

# Презентация по выполнению индивидуального проекта №5

Основы информационной безопасности

---

Дворкина Е. В

09 мая 2024

Российский университет дружбы народов, Москва, Россия

# Информация

---

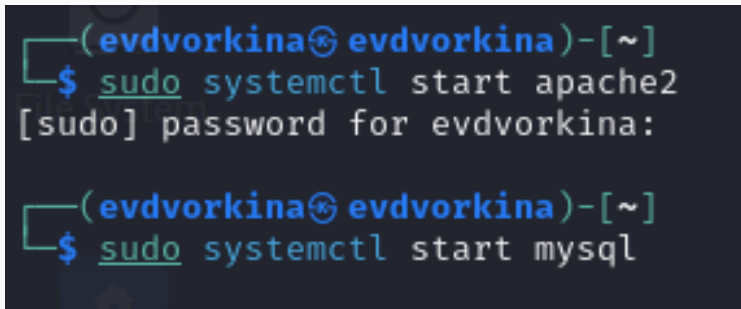
- Дворкина Ева Владимировна
- студентка группы НКАбд-01-22
- Российский университет дружбы народов
- <https://vk.com/yuri.kamori>



Научиться использовать Burp Suite.

## Выполнение лабораторной работы

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

A terminal window with a dark background. The prompt is '(evdvorkina@evdvorkina)-[~]'. The first command entered is '\$ sudo systemctl start apache2', followed by the password prompt '[sudo] password for evdvorkina:'. The second command entered is '\$ sudo systemctl start mysql'.

```
(evdvorkina@evdvorkina)-[~]  
$ sudo systemctl start apache2  
[sudo] password for evdvorkina:  
  
(evdvorkina@evdvorkina)-[~]  
$ sudo systemctl start mysql
```

Рис. 1: Запуск локального сервера

## Запускаю инструмент Burp Suite

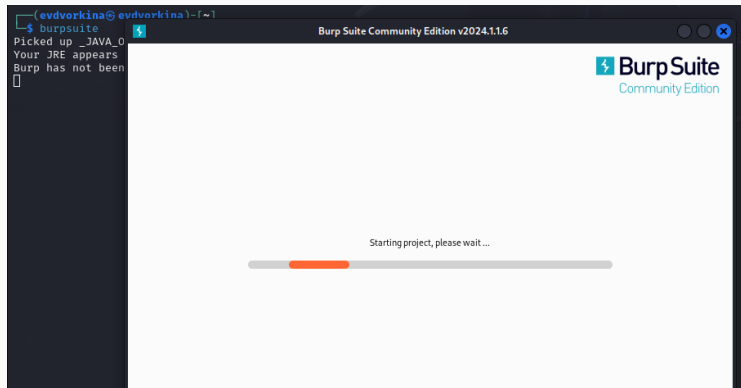
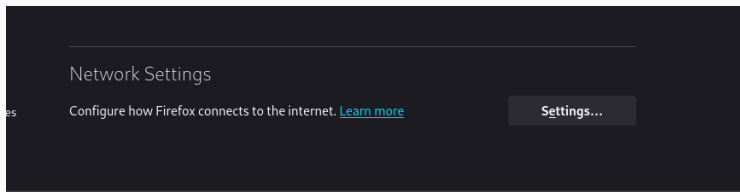


Рис. 2: Запуск приложения

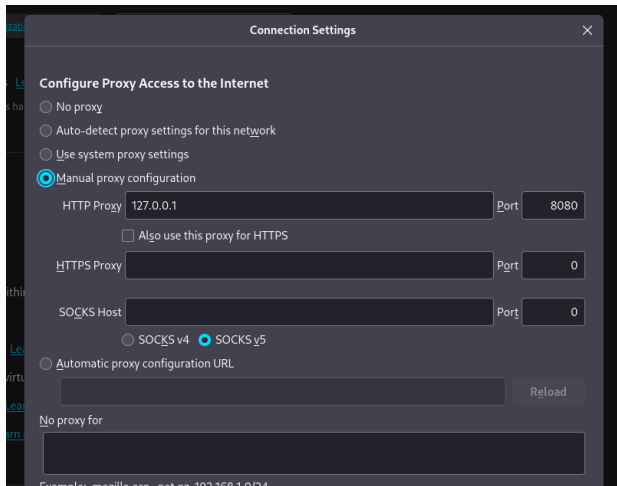
Открываю сетевые настройки браузера, для подготовке к работе



**Рис. 3:** Сетевые настройки браузера

# Выполнение лабораторной работы

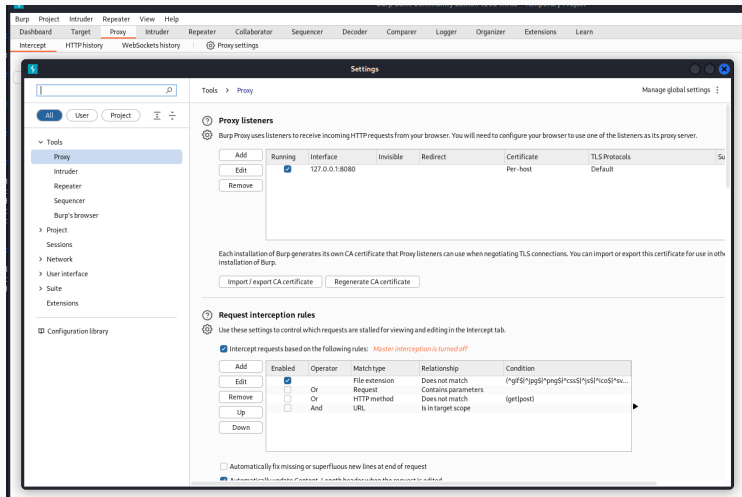
Изменение настроек сервера для работы с проху и захватом данных с помощью Burp Suite





# Выполнение лабораторной работы

## Изменяю настройки Proxu инструмента Burp Suite для дальнейшей работы



Во вкладке Proxy устанавливаю “Intercept is on”

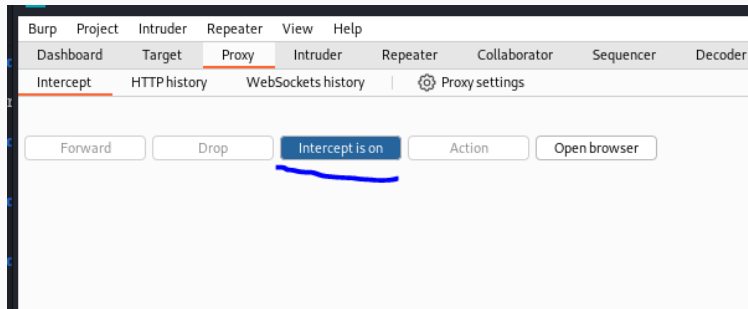


Рис. 6: Настройки Proxy

# Выполнение лабораторной работы

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network.allow_hijacking_localhost` на `true`

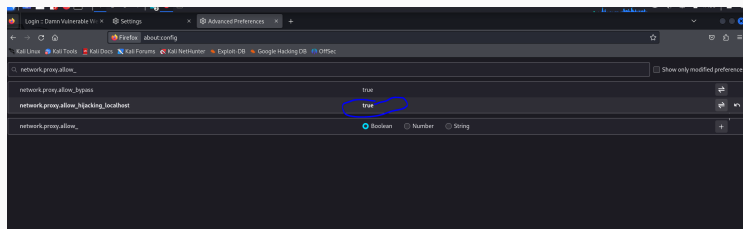


Рис. 7: Настройки параметров

# Выполнение лабораторной работы

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

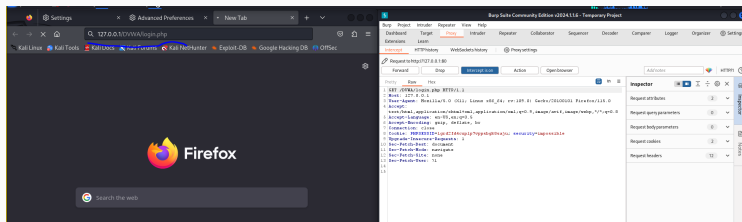


Рис. 8: Получаемые запросы сервера

# Выполнение лабораторной работы

Загрузилась страница авторизации, текст запроса поменялся

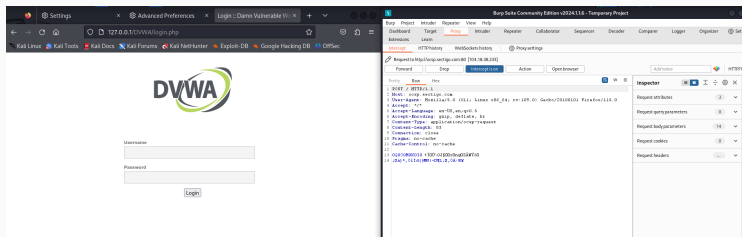


Рис. 9: Страница авторизации

# Выполнение лабораторной работы

## История запросов хранится во вкладке Target

The screenshot shows the Burp Suite Community Edition v2024.1.1.6 interface. The 'Target' tab is active, displaying a list of requests. The first request is a GET request to `/DVWA/login.php` with a status code of 200. The second request is a GET request to `/DVWA/dwa/images...`.

Below the list, the 'Request' and 'Response' tabs are visible. The 'Request' tab is selected, showing the raw request data in a text editor. The request is a GET request to `/DVWA/login.php` with the following headers:

```
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=lgrdCfd4cuplp7vpysbgk0saju; 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
15
```

The 'Inspector' panel on the right shows the request attributes, request cookies, request headers, and response headers.

# Выполнение лабораторной работы

Попробуем ввести неправильные, случайные данные в веб-приложении и нажмем Login. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода

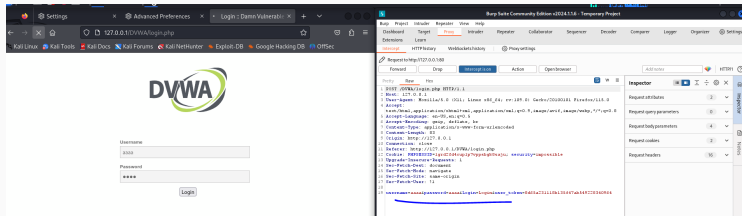
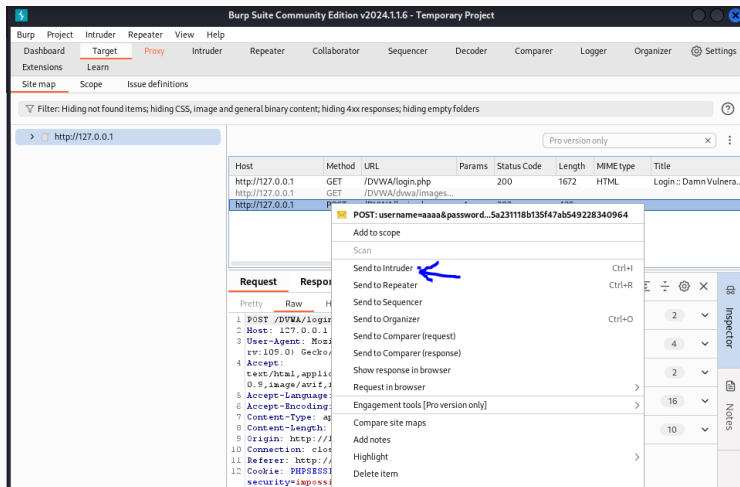


Рис. 11: Ввод случайных данных

# Выполнение лабораторной работы

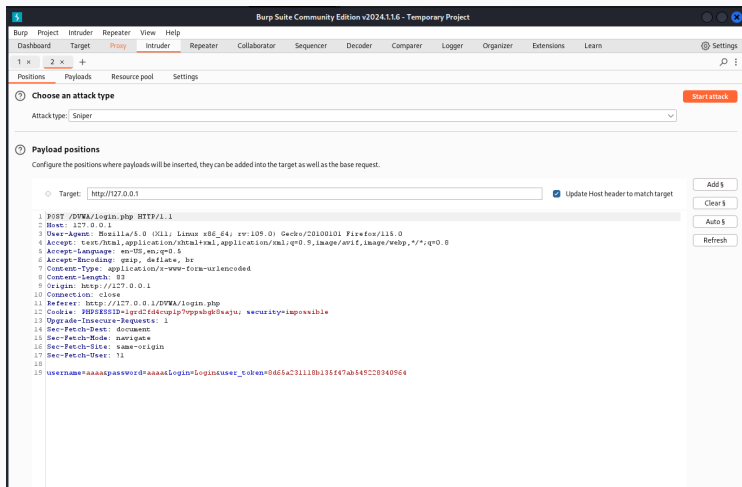
Этот запрос так же можно найти во вкладке Target, там же жмем правой кнопкой мыши на хост нужного запроса, и далее нажимаем “Send to Intruder”





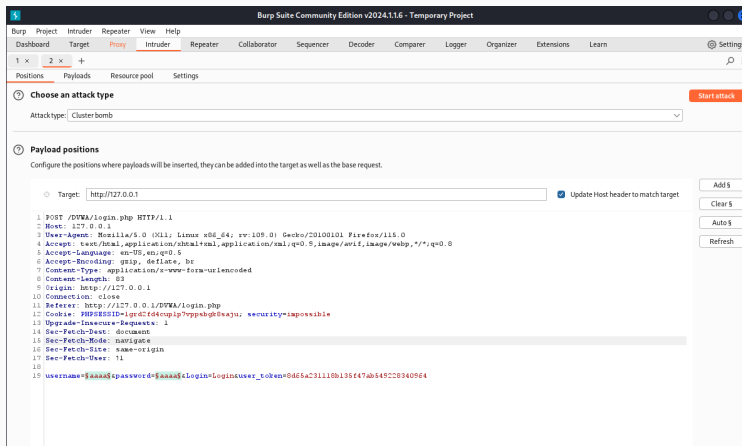
# Выполнение лабораторной работы

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос



# Выполнение лабораторной работы

Изменяем значение типа атаки на Cluster bomb и проставляем специальные символы у тех данных в форме для ввода, которые будем пробивать, то есть у имени пользователя и пароля



# Выполнение лабораторной работы

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting

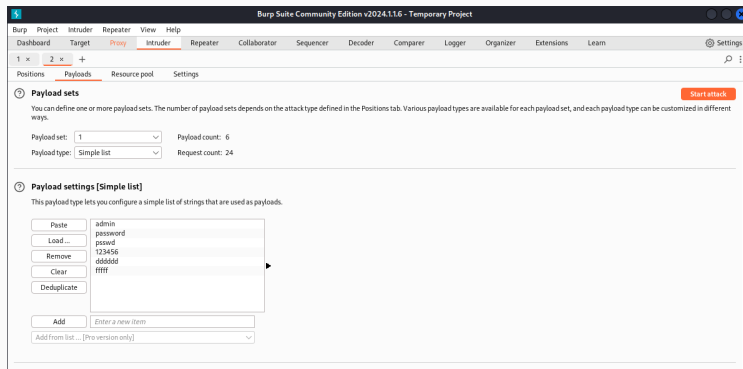


Рис. 15: Первый Simple list

# Выполнение лабораторной работы

Переключаемся на второй список и добавляем значения в него. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль

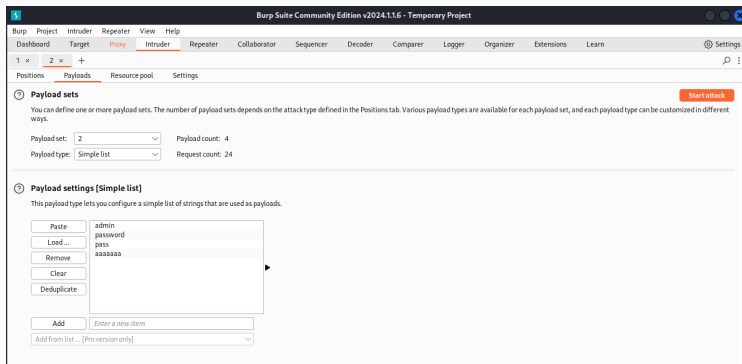
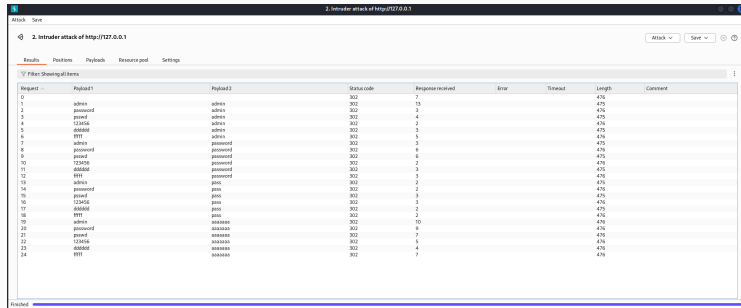


Рис. 16: Второй Simple list

# Выполнение лабораторной работы

## Запускаю атаку и начинаю подбор



Attack Save

2. Intruder attack of http://127.0.0.1

Attack ▾ Save ▾

Results Positions Payloads Resource pool Settings

Filter Showing all items

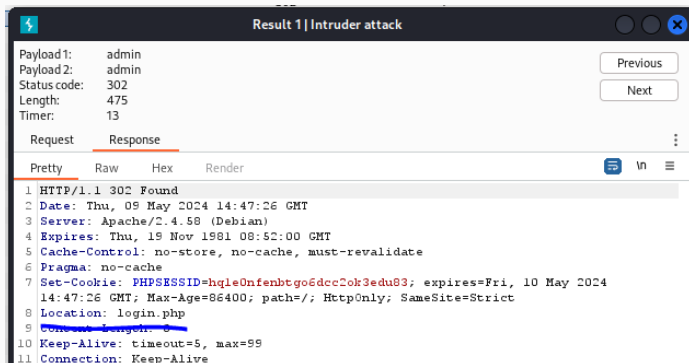
Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			476	
1	admin	admin	302	13			475	
2	password	password	302	3			476	
3	passwd	admin	302	4			475	
4	123456	admin	302	2			476	
5	666666	admin	302	3			475	
6	HHH	admin	302	5			476	
7	admin	password	302	3			475	
8	password	password	302	6			476	
9	passwd	password	302	6			475	
10	123456	password	302	2			476	
11	666666	password	302	3			475	
12	HHH	password	302	3			476	
13	admin	pass	302	2			475	
14	password	pass	302	2			476	
15	passwd	pass	302	3			475	
16	123456	pass	302	3			476	
17	666666	pass	302	2			475	
18	HHH	pass	302	2			476	
19	admin	aaaaaa	302	10			476	
20	password	aaaaaa	302	9			476	
21	passwd	aaaaaa	302	7			476	
22	123456	aaaaaa	302	5			476	
23	666666	aaaaaa	302	4			476	
24	HHH	aaaaaa	302	7			476	

Finished

Рис. 17: Запуск атаки

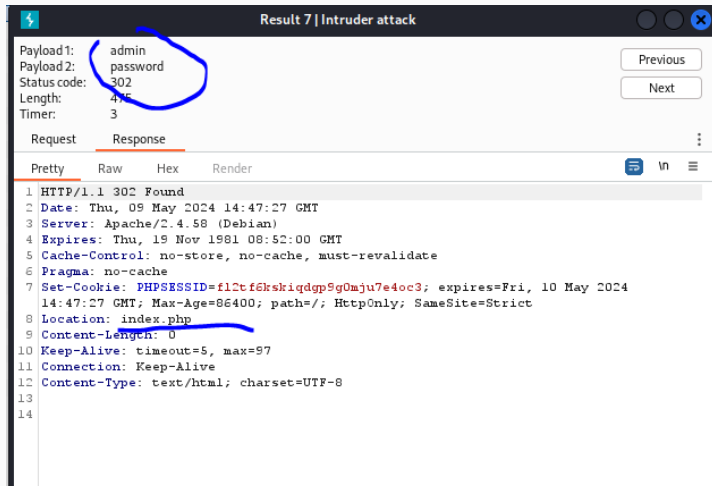
# Выполнение лабораторной работы

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит



# Выполнение лабораторной работы

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной



# Выполнение лабораторной работы

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater”

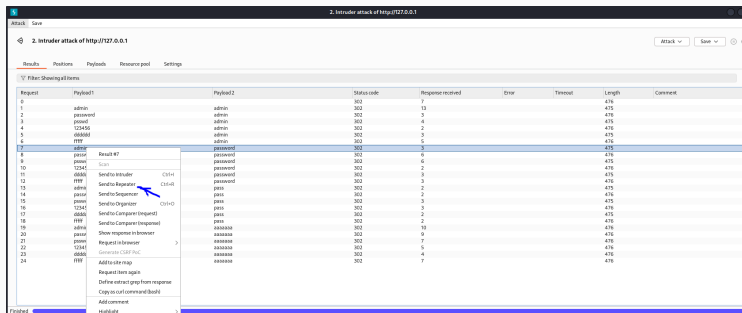
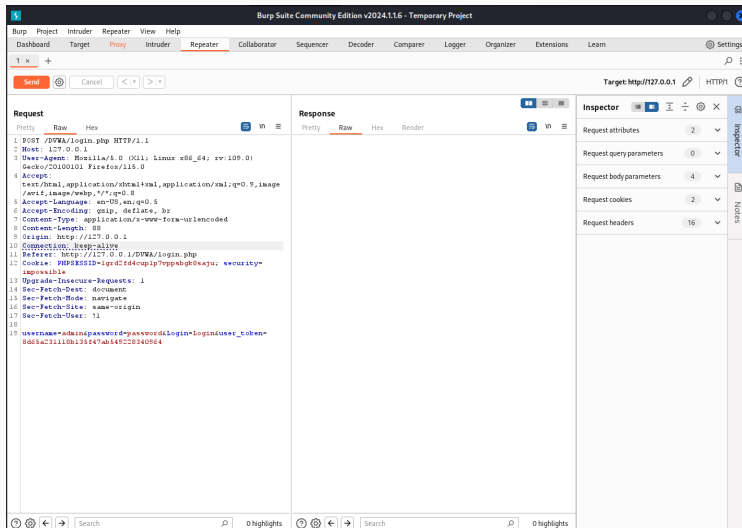


Рис. 20: Дополнительная проверка результата



# Выполнение лабораторной работы

## Переходим во вкладку “Repeater”



# Выполнение лабораторной работы

Нажимаем “send”, получаем в Response в результат перенаправление на index.php

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Send' button is highlighted in red. The 'Request' pane on the left shows the raw HTTP request, and the 'Response' pane on the right shows the raw HTTP response. The 'Inspector' pane on the far right shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.

**Request**

```
1 POST /DUWA/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/DUWA/login.php
12 Cookie: PHPSESSID=1grdZt44cuplp7oppabgk8eaju; security=
  impossible
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=admin&password=password&login=loginuser_token=
  8d6fa23118b135f47ab5492c8340964
```

**Response**

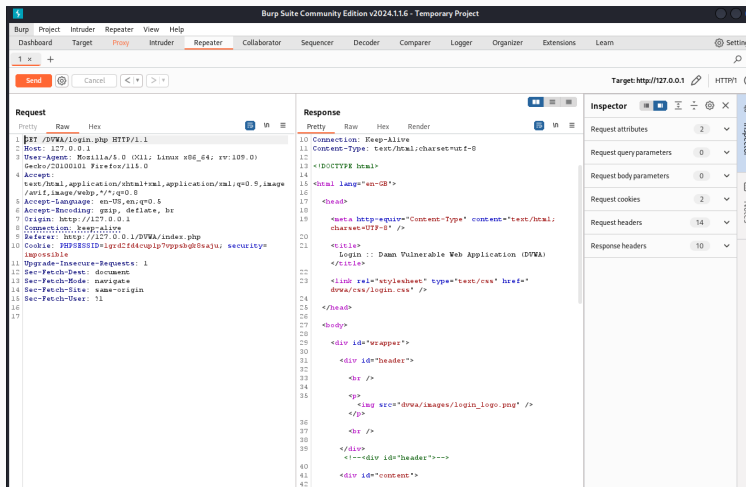
```
1 HTTP/1.1 302 Found
2 Date: Thu, 09 May 2024 14:51:42 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=do7q7luwnslu7vb7mc7b856c9;
  expires=Fri, 10 May 2024 14:51:42 GMT; Max-Age=86400;
  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 query parameters: 0
- Request body parameters: 4
- Request cookies: 2
- Request headers: 16
- Response headers: 11

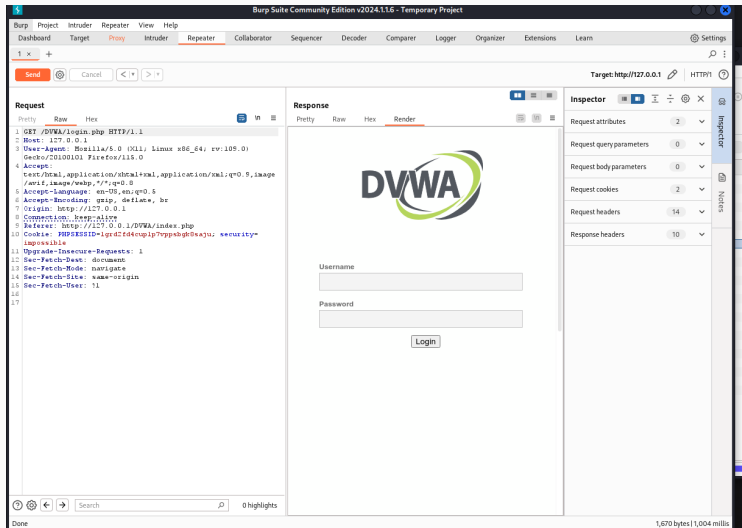
# Выполнение лабораторной работы

После нажатия на Follow redirection, получим неcompiled html код в окне Response



# Выполнение лабораторной работы

Далее в подокне Render получим то, как выглядит полученная страница



При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

...