

# Цель работы

Цель работы — приобретение практических навыков по использованию инструмента Burp Suite.

## Выполнение этапа индивидуального проекта

### Steps 1-7

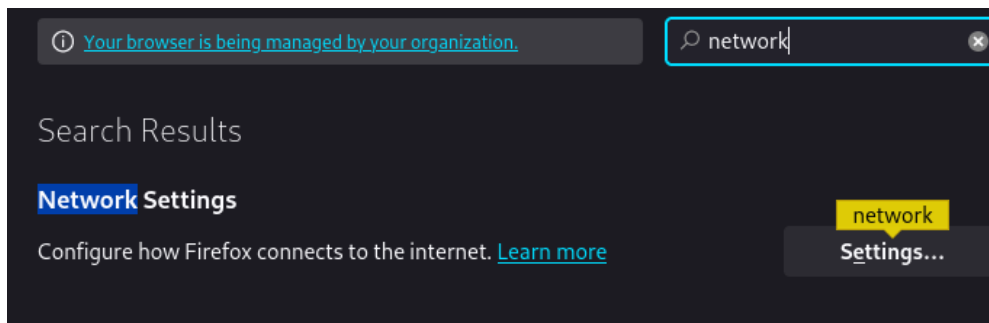
Подготовка к использованию Burp Suite:

```
(kali㉿kali)-[~]  
$ sudo service apache2 start && sudo service mysql start  
[sudo] password for kali:
```

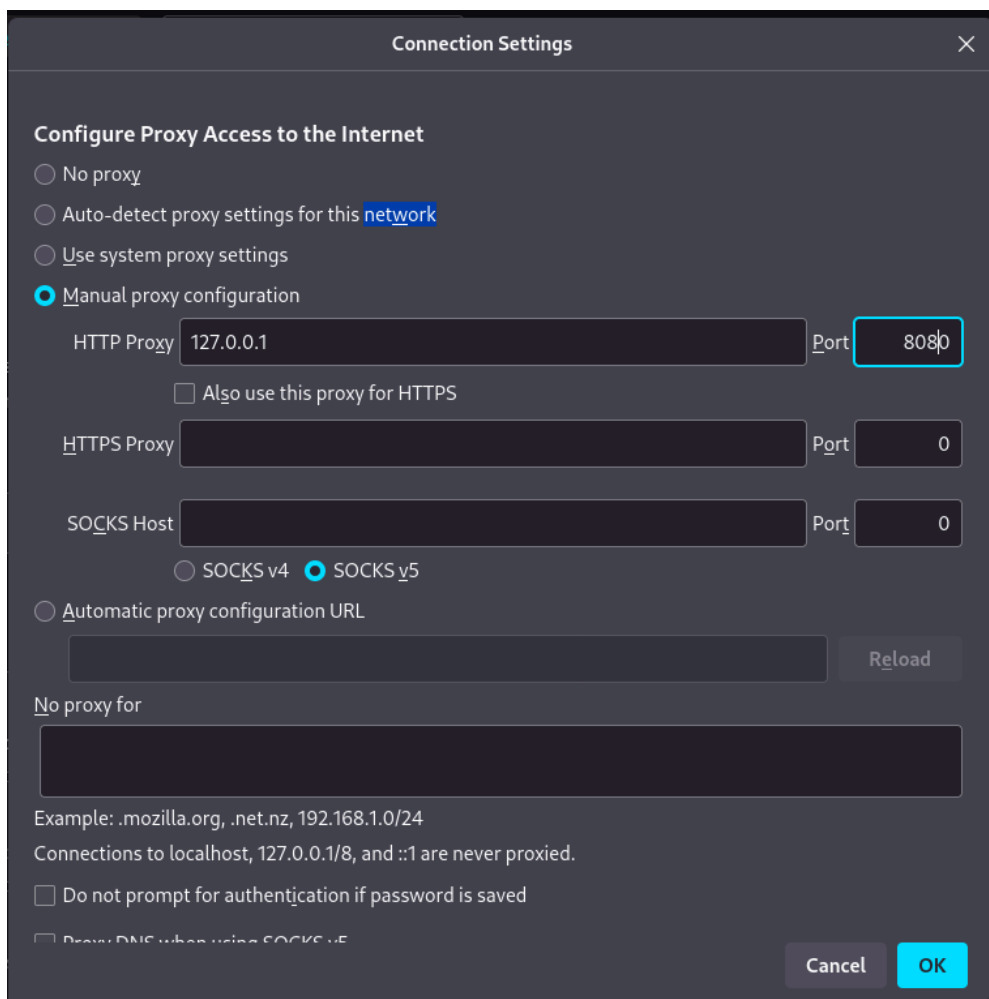
Запуск сервисов

```
(kali㉿kali)-[~]  
$ burpsuite  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
^X@sSYour JRE appears to be version 23-ea from Debian  
Burp has not been fully tested on this platform and you may experience problems.  
[]
```

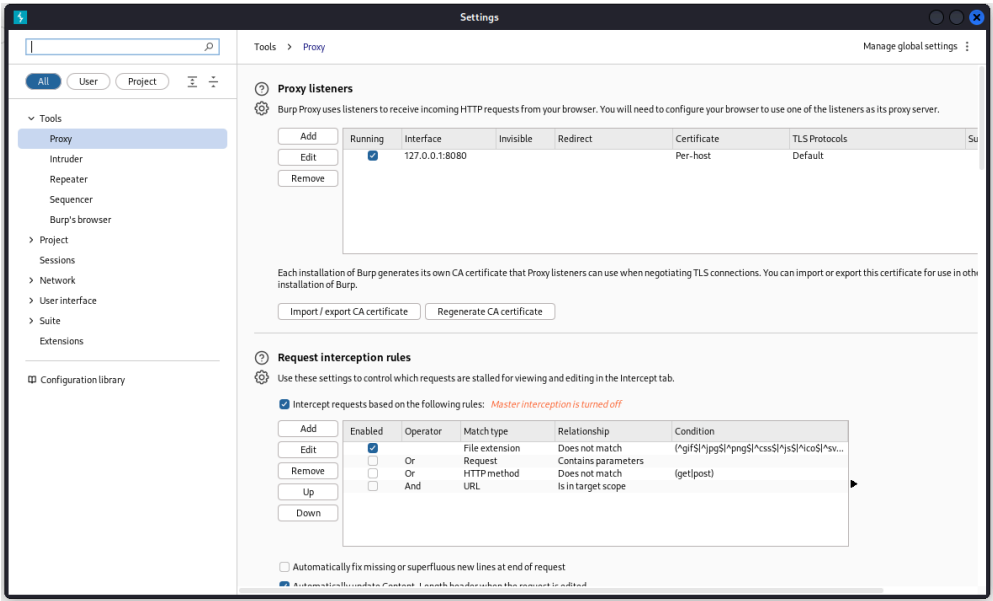
Запуск Burp Suite



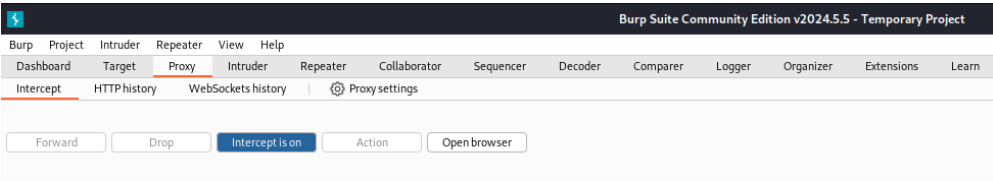
Открытие настроек браузера



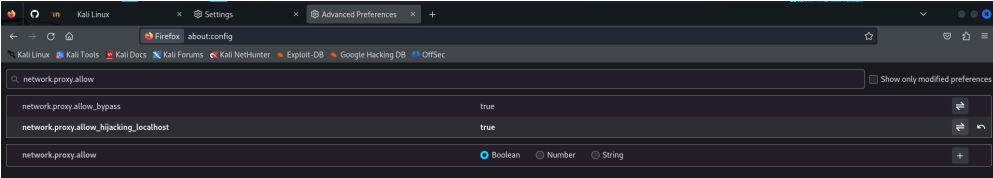
# Изменение Connection settings



## Изменение настроек проху в Burp Suite



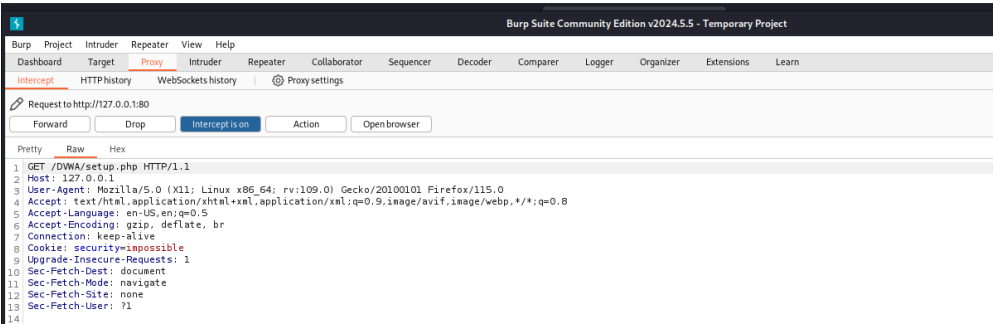
## Intercept is on



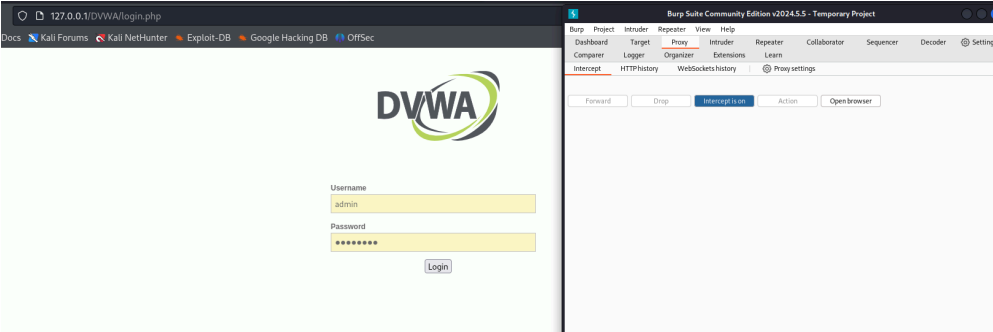
network\_allow\_hijacking\_localhost = true

# Steps 8-11

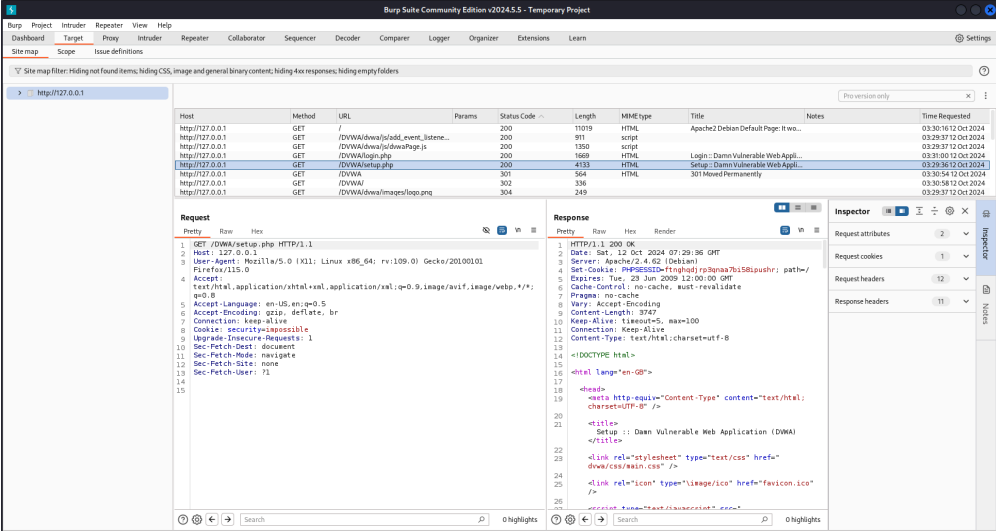
Работа с Burp Suite - захват запроса:



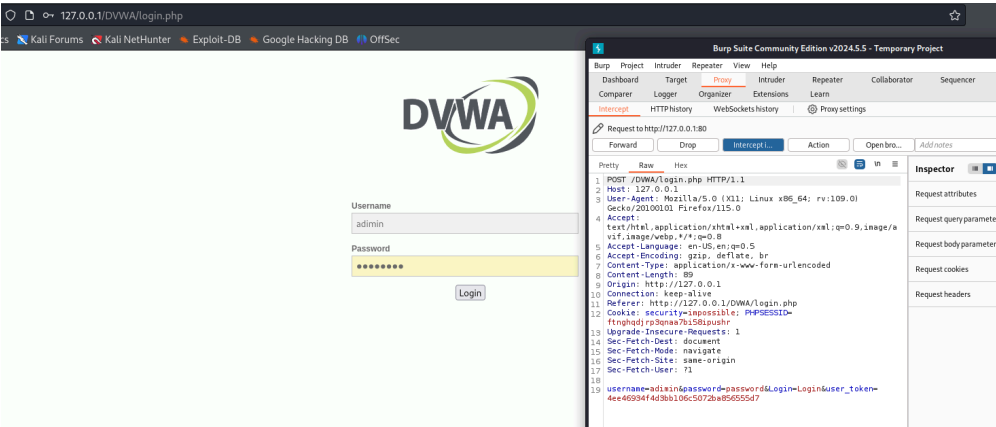
## Forward для загрузки страницы DVWA



## Страница авторизации



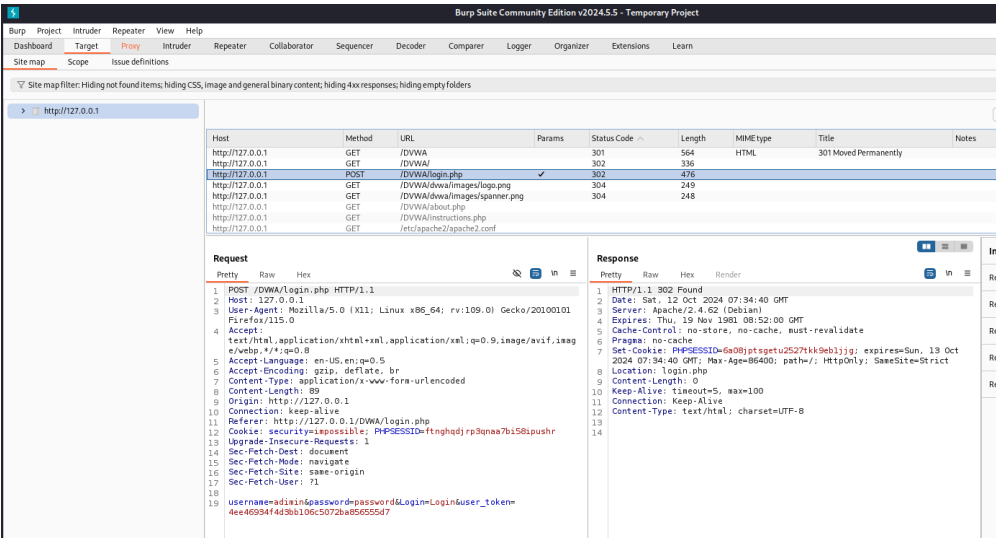
## Вкладка Target



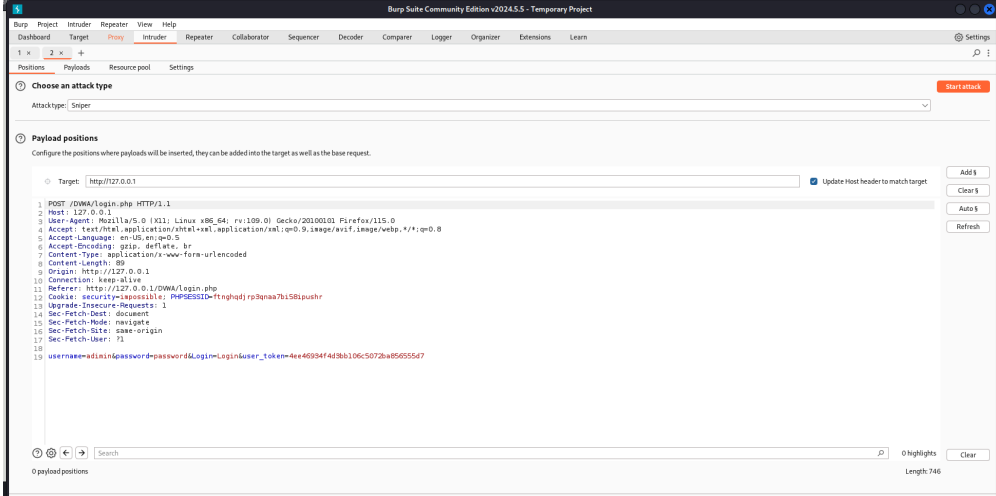
## Неверный логин

# Steps 12-17

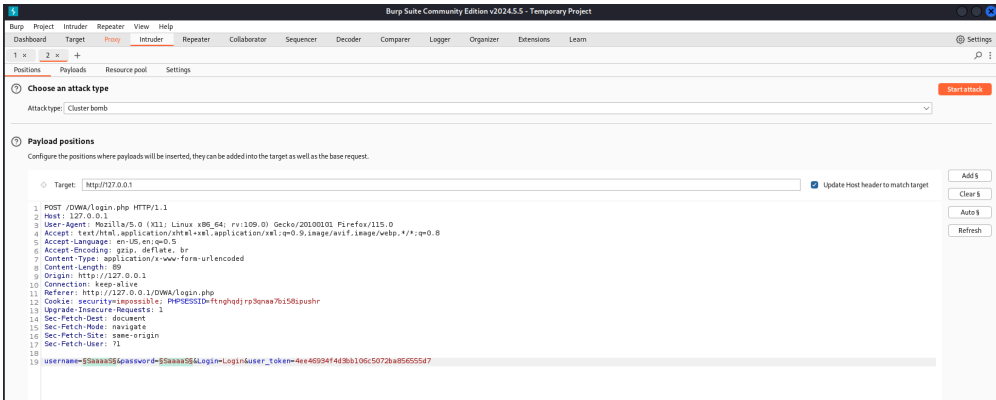
Подготовка к атаке и сама атака (подбор логина и пароля для входа в DVWA):



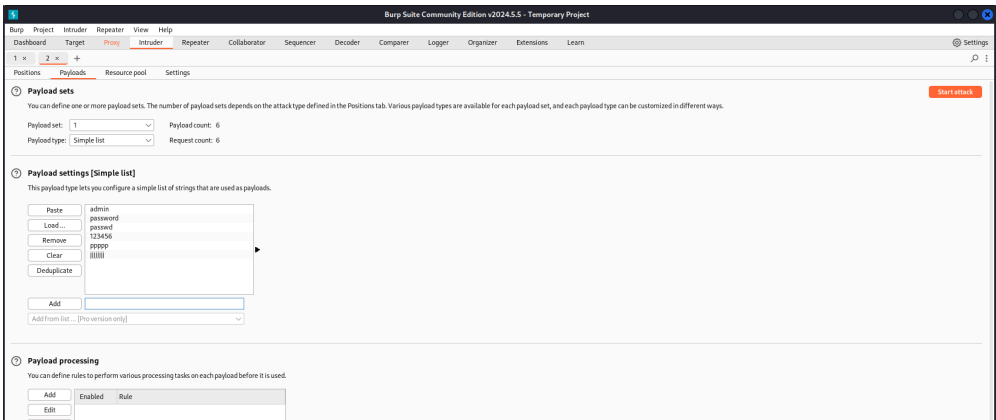
## Send to Intruder



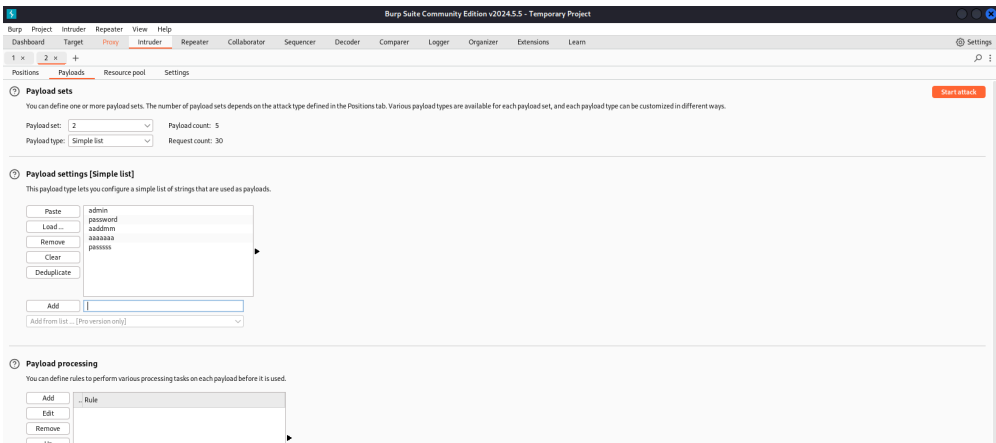
## Иintruder



## Смена типа атаки и проставление специальных символов



## Первый список подбора



## Второй список подбора

Attack Save

2. Intruder attack of http://127.0.0.1

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	16			476	
1	admin	admin	302	12			475	
2	password	admin	302	18			475	
3	password	admin	302	3			476	
4	123456	admin	302	20			476	
5	ppppp	admin	302	3			476	
6		admin	302	13			475	
7	admin	password	302	25			475	
8	password	password	302	11			476	
9	password	password	302	10			476	
10	123456	password	302	2			475	
11	ppppp	password	302	11			475	
12		password	302	3			476	
13	admin	admin	302	4			475	
14	password	admin	302	12			475	
15	password	admin	302	13			476	
16	123456	admin	302	4			475	
17	ppppp	admin	302	11			475	
18		admin	302	7			476	
19	admin	aaaaaa	302	5			475	
20	password	aaaaaa	302	7			476	
21	password	aaaaaa	302	6			476	
22	123456	aaaaaa	302	4			476	
23	ppppp	aaaaaa	302	5			476	
24		aaaaaa	302	3			476	
25	admin	passss	302	2			476	
26	password	passss	302	3			476	
27	password	passss	302	7			476	
28	123456	passss	302	2			476	
29	ppppp	passss	302	1			476	
30		passss	302	3			476	

Атака запущена

# Steps 18-23

Анализ полученных результатов атаки:

Attack Save

2. Intruder attack of http://127.0.0.1

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	16			476	
1	admin	admin	302	12			475	
2	password	admin	302	18			475	
3	password	admin	302	3			476	
4	123456	admin	302	20			476	
5	ppppp	admin	302	3			476	
6		admin	302	13			475	
7	admin	password	302	25			475	
8	password	password	302	11			476	
9	password	password	302	10			476	
10	123456	password	302	2			475	
11	ppppp	password	302	11			475	
12		password	302	3			476	
13	admin	admin	302	4			475	
14	password	admin	302	12			475	
15	password	admin	302	13			476	
16	123456	admin	302	4			475	
17	ppppp	admin	302	11			475	
18		admin	302	7			476	
19	admin	aaaaaa	302	5			475	
20	password	aaaaaa	302	7			476	
21	password	aaaaaa	302	6			476	
22	123456	aaaaaa	302	4			476	
23	ppppp	aaaaaa	302	5			476	
24		aaaaaa	302	3			476	
25	admin	passss	302	2			476	
26	password	passss	302	3			476	
27	password	passss	302	7			476	
28	123456	passss	302	2			476	
29	ppppp	passss	302	1			476	
30		passss	302	3			476	

Result 1 | Intruder attack

Previous Next

Request Response

Raw Hex Render

```
1. HTTP/1.1 302 Found
2. Date: Sat, 12 Oct 2024 07:50:08 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=28gvqrgf7s74fn46fn0u0g4e; expires=Sun, 13 Oct 2024 07:50:08 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
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
```

Смотрю ответ на пару admin-admin

Result 7 | Intruder attack

Payload1: admin

Payload2: password

Status code: 302

Length: 475

Timer: 25

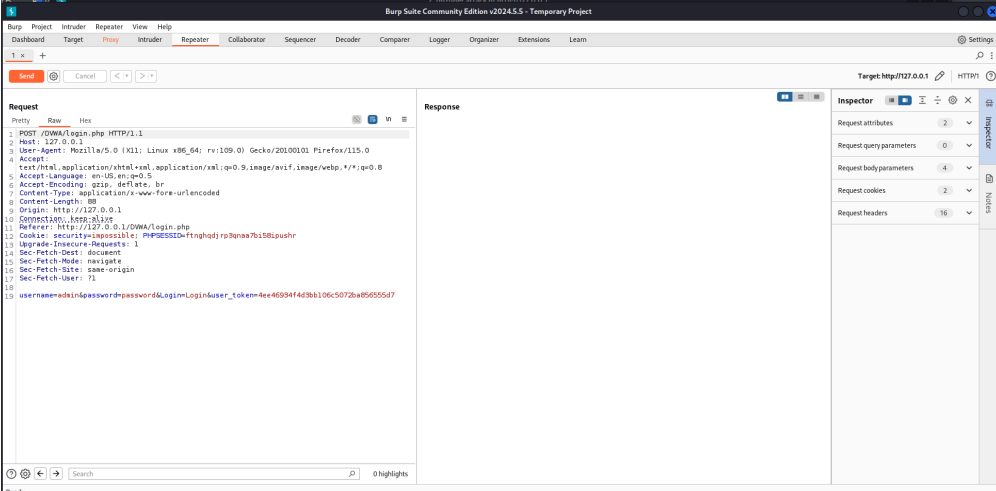
Previous Next

Request Response

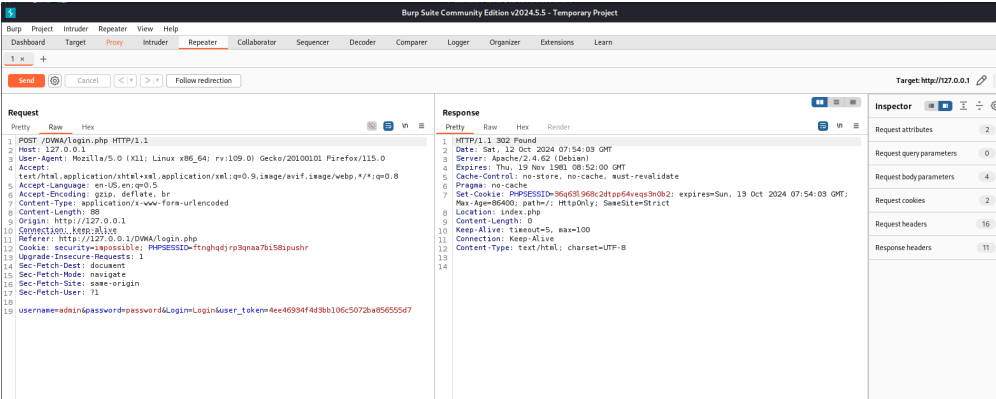
Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 07:50:09 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=rnrhfrn8i85gjopg3iaijarbdn; expires=Sun, 13 Oct 2024 07:50:09 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=97
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
```

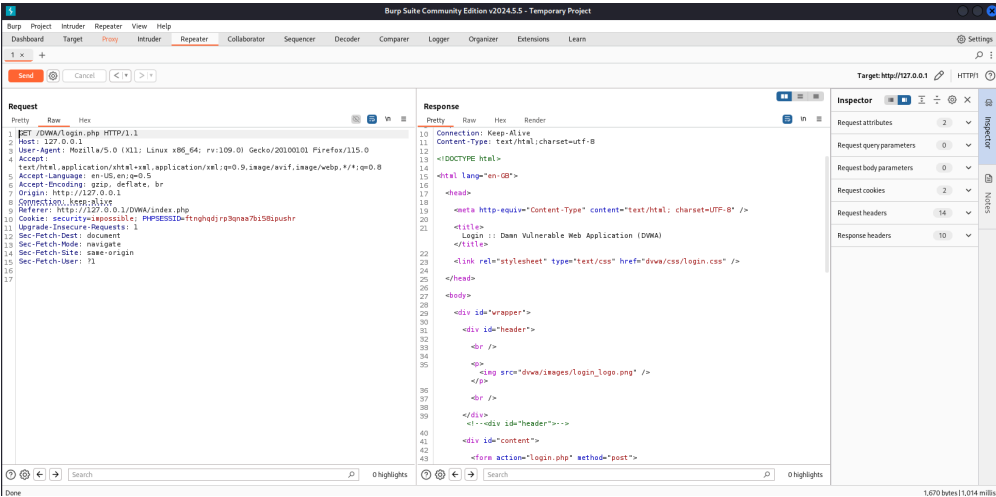
Смотрю ответ на пару admin-password



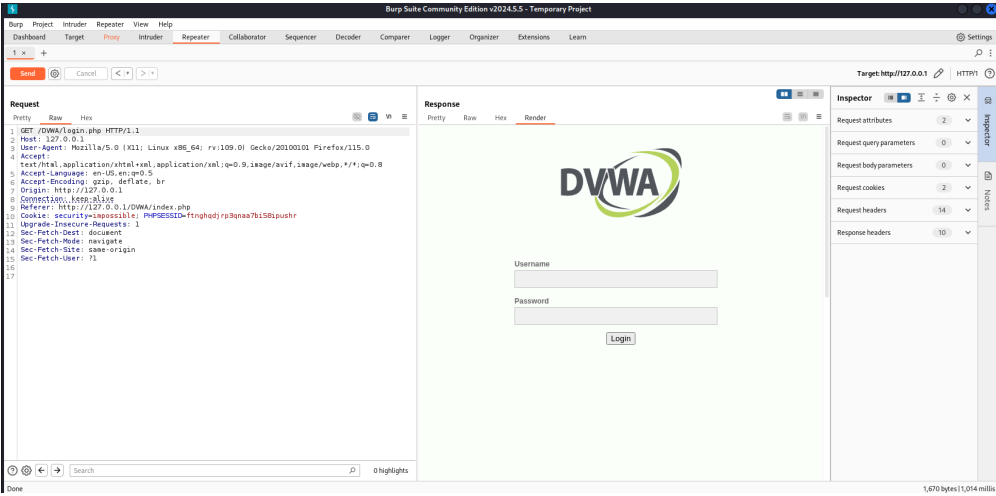
## Дополнительная проверка с Repeater



## Результат запроса



## Follow redirection result



## Follow redirection visual result

Приобрела практический навык по использованию инструмента Burp Suite.

# Библиография

- <https://www.kaznu.kz/content/files/news/folder23191/%D0%9B%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%2012%20rus.pdf>
- <https://esystem.rudn.ru/mod/page/view.php?id=1140635>

Спасибо за внимание!