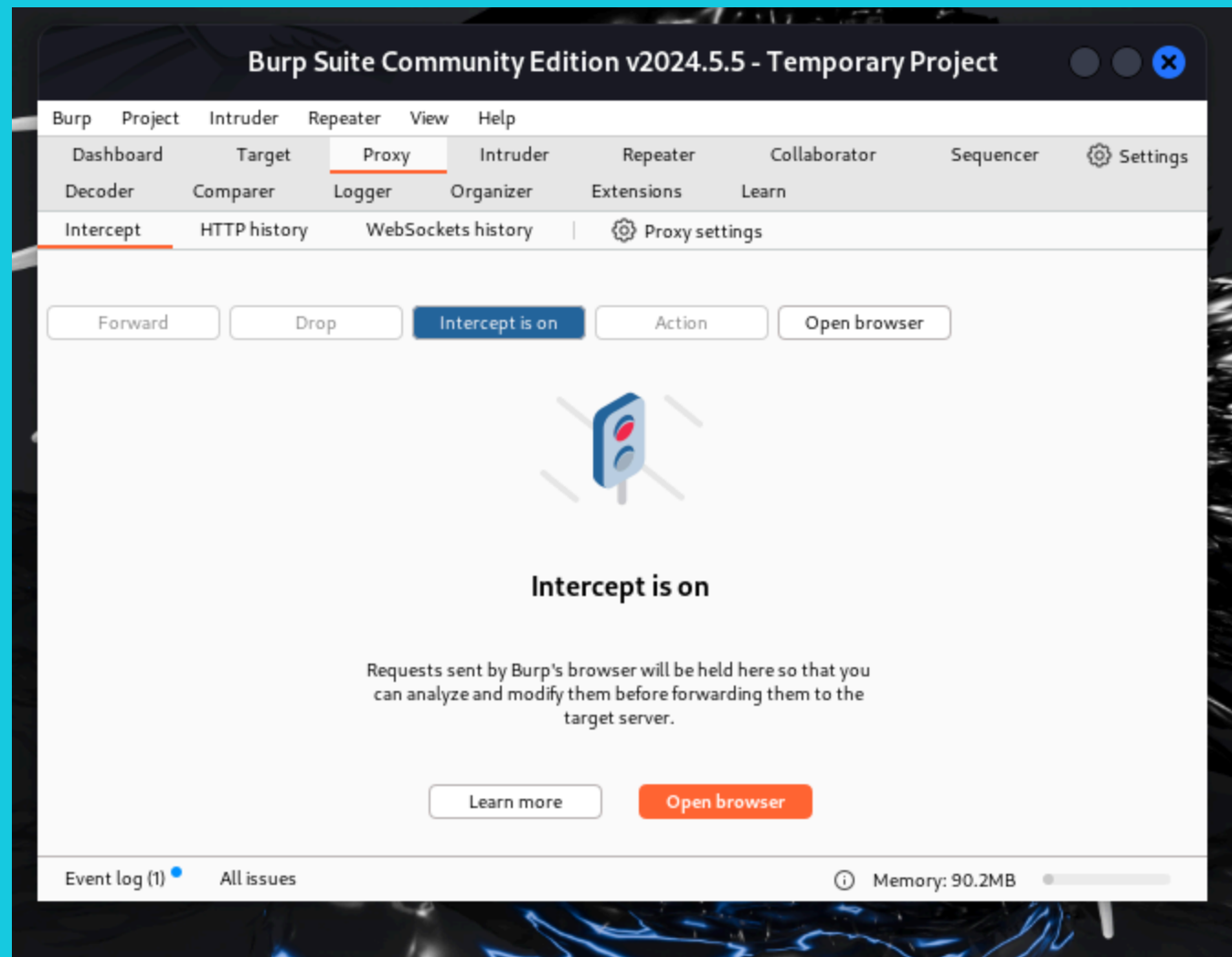
AddEditRemoveUpDown

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico...
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

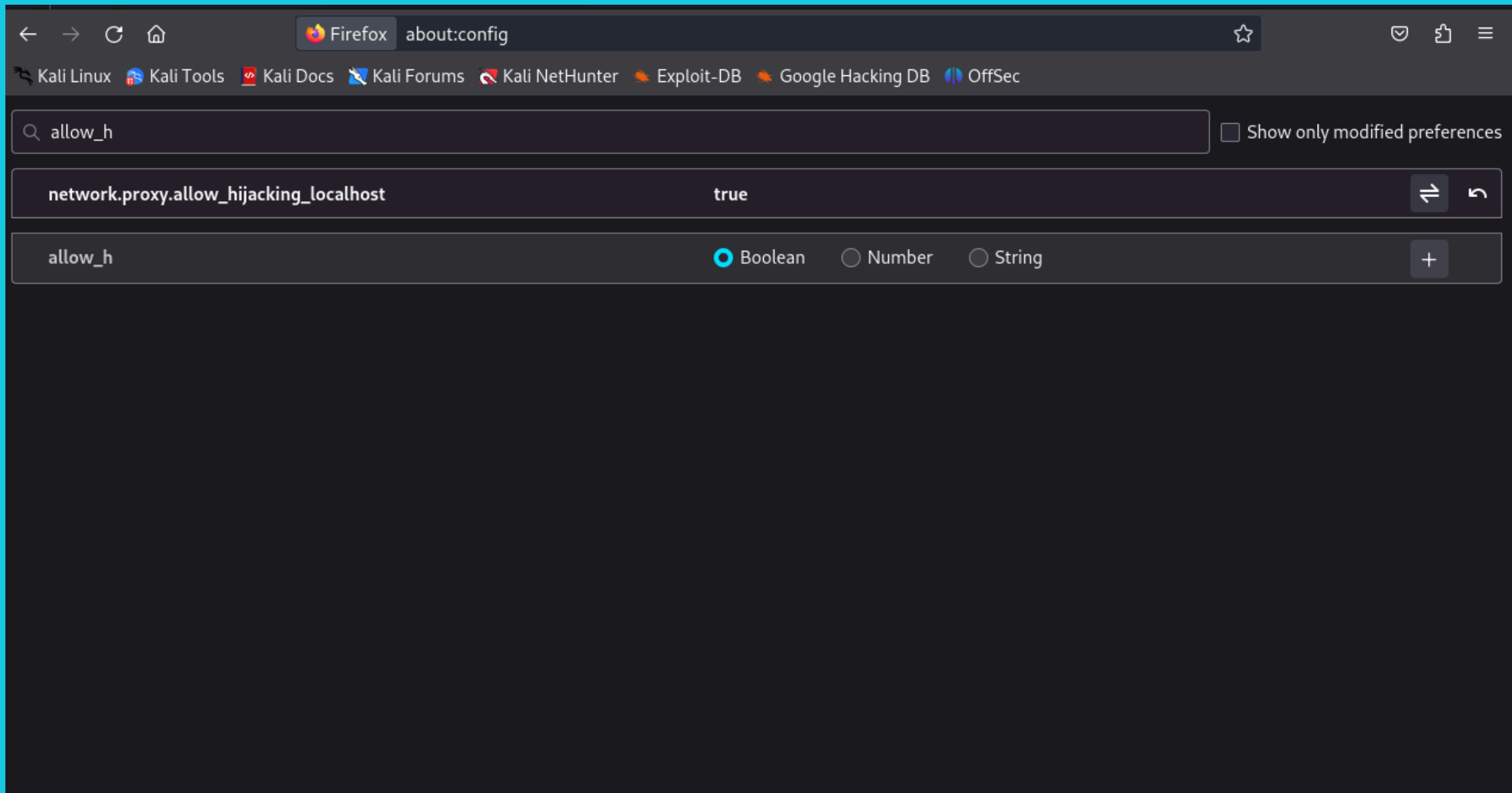
☐ Automatically fix missing or superfluous new lines at end of request

☒ Automatically update Content-Length header when the request is edited

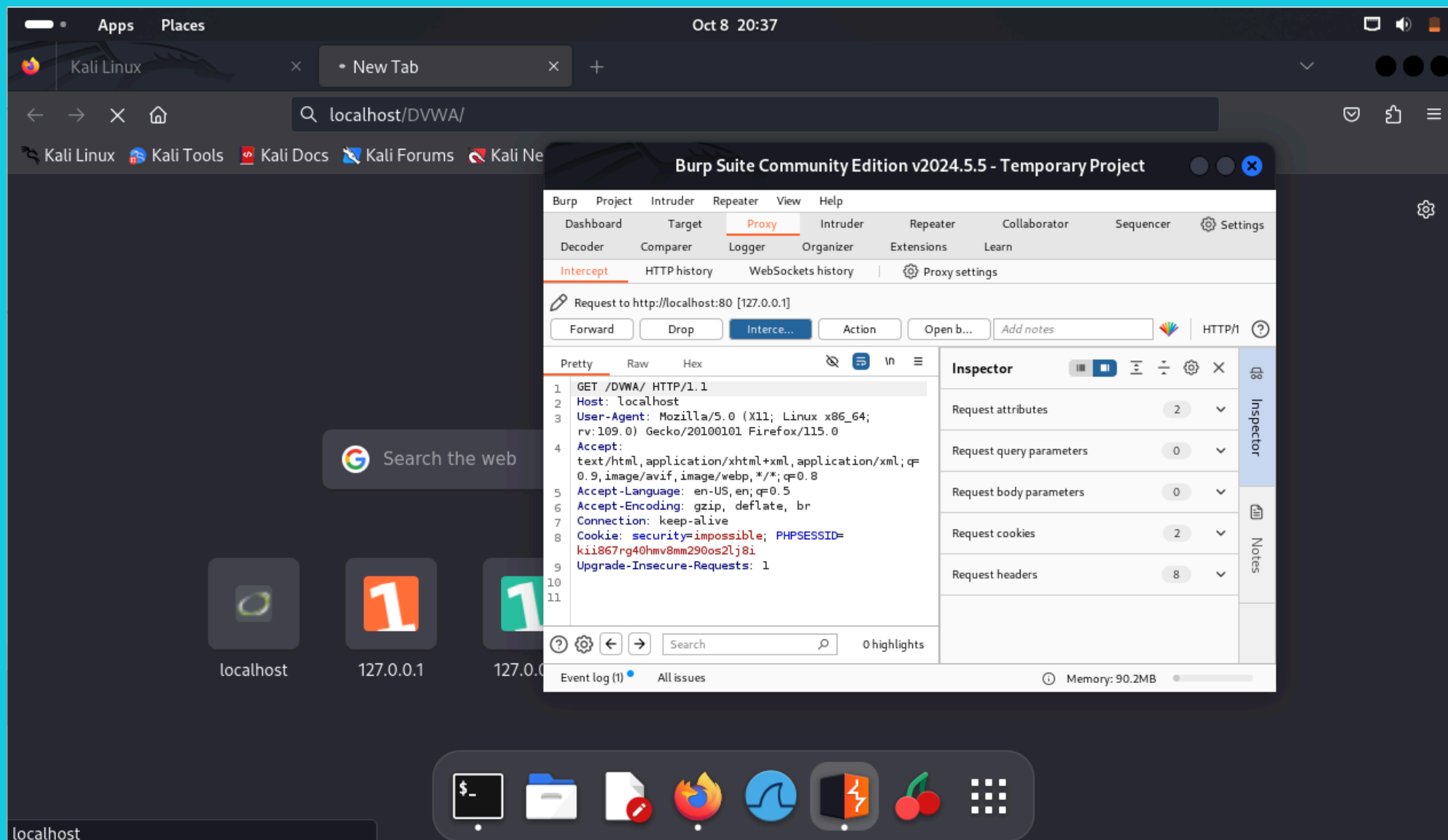
Внедрение Burp Suite



Изменение переменных браузера



Перехваченный запрос



Загрузка страницы

The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) login page. The page has a large DVWA logo at the top and two input fields for 'Username' and 'Password', with a 'Login' button below them. The browser's address bar shows 'localhost/DVWA/login.php'. The browser's taskbar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', and 'Exploit-DB'.

Overlaid on the right is the Burp Suite Community Edition v2024.5.5 interface. The 'Intercept' tab is active, showing a POST request to 'http://r11.o.lencr.org:80 [2.20.255.114]'. The request details are visible in the 'Inspector' panel on the right, showing request attributes, query parameters, body parameters, cookies, and headers. The 'Raw' tab shows the raw HTTP request data.

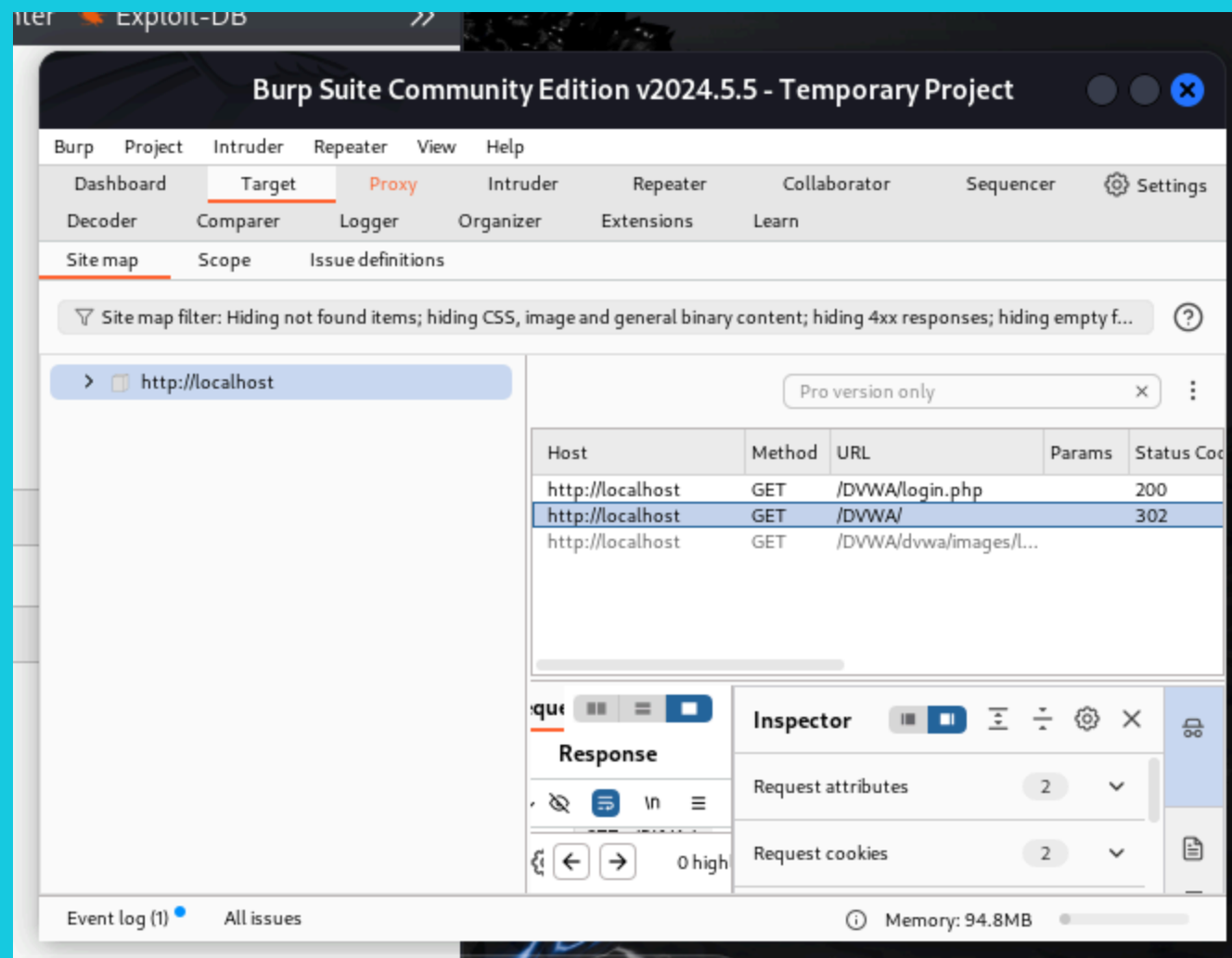
Request details (Inspector):

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 11
- Request cookies: 0
- Request headers: ..

Raw request data:

```
POST / HTTP/1.1
Host: r11.o.lencr.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/ocsp-request
Content-Length: 85
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
050Q000M0K0+R+YäÄ3!~mK2; ÖgÎ¹; #D'è -Ü8'Ö{!E!pXæÙ-
```

Раздел Target



Перехват отправки формы

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 "bobr") and "Password" (masked with dots). A "Login" button is below the fields. The message "Login failed" is visible at the bottom of the form. The browser's address bar shows "localhost/DVWA/login.php".

Overlaid on the browser is the Burp Suite Community Edition v2024.5.5 interface. The "Intercept" tab is active, showing a request to "http://localhost:80 [127.0.0.1]". The "Pretty" view of the request is displayed in the main pane, showing headers and body parameters. The "Inspector" pane on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Request Headers (Pretty View):

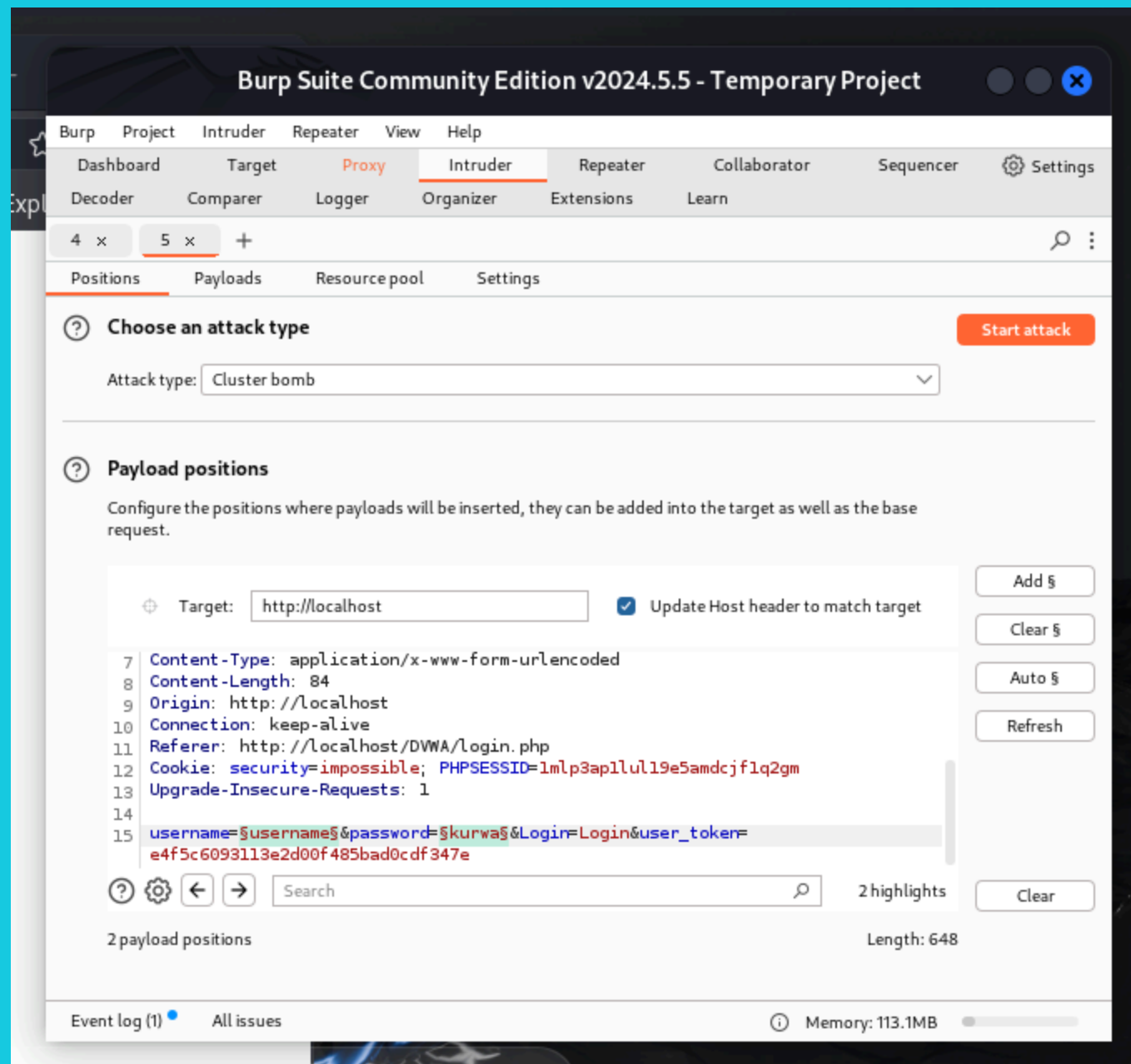
```
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 84
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/DVWA/login.php
12 Cookie: security=impossible; PHPSESSID=4s3ao6bkloqpo3o2gv34hb8isf
13 Upgrade-Insecure-Requests: 1
```

Request Body Parameters (Pretty View):

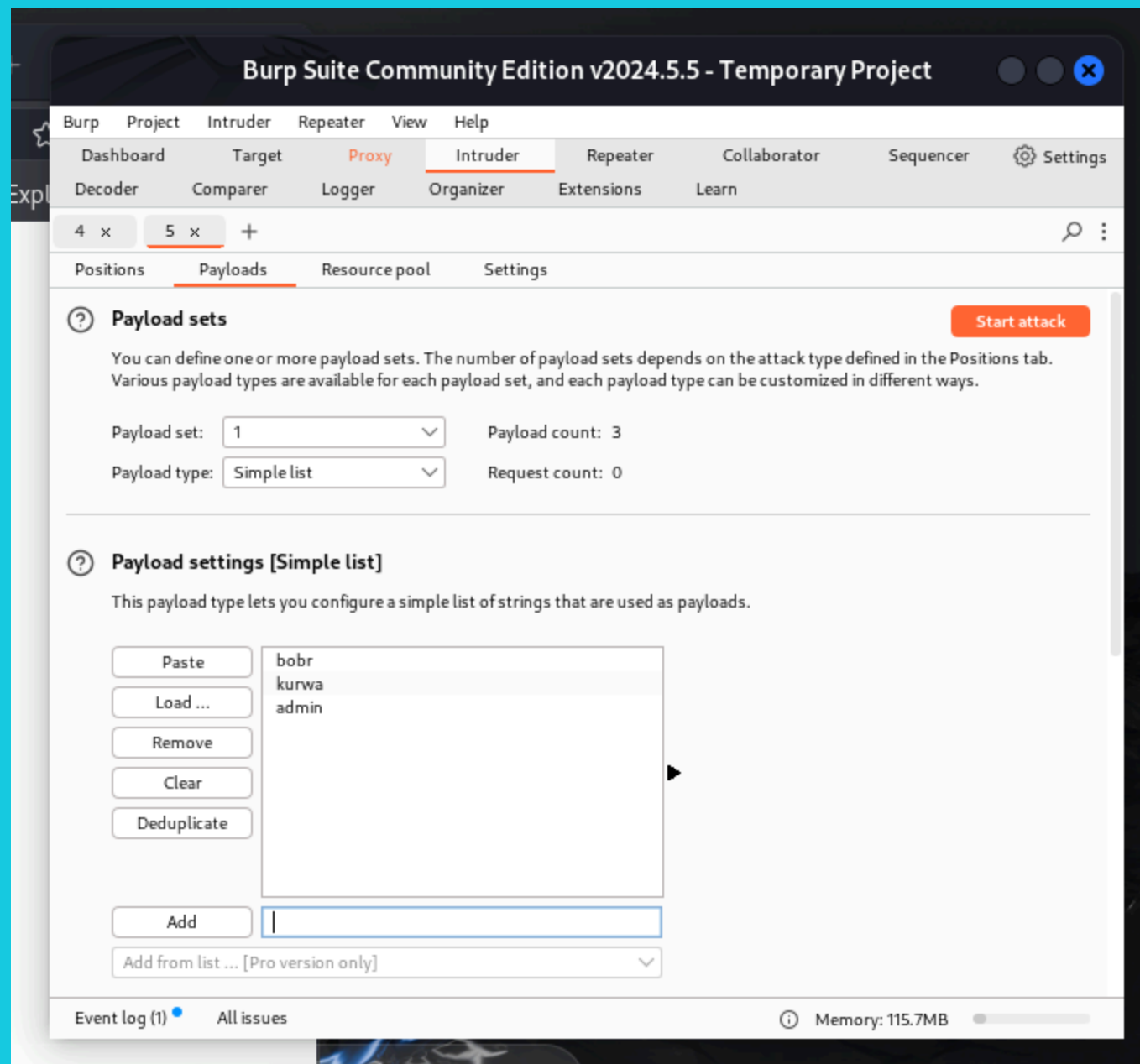
```
14 username=bobr&password=kurwa&Login=Login&
15 user_token=40df750eac91d63b052b2c51582731d1
```

The Burp Suite interface also shows the "Event log (1)" at the bottom, indicating one intercepted event.

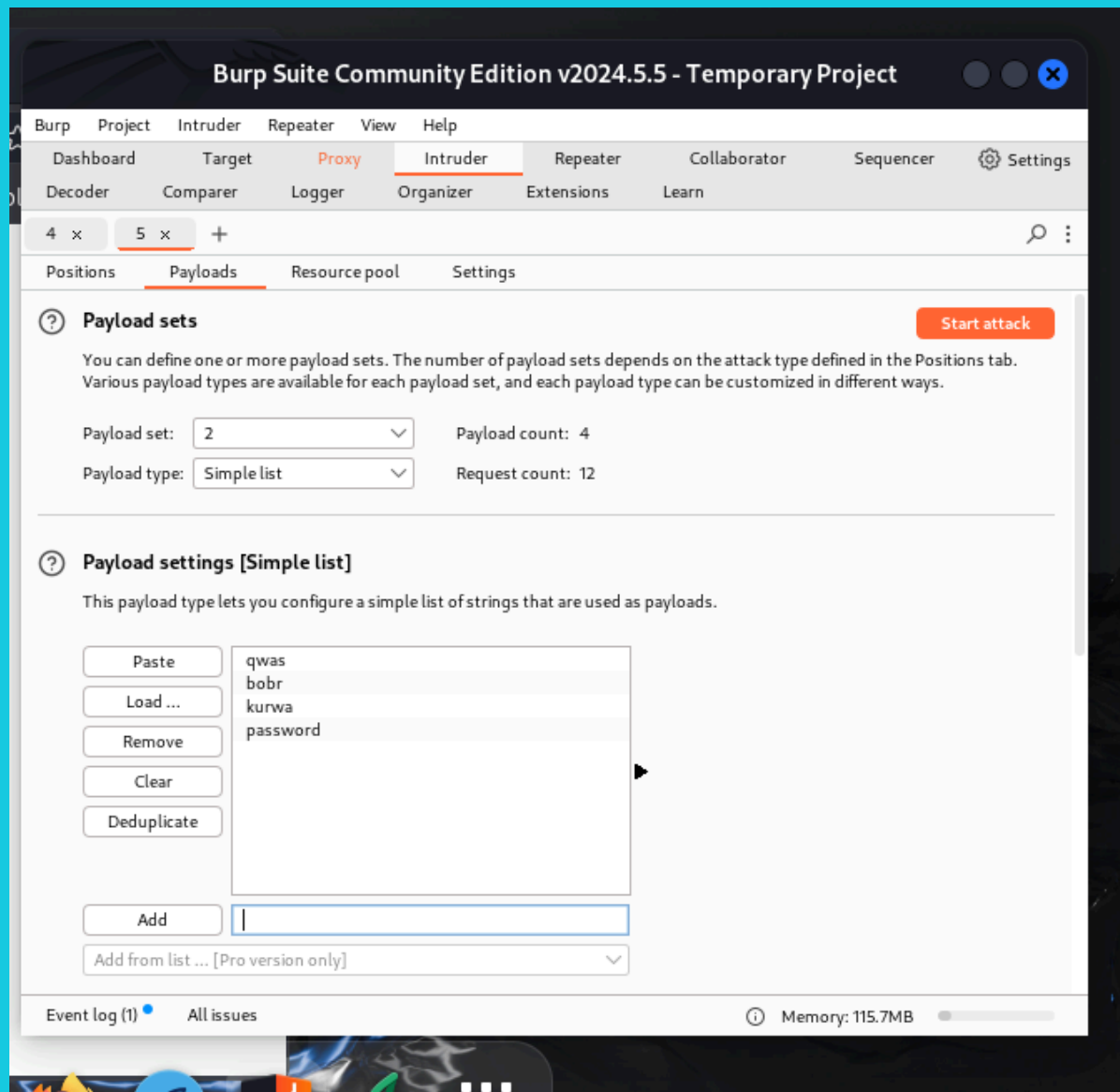
Попытка подбора логина и пароля



Подбор логина



Подбор пароля



Имитация атаки

Attack Save

2. Intruder attack of http://localhost

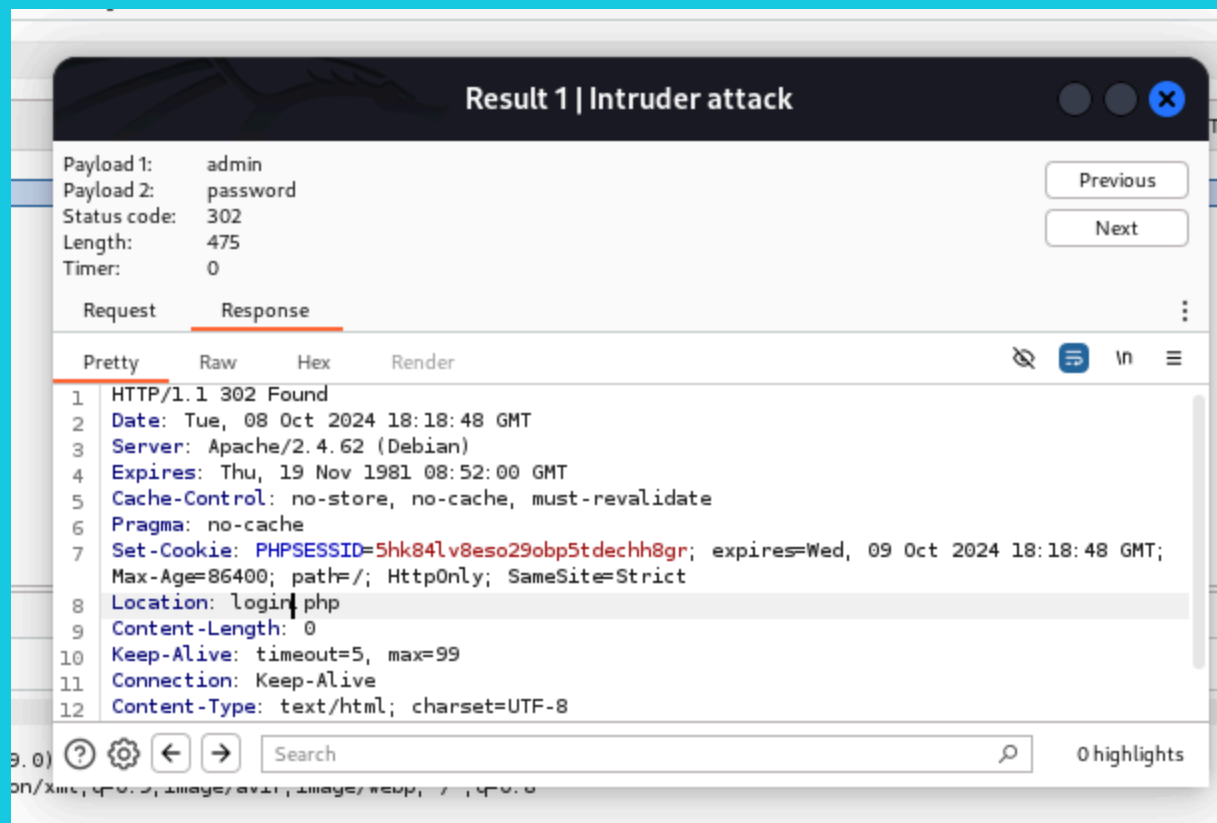
Attack Save ?

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	0			476	
1	bobr	qwas	302	0			475	
2	kurwa	qwas	302	0			476	
3	admin	qwas	302	22			475	
4	bobr	bobr	302	11			476	
5	kurwa	bobr	302	2			475	
6	admin	bobr	302	0			476	
7	bobr	kurwa	302	0			475	
8	kurwa	kurwa	302	2			476	
9	admin	kurwa	302	13			475	
10	bobr	password	302	1			476	
11	kurwa	password	302	0			475	
12	admin	password	302	3			476	

Имя скрипта



Вкладка Repeater

Burp Suite Community Edition v2024.5.5 - Temporary Project

Menu: Burp, Project, Intruder, Repeater, View, Help

Sub-menu: Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Settings

Organizer, Extensions, Learn

3 x +

Send Cancel < >

Target: http://localhost HTTP/1

Request

Pretty Raw Hex

```
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://localhost  
10 Connection: keep-alive  
11 Referer: http://localhost/DVWA/Login.php  
12 Cookie: security=impossible; PHPSESSID=  
1mlp3ap1lul19e5amdcjflq2gm  
13 Upgrade-Insecure-Requests: 1  
14  
15 username=admin&password=password&Login=  
Login&user_token=  
e4f5c6093113e2d00f485bad0cdf347e
```

Response

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 4
- Request cookies: 2
- Request headers: 12

Inspector Notes

Ready

Event log (2) All issues

Memory: 134.2MB

Разметка страницы авторизации

The screenshot displays the Burp Suite Community Edition v2024.5.5 interface. The 'Repeater' tab is active, showing a single request and response. The target is set to `http://localhost`.

Request:

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
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 Origin: http://localhost
8 Connection: keep-alive
9 Referer: http://localhost/DVWA/login.php
10 Cookie: security=impossible; PHPSESSID=1mlp3ap1lul19e5amdcjflq2gm
11 Upgrade-Insecure-Requests: 1
12
13
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Tue, 08 Oct 2024 18:24:38 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 1342
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13 <!DOCTYPE html>
14 <html lang="en-GB">
15 <head>
16
17 <meta http-equiv="Content-Type"
18 content="text/html; charset=UTF-8" />
19
20 <title>
21
```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 10
- Response headers: 10

Footer:

Done 1,670 bytes | 1,005 millis

Event log (2) All issues Memory: 146.8MB

Раздел Render

Burp Suite Community Edition v2024.5.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Settings

3 x +

Send Cancel < >

Target: http://localhost HTTP/1


Request

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
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 Origin: http://localhost
8 Connection: keep-alive
9 Referer: http://localhost/DVWA/login.php
10 Cookie: security=impossible; PHPSESSID=
  1mlp3ap1lul19e5amdcjflq2gm
11 Upgrade-Insecure-Requests: 1
12
13
```

Response

Pretty Raw Hex **Render**



Username

Password

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 10

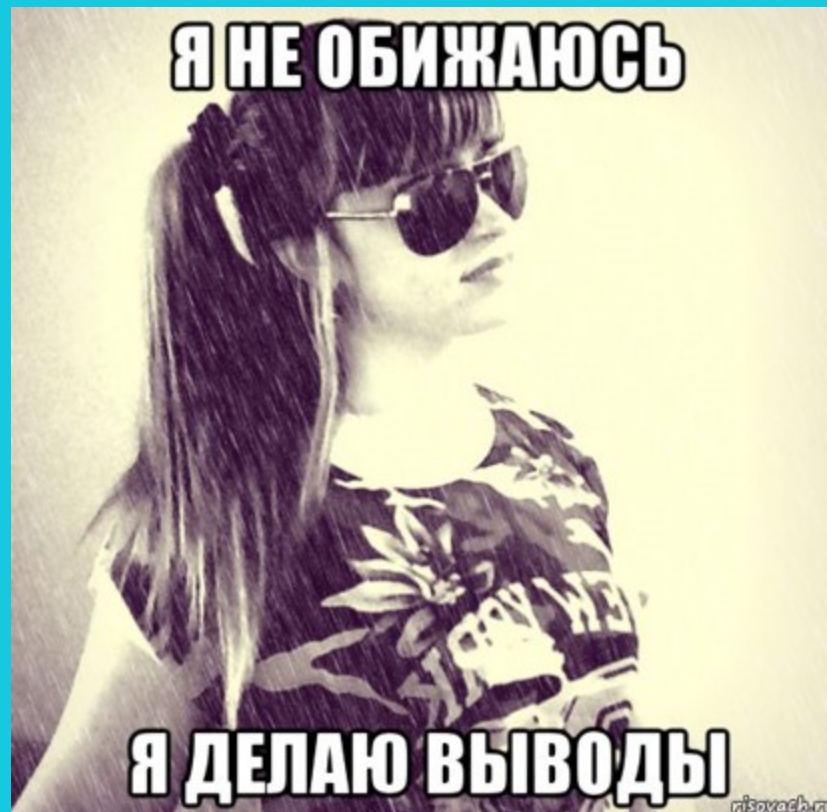
Response headers 10

Done 1,670 bytes | 1,005 millis

Event log (2) All issues Memory: 146.8MB

Вывод

В рамках выполнения работы я приобрел практический навык по использованию инструмента Burp Suite - набора мощных инструментов безопасности веб-приложений.



Финал

