

Отчет по выполнению индивидуального проекта. Этап №5

Основы информационной безопасности

Ничипорова Е.Д.

Содержание

Цель работы	1
Теоретическое введение	1
Выполнение лабораторной работы	1
Выводы.....	11
Список литературы.....	11

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

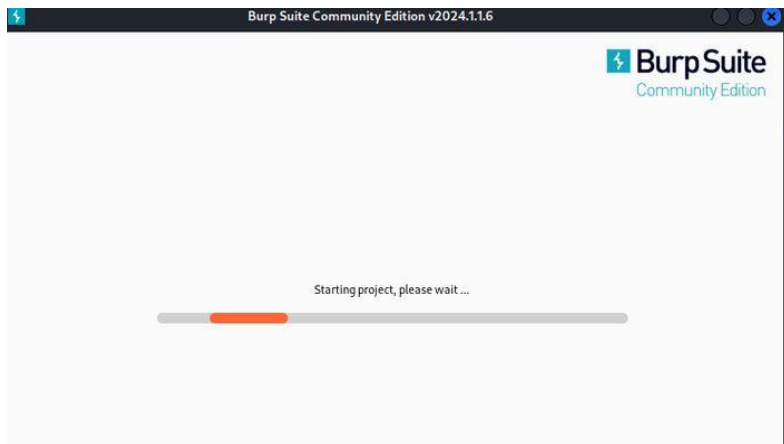
Запускаю локальный сервер, на котором открою веб-приложение DVWA для тестирования инструмента Burp Suite (рис. [-@fig:001]).

```
(kali@kali)-[~/Downloads]
$ sudo systemctl start apache2

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

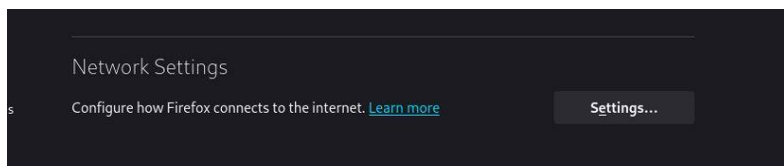
Запуск локального сервера

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



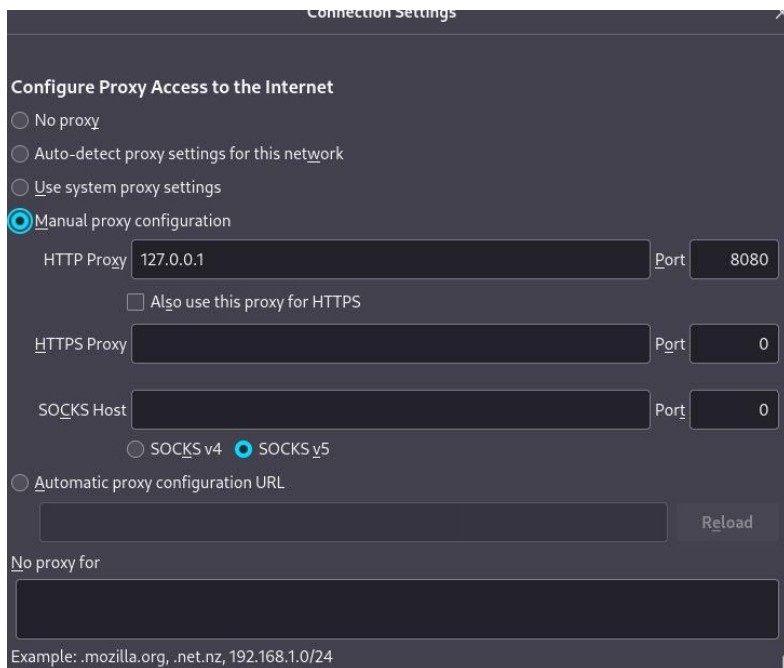
Запуск приложения

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



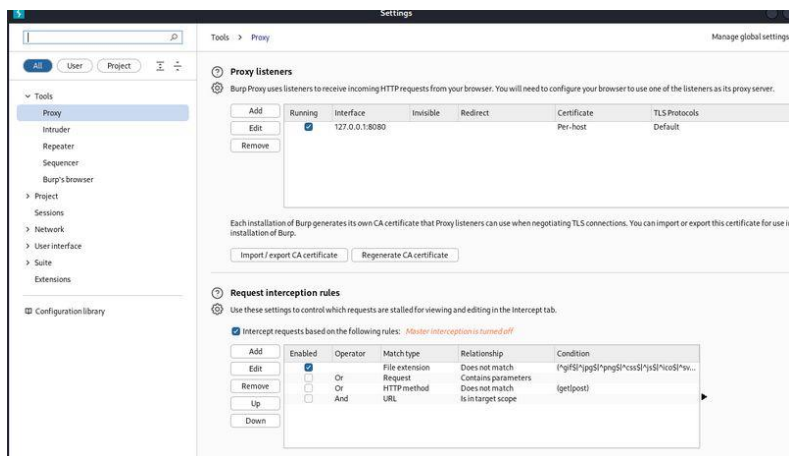
Сетевые настройки браузера

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



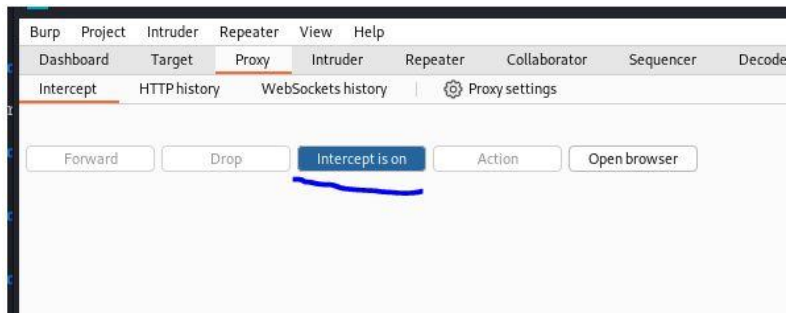
Настройка сервера

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



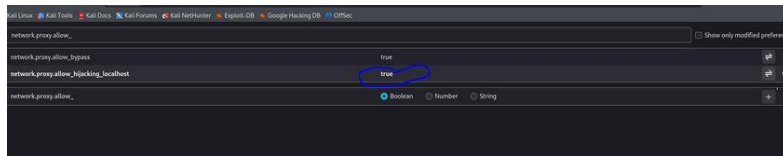
Настройка Burp Suite

Во вкладке Прокси устанавливаю “Intercept is on” (рис. [-@fig:006]).



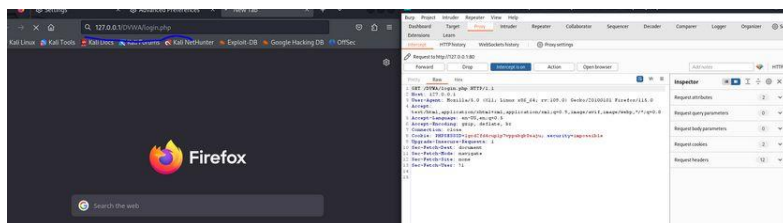
Настройки Proxy

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



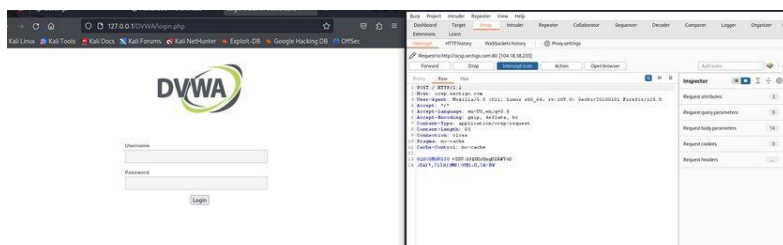
Настройки параметров

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



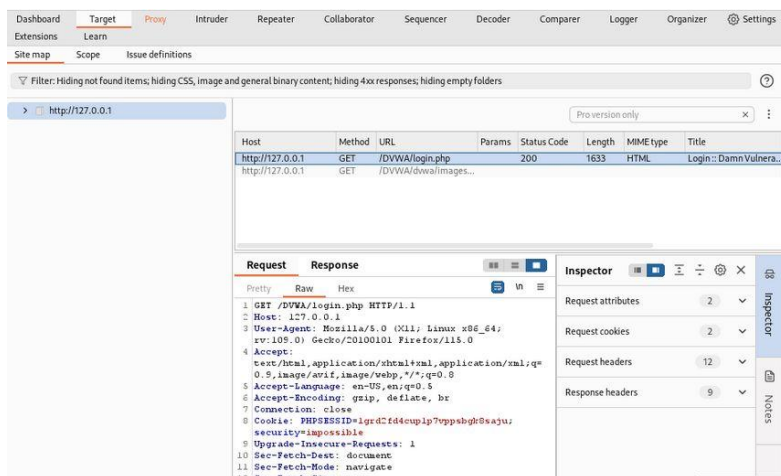
Получаемые запросы сервера

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



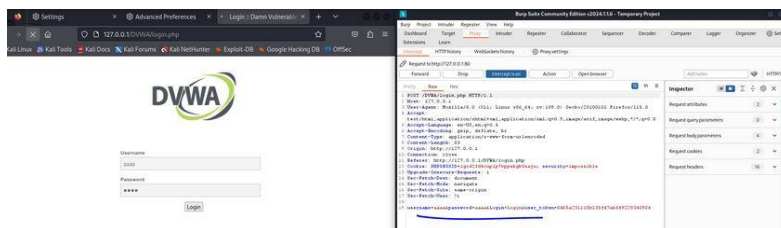
Страница авторизации

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



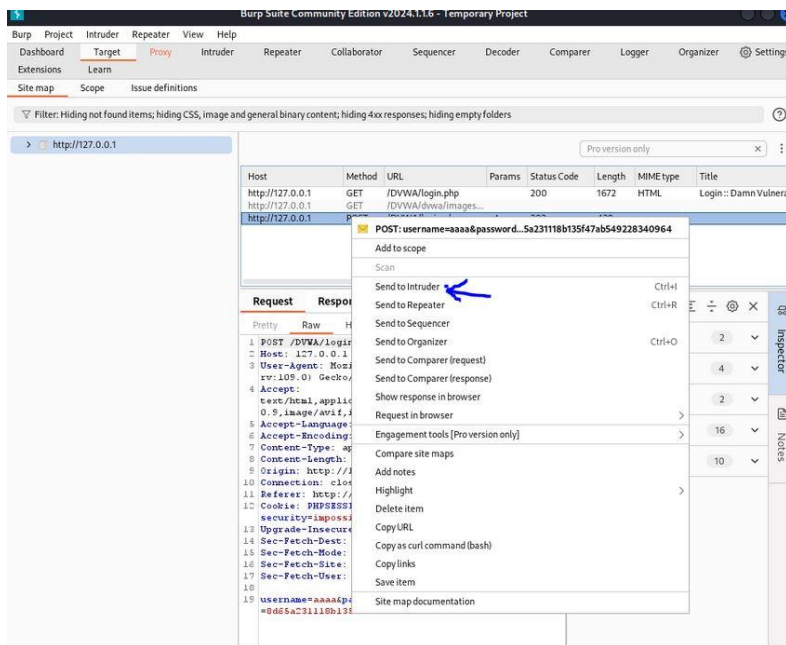
История запросов

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]).



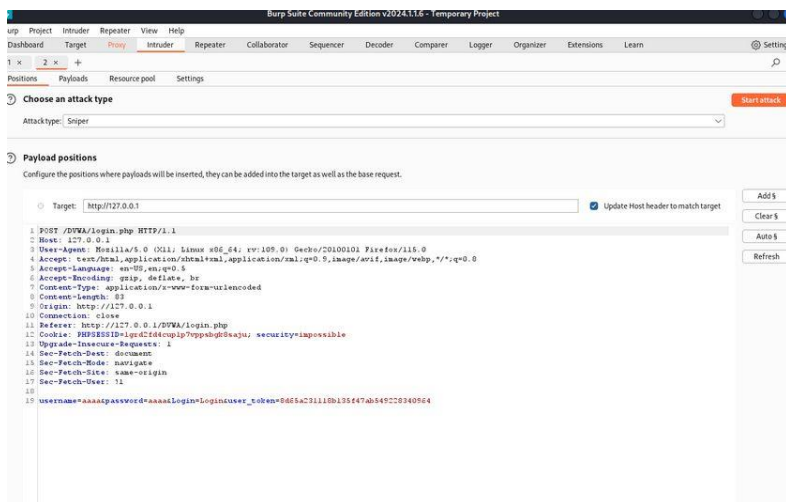
Ввод случайных данных

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]).



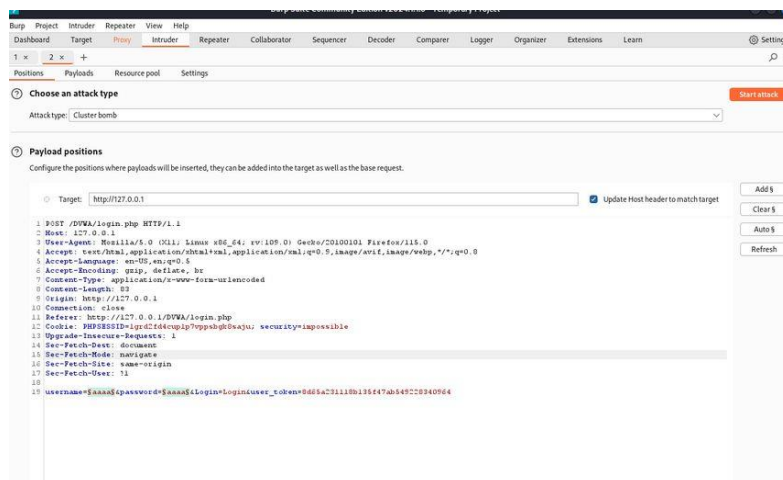
POST-запрос с вводом пароля и логина

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



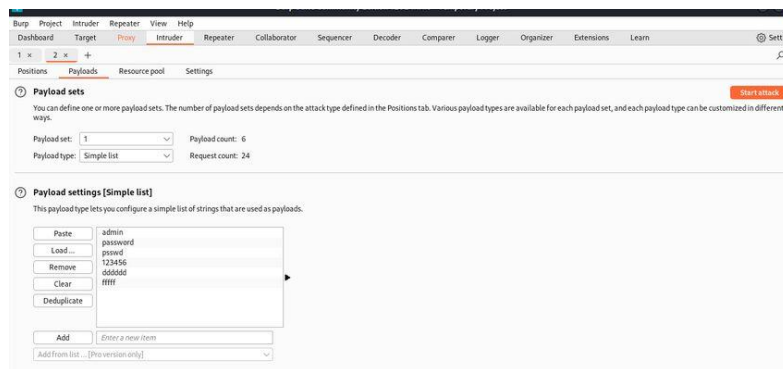
Вкладка Intruder

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]).



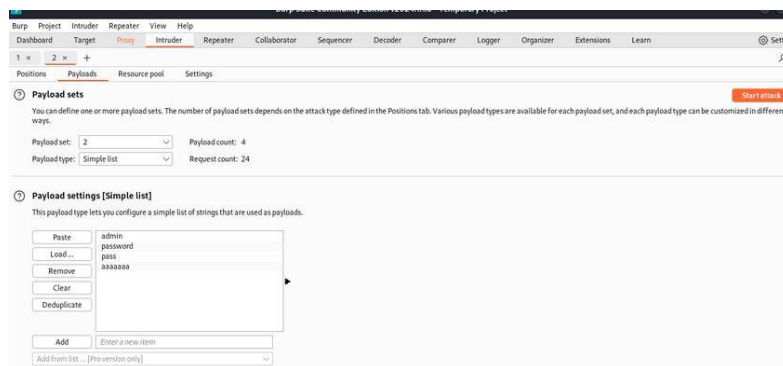
Изменение типа атаки

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]).



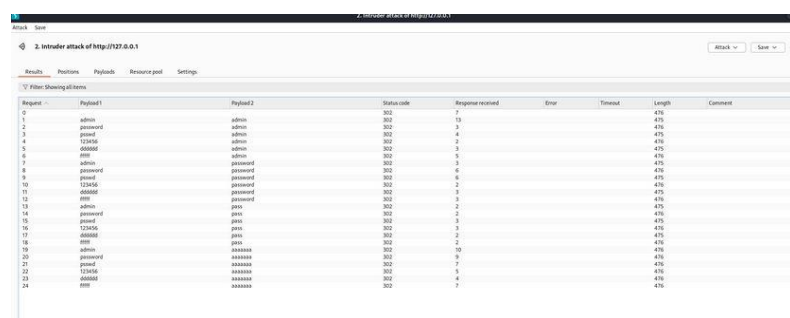
Первый Simple list

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]).



Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			475	
1	admin	admin	302	13			475	
2	password	admin	302	3			475	
3	passw	admin	302	4			475	
4	123456	admin	302	2			475	
5	admin	admin	302	3			475	
6	pass	admin	302	5			475	
7	admin	password	302	1			475	
8	password	password	302	6			475	
9	passw	password	302	6			475	
10	123456	password	302	2			475	
11	admin	password	302	3			475	
12	pass	password	302	3			475	
13	admin	pass	302	2			475	
14	password	pass	302	2			475	
15	passw	pass	302	3			475	
16	123456	pass	302	3			475	
17	admin	pass	302	2			475	
18	pass	pass	302	2			475	
19	admin	xxxxxx	302	10			475	
20	password	xxxxxx	302	9			475	
21	passw	xxxxxx	302	7			475	
22	123456	xxxxxx	302	5			475	
23	admin	xxxxxx	302	4			475	
24	pass	xxxxxx	302	4			475	

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]).

Payload1: admin

Payload2: admin

Status code: 302

Length: 475

Timer: 13

Previous

Next

Request

Response

Pretty

Raw

Hex

Render

1 HTTP/1.1 302 Found

2 Date: Thu, 09 May 2024 14:47:26 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=hqle0nfenbtgo6dec2ok3edu83; expires=Fri, 10 May 2024 14:47:26 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

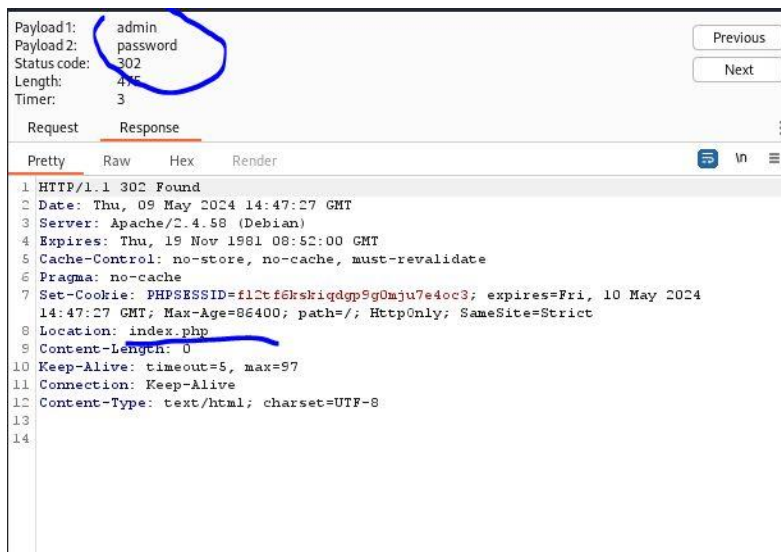
12 Content-Type: text/html; charset=UTF-8

13

14

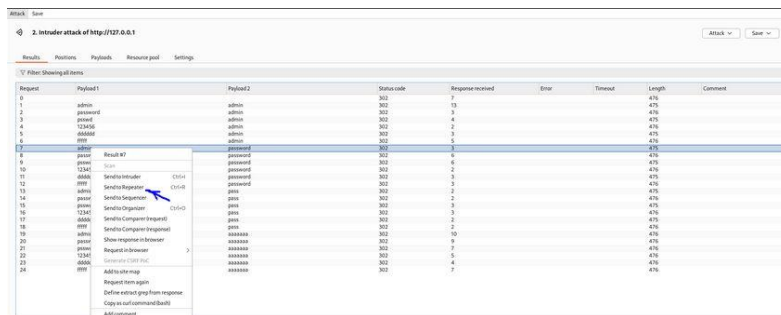
Результат запроса

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



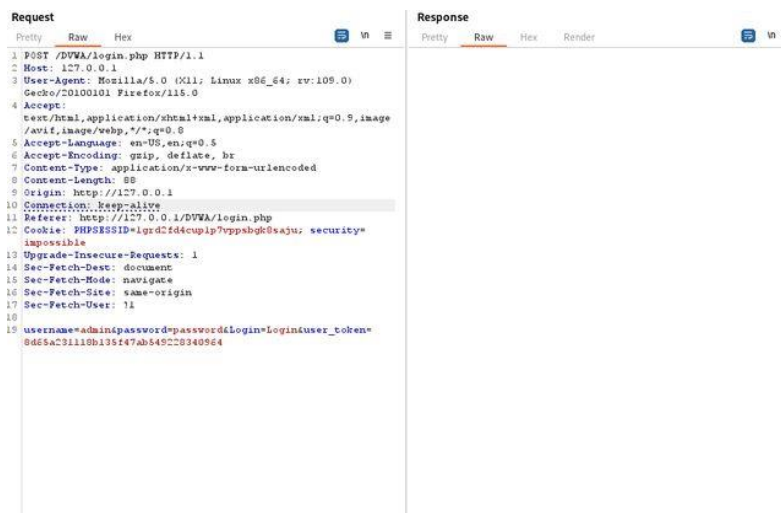
Результат запроса

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



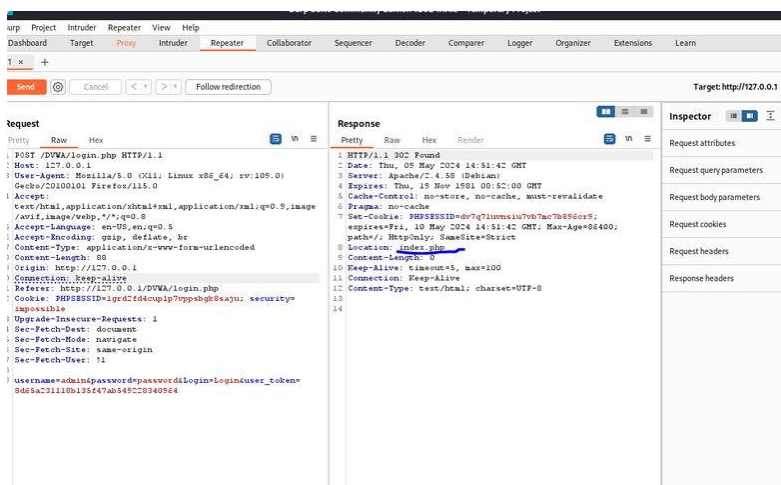
Дополнительная проверка результата

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



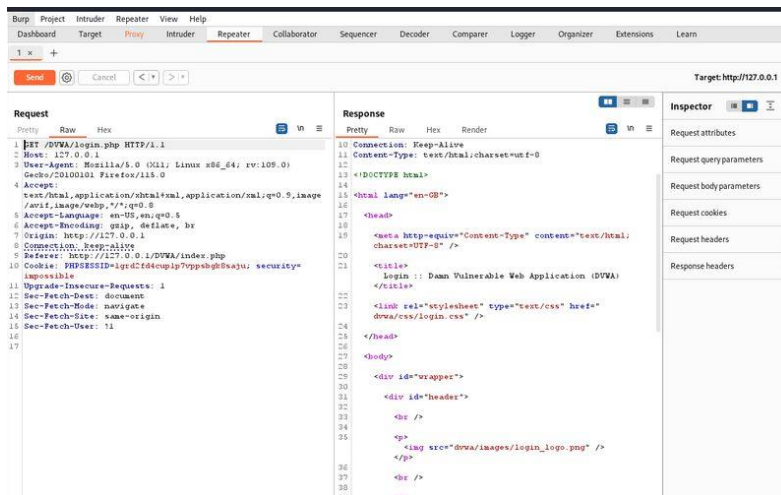
Вкладка Repeater

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



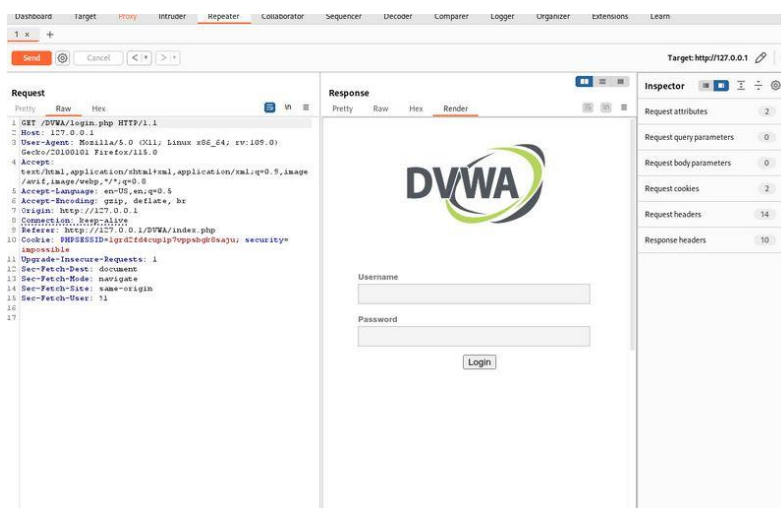
Окно Response

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.

Список литературы