

Отчет по выполнению индивидуального проекта. Этап №5

Основы информационной безопасности

Кабанова Варвара, НПМбд02-21

Содержание

Цель работы	1
Теоретическое введение	1
Выполнение лабораторной работы	1
Выводы.....	12

Цель работы

Научиться использовать Burp Suite.

Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений. [@parasram].

Выполнение лабораторной работы

Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. [-@fig:001]).

```

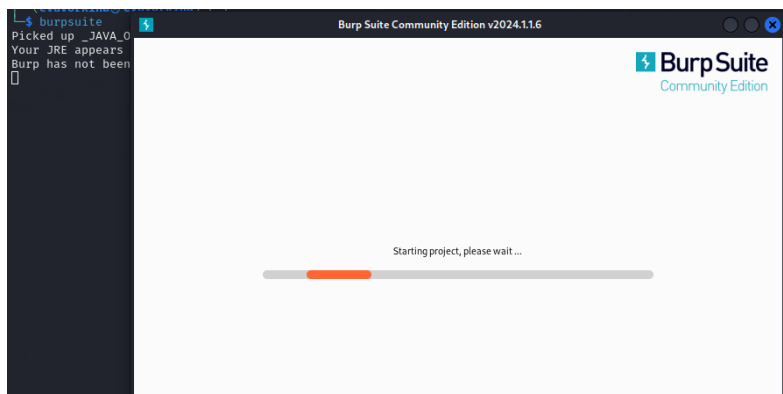
(kali@kali)-[~]
$ sudo systemctl start apache2
[sudo] password for kali:

(kali@kali)-[~]
$ sudo systemctl start mysql

```

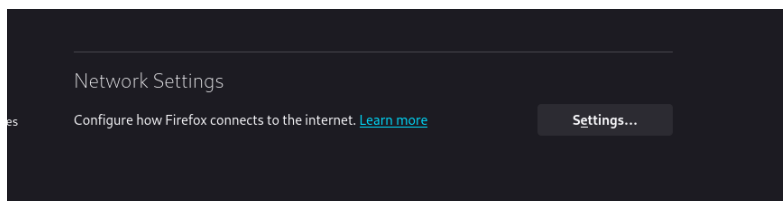
Запуск локального сервера

Запускаю инструмент Burp Suite (рис. [-@fig:002]).



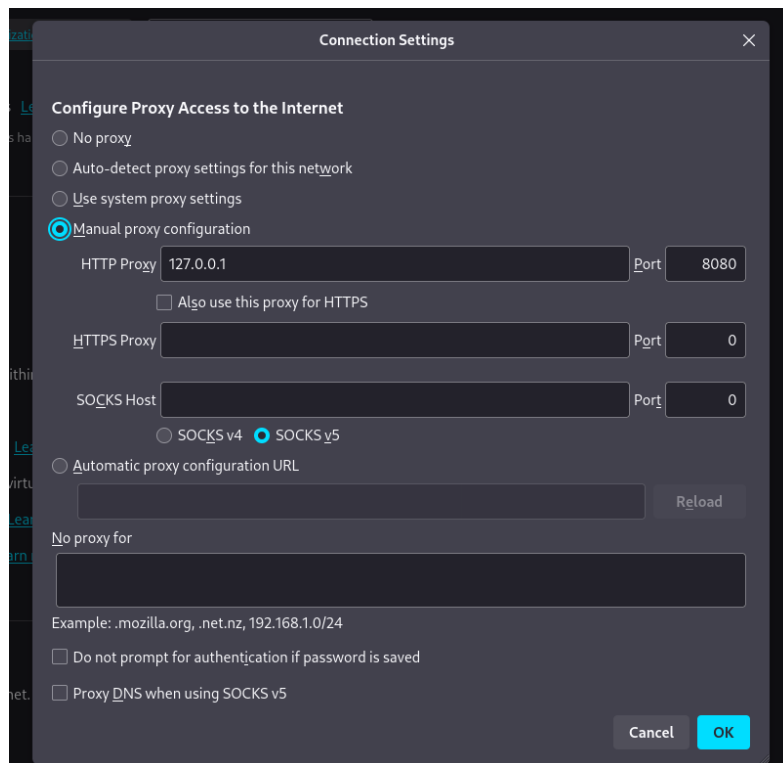
Запуск приложения

Открываю сетевые настройки браузера, для подготовке к работе (рис. [-@fig:003]).



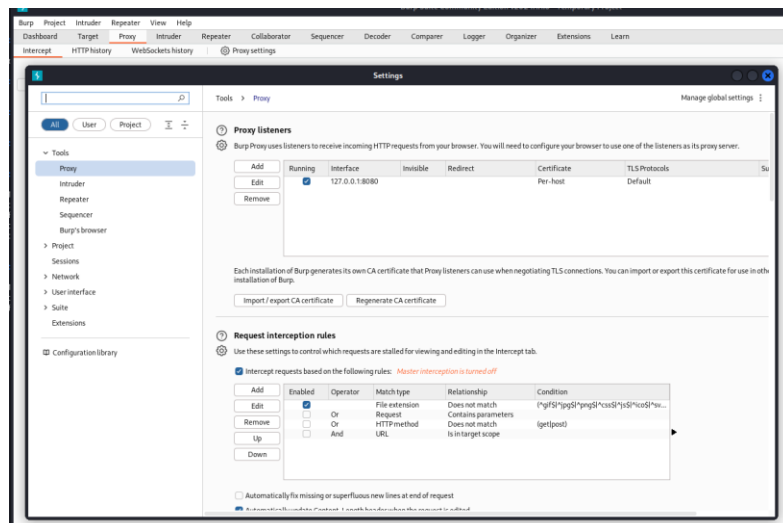
Сетевые настройки браузера

Изменение настроек сервера для работы с проху и захватом данных с помощью Burp Suite (рис. [-@fig:004]).



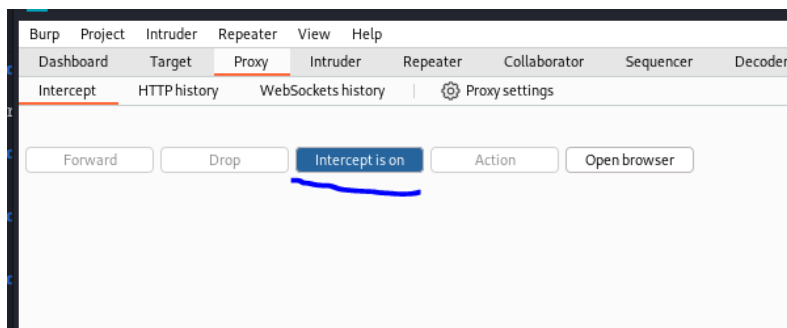
Настройка сервера

Изменяю настройки Proxy инструмента Burp Suite для дальнейшей работы (рис. [-@fig:005]).



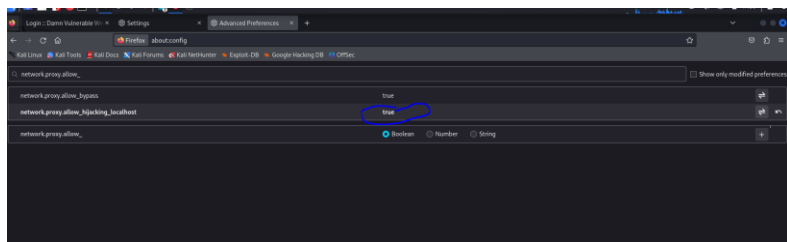
Настройка Burp Suite

Во вкладке Proxy устанавливаю "Intercept is on" (рис. [-@fig:006]).



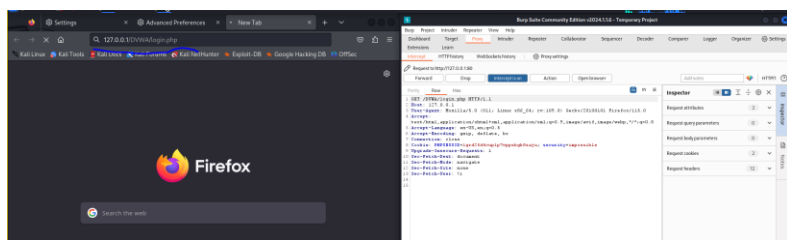
Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_loacalhost` на `true` (рис. [-@fig:007]).



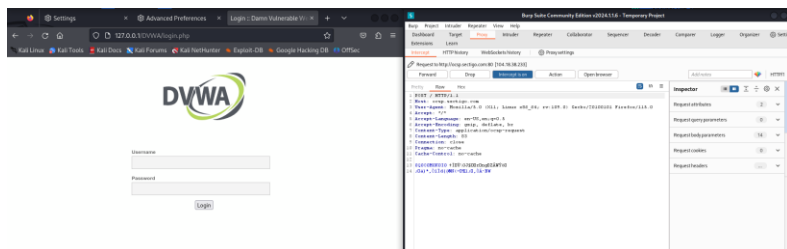
Настройка параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем "Forward", чтобы загрузить страницу (рис. [-@fig:008]).



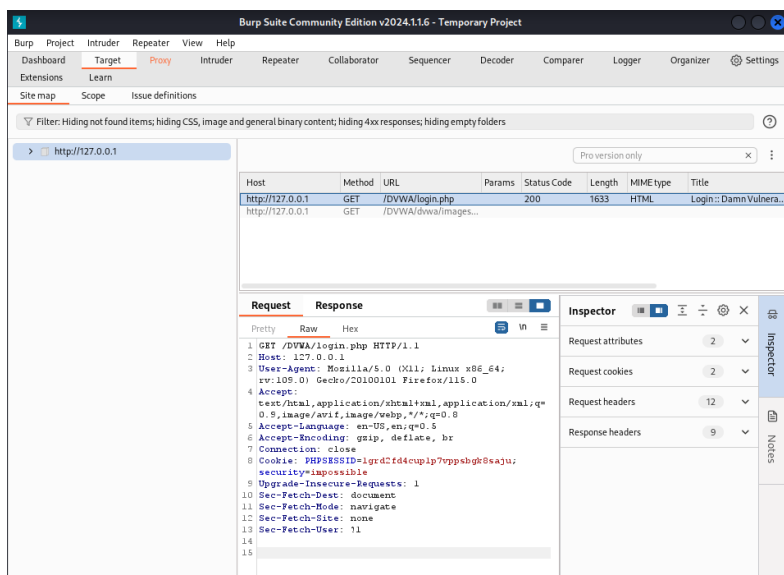
Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:009]).



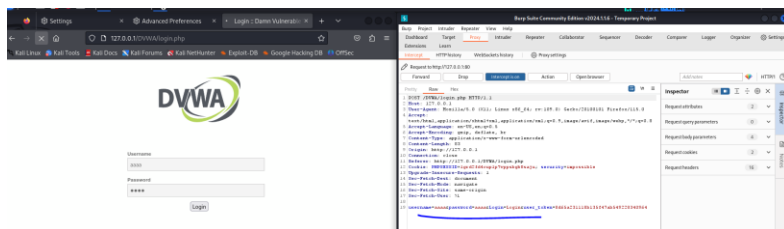
Страница авторизации

История запросов хранится во вкладке Target (рис. [-@fig:010]).



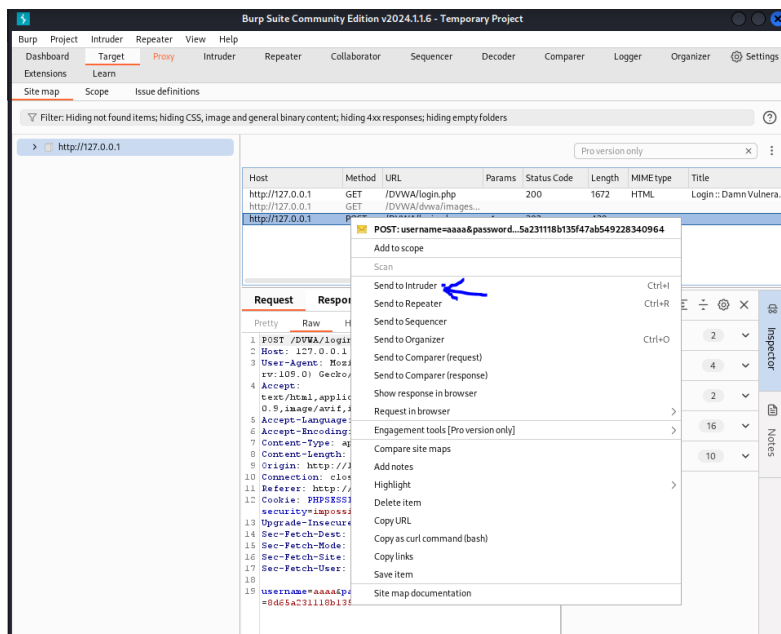
История запросов

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. [-@fig:011]).



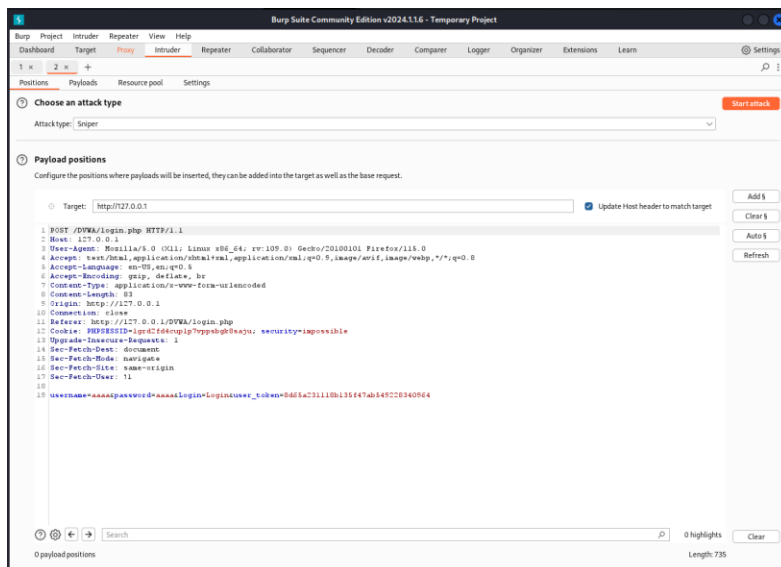
Ввод случайных данных

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” (рис. [-@fig:012]).



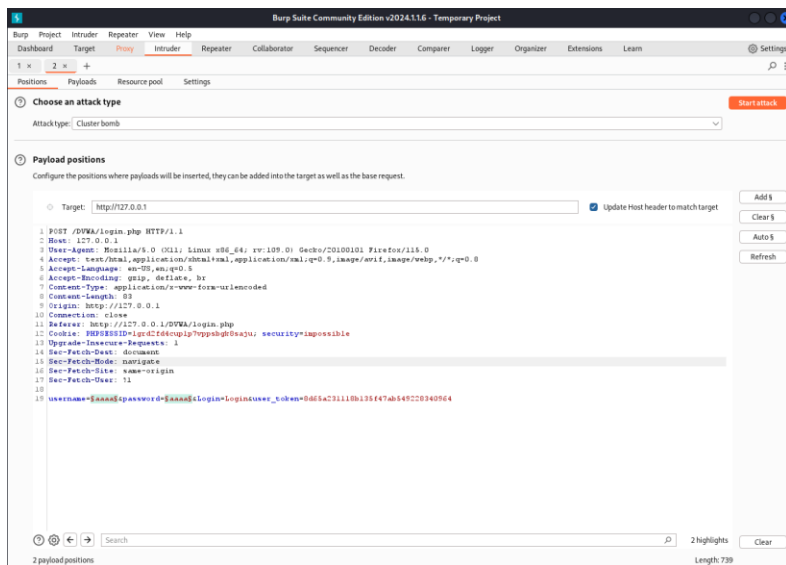
POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:013]).



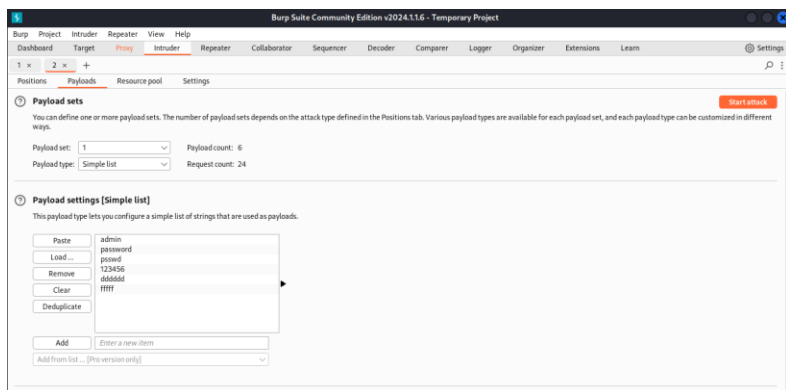
Вкладка Intruder

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 (рис. [-@fig:014]).



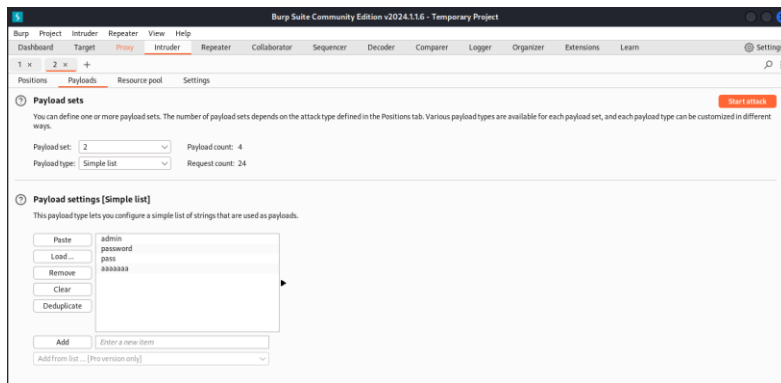
Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. [-@fig:015]).



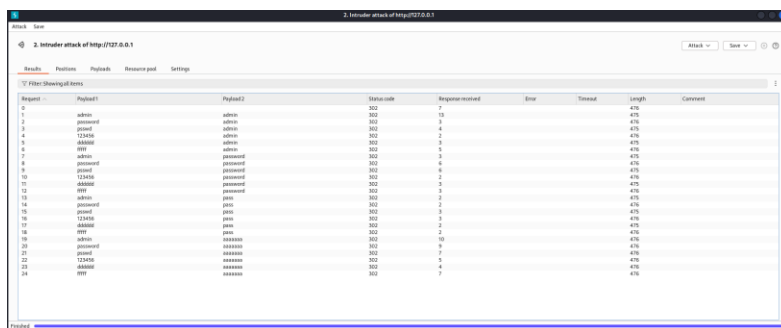
Первый Simple list

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. [-@fig:016]).



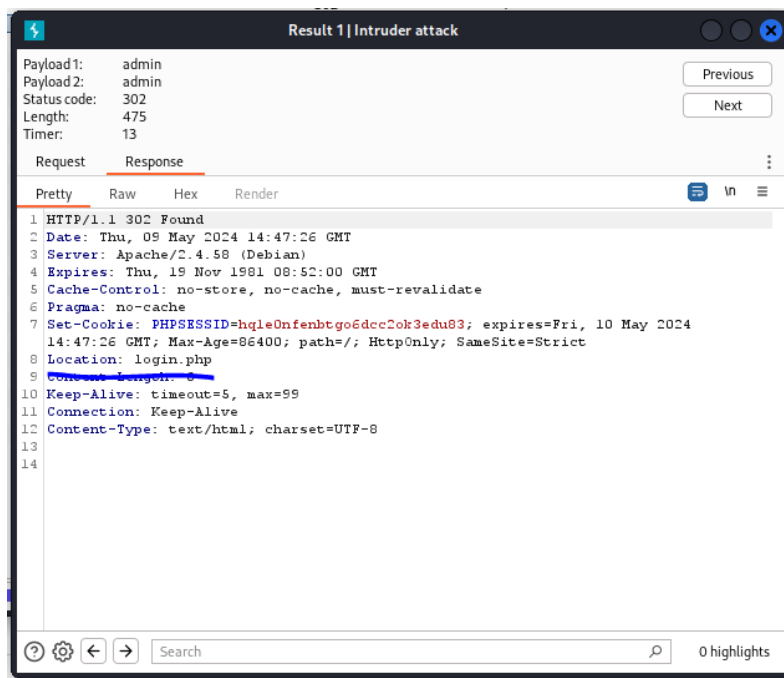
Второй Simple list

Запускаю атаку и начинаю подбор (рис. [-@fig:017]).



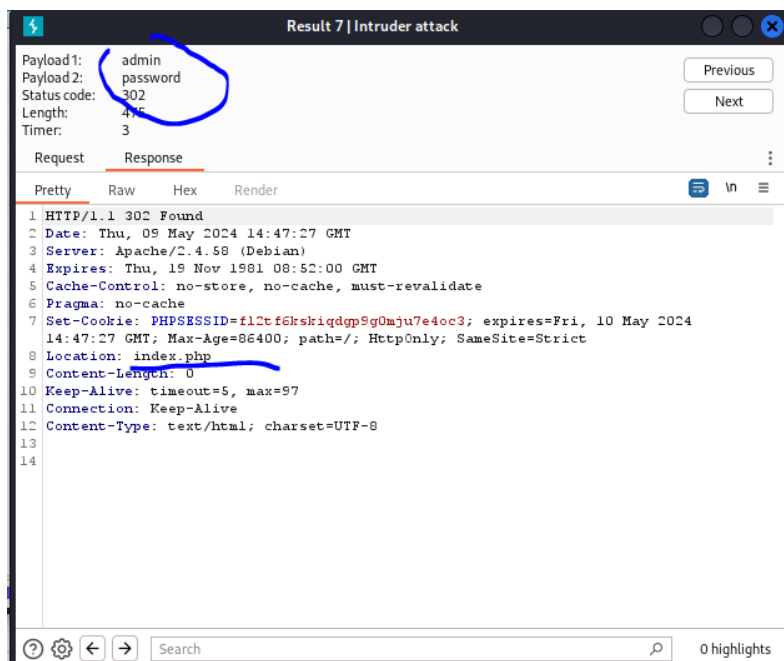
Запуск атаки

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 (рис. [-@fig:018]).



Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [-@fig:019]).



Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем "Send to Repeater" (рис. [-@fig:020]).

Request	Payload1	Payload2	Statuscode	Response received	Error	Timeout	Length	Comment
1	admin	admin	302	1			476	
2	password	password	302	10			476	
3	password	admin	302	3			476	
4	password	admin	302	4			476	
5	password	admin	302	3			476	
6	password	admin	302	5			476	
7	password	password	302	3			476	
8	password	Result:07	302	6			476	
9	password	Sum	302	6			476	
10	123456	password	302	2			476	
11	Send to Repeater	Send to Repeater	302	3			476	
12	Send to Repeater	Send to Repeater	302	3			476	
13	Send to Repeater	Send to Repeater	302	3			476	
14	Send to Repeater	Send to Repeater	302	2			476	
15	Send to Repeater	Send to Repeater	302	3			476	
16	Send to Repeater	Send to Repeater	302	3			476	
17	Send to Repeater	Send to Repeater	302	2			476	
18	Send to Repeater	Send to Repeater	302	10			476	
19	Send to Repeater	Send to Repeater	302	6			476	
20	Send to Repeater	Send to Repeater	302	7			476	
21	Send to Repeater	Send to Repeater	302	6			476	
22	Send to Repeater	Send to Repeater	302	7			476	
23	Send to Repeater	Send to Repeater	302	7			476	
24	Send to Repeater	Send to Repeater	302	7			476	

Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. [-@fig:021]).

Target: http://127.0.0.1

Request:

```

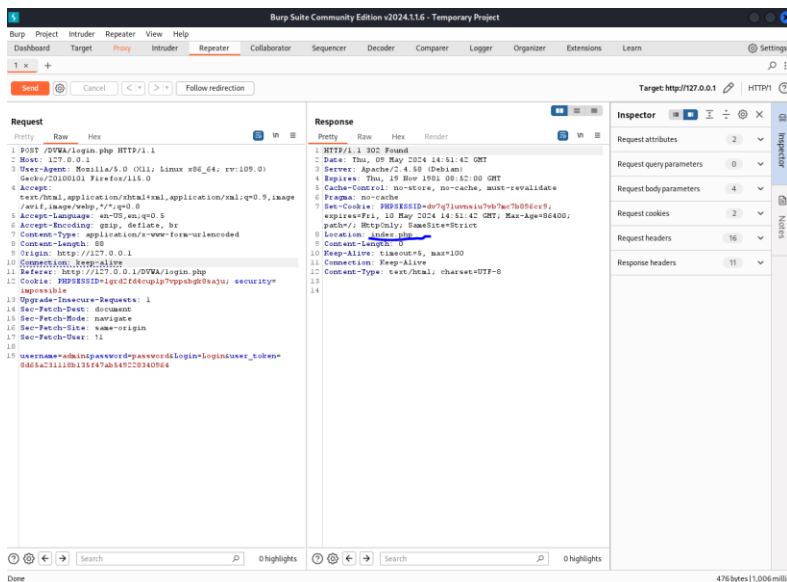
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 80
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: PHPSESSID=pe4Cf6d6wip7p9pshg8tazj; 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_admin=5d65a7311b0135467a0449c23340564

```

Response:

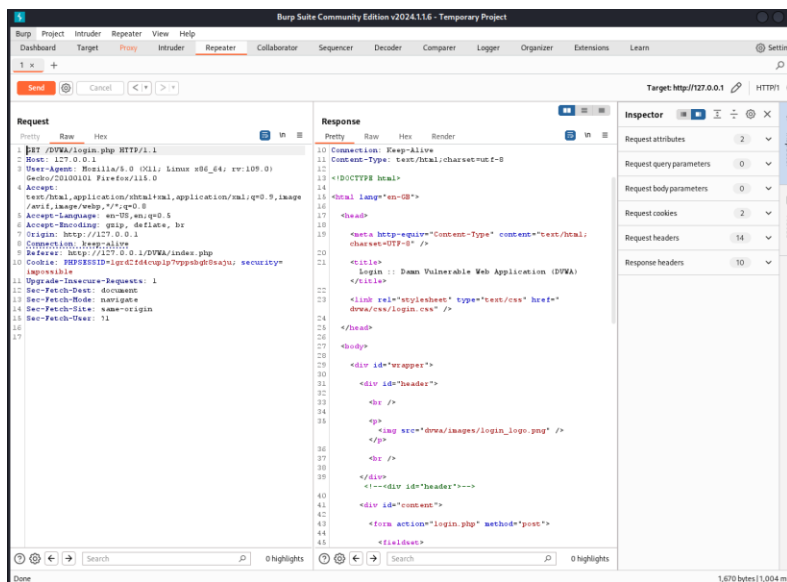
Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. [-@fig:022]).



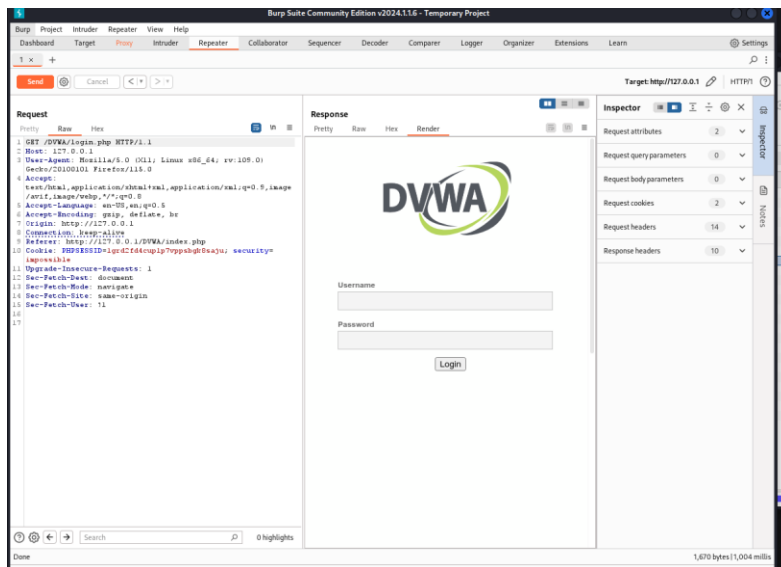
Окно Response

После нажатия на Follow redirection, получим неcompiled html код в окне Response (рис. [-@fig:023]).



Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [-@fig:024]).



Полученная страница

Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.