

Отчет по 5 этапу индивидуального проекта

Основы информационной безопасности

Чванова Ангелина Дмитриевна, НПИбд02-21

Содержание

Цель работы	5
Теоретическое введение	6
Выполнение лабораторной работы	7
Выводы	18
Список литературы	19

Список иллюстраций

1	Запуск локального сервера	7
2	Запуск приложения	7
3	Сетевые настройки браузера	8
4	Настройки сервера	8
5	Настройки Burp Suite	9
6	Настройки Proxu	9
7	Настройки параметров	9
8	Получаемые запросы сервера	10
9	Страница авторизации	10
10	История запросов	10
11	Ввод случайных данных	11
12	POST-запрос с вводом пароля и логина	11
13	Вкладка Intruder	12
14	Изменение типа атаки	12
15	Первый Simple list	13
16	Второй Simple list	13
17	Запуск атаки	14
18	Результат запроса	14
19	Результат запроса	15
20	Дополнительная проверка результата	15
21	Вкладка Repeater	16
22	Окно Response	16
23	Изменение в окне Response	17
24	Полученная страница	17

Список таблиц

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.

Выполнение лабораторной работы

Запускаем локальный сервер, на котором необходимо открыть 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
```

Рис. 1: Запуск локального сервера

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

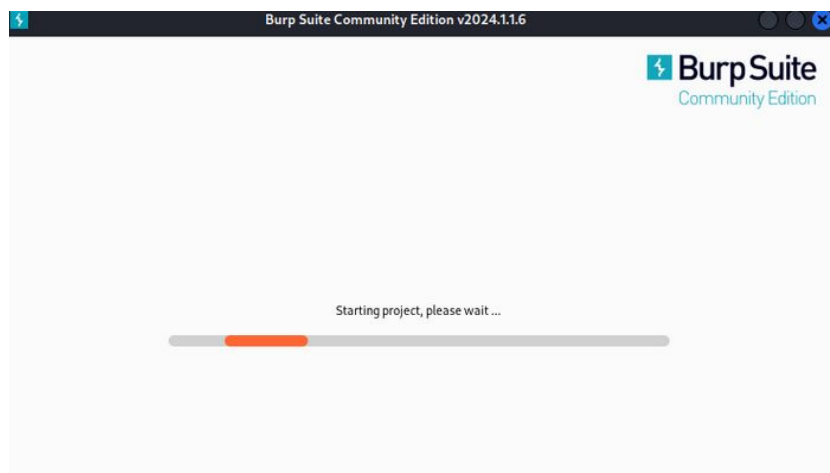


Рис. 2: Запуск приложения

Открываем сетевые настройки браузера для подготовки к работе (рис. [-@fig:003]).

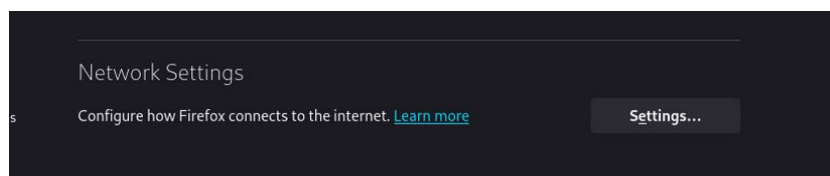


Рис. 3: Сетевые настройки браузера

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

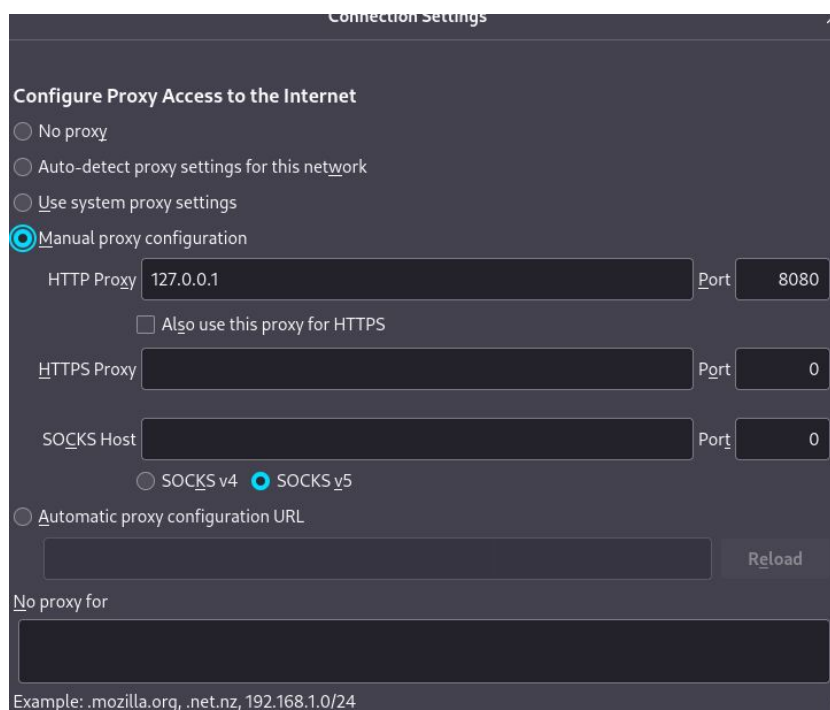


Рис. 4: Настройки сервера

Изменяем настройки Проху инструмента Burp Suite (рис. [-@fig:005]).

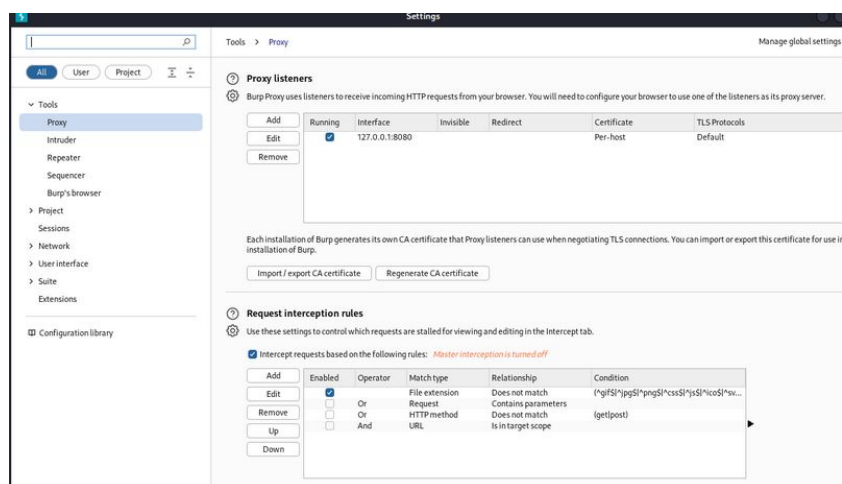


Рис. 5: Настройки Burp Suite

Устанавливаем значение “Intercept is on” во вкладке Proxy (рис. [-@fig:006]).

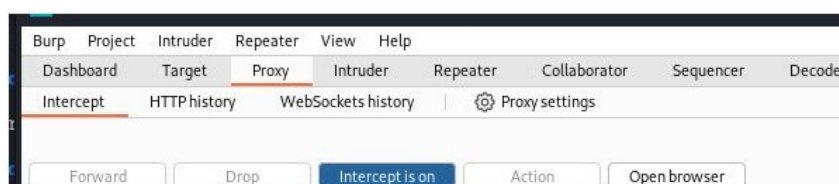


Рис. 6: Настройки Proxy

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

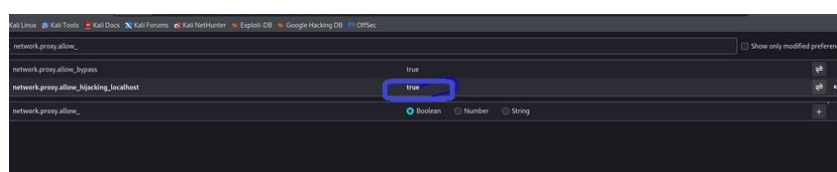


Рис. 7: Настройки параметров

При входе в браузер на DVWA, во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:008]).

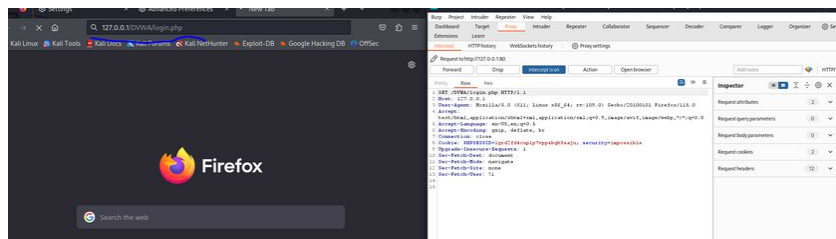


Рис. 8: Получаемые запросы сервера

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

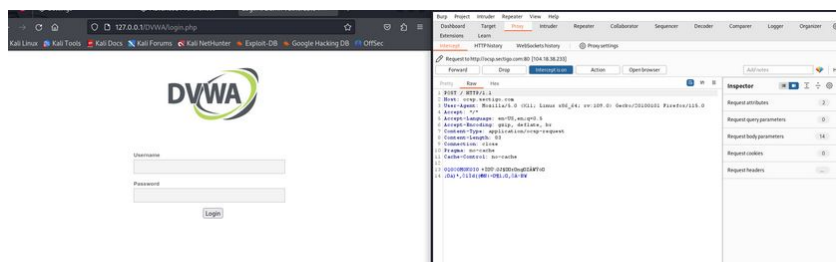


Рис. 9: Страница авторизации

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

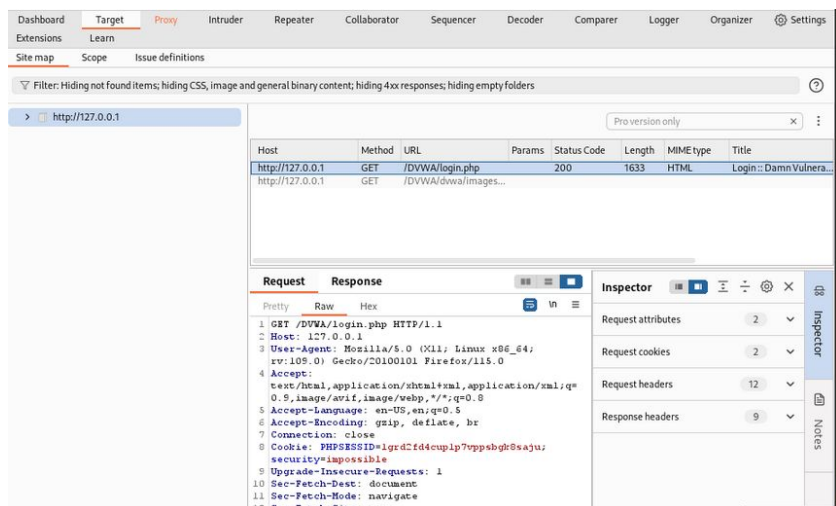


Рис. 10: История запросов

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]).

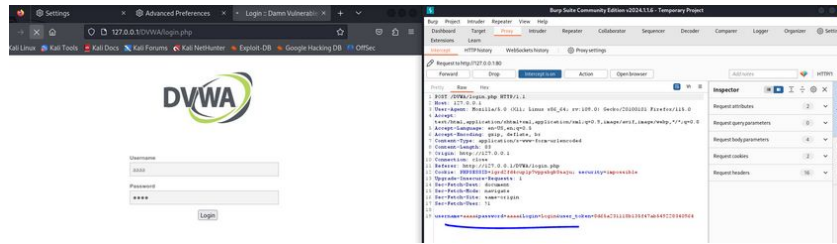


Рис. 11: Ввод случайных данных

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]).

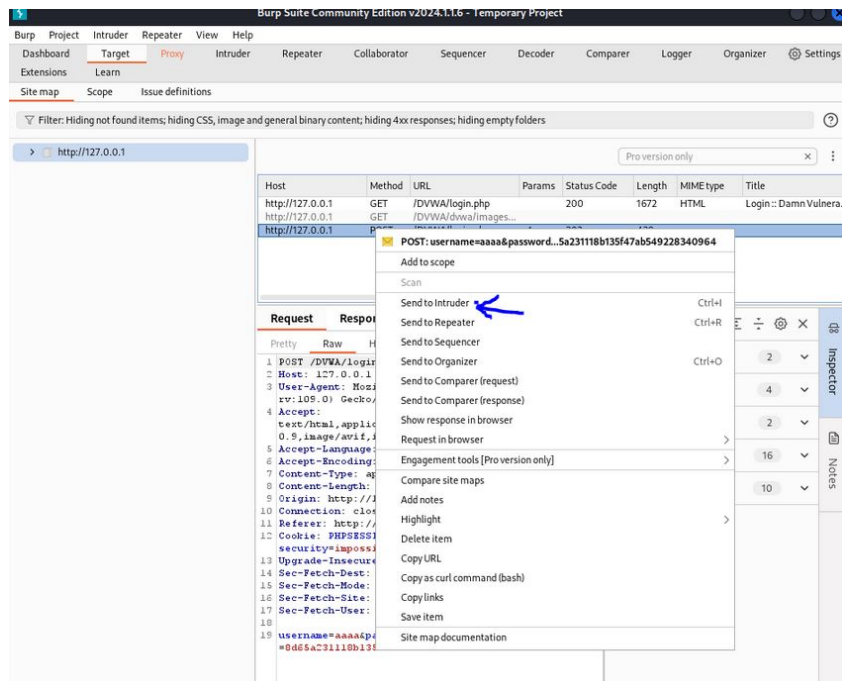


Рис. 12: POST-запрос с вводом пароля и логина

На вкладке Intruder видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:013]).

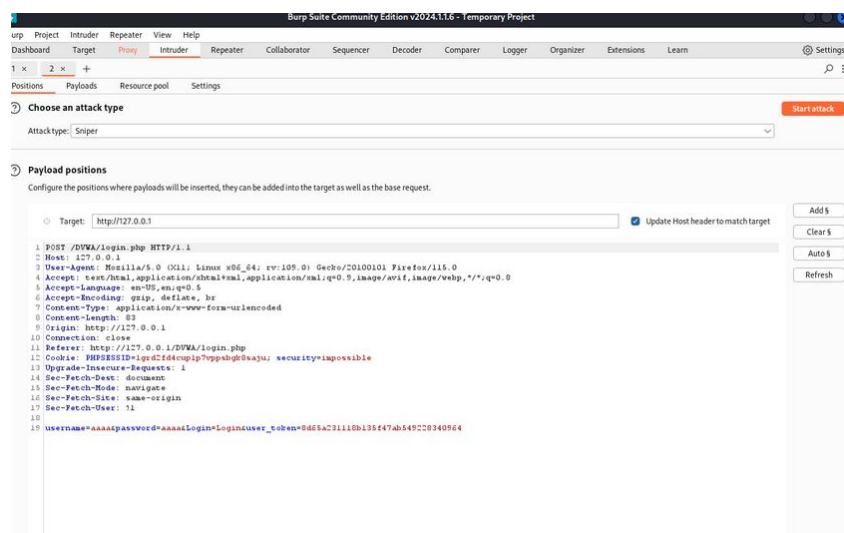


Рис. 13: Вкладка Intruder

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]).

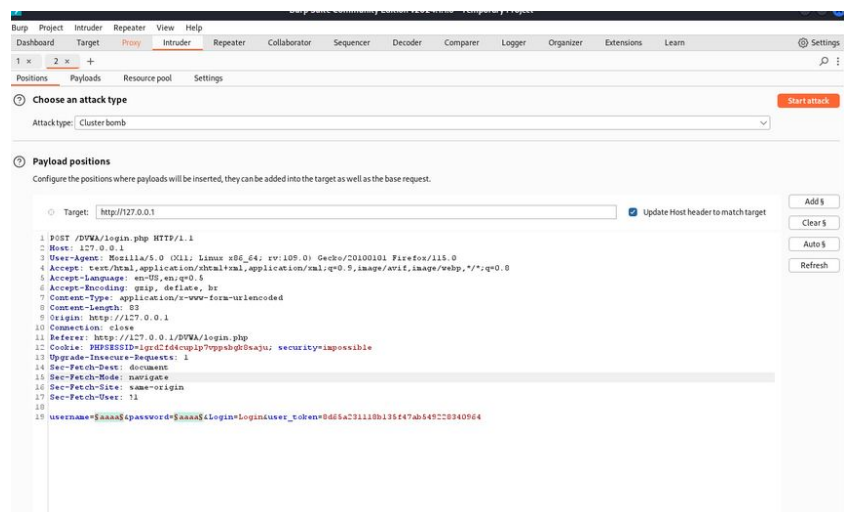


Рис. 14: Изменение типа атаки

Так как мы отметили 2 параметра для подбора, то нам необходимо 2 списка со значениями для подбора. Заполняем первый список в Payload setting (рис. [-@fig:015]).

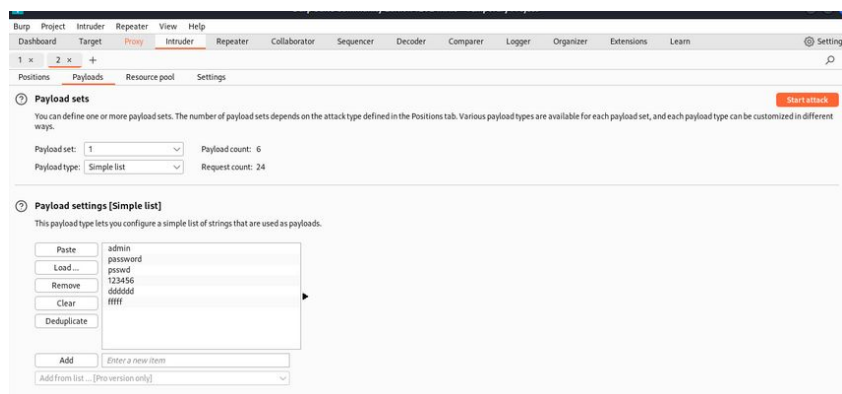


Рис. 15: Первый Simple list

Заполняем значениями второй список. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль (рис. [-@fig:016]).

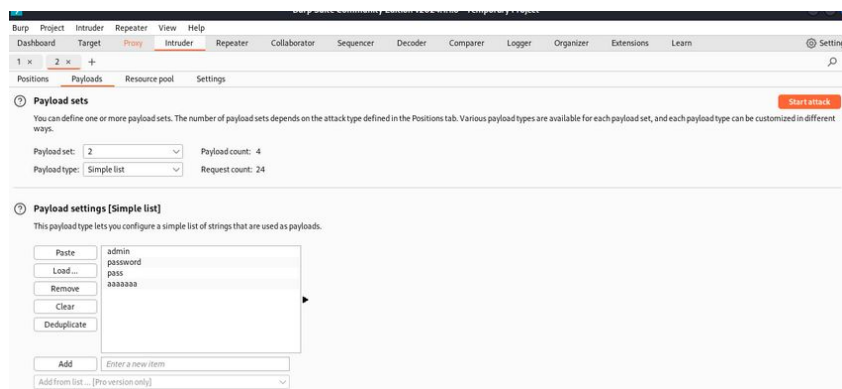


Рис. 16: Второй Simple list

Запускаем атаку и начинаем 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	password	302	3			475	
3	123456	123456	302	4			475	
4	admin	admin	302	3			475	
5	password	password	302	3			475	
6	123456	123456	302	3			475	
7	admin	password	302	3			475	
8	password	password	302	6			475	
9	password	password	302	6			475	
10	123456	password	302	3			475	
11	password	password	302	3			475	
12	admin	password	302	3			475	
13	password	password	302	2			475	
14	password	password	302	2			475	
15	password	password	302	3			475	
16	123456	password	302	3			475	
17	password	password	302	2			475	
18	admin	password	302	2			475	
19	password	password	302	10			475	
20	password	password	302	9			475	
21	password	password	302	7			475	
22	123456	password	302	3			475	
23	password	password	302	4			475	
24	admin	password	302	7			475	

Рис. 17: 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]).

Request	Response
Payload 1: admin Payload 2: admin Status code: 302 Length: 475 Timer: 13	<div>Previous</div> <div>Next</div> <div> Pretty Raw Hex Render </div> <pre> 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=hqle0nfenbtgo6dccc2ok3edu83; 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 </pre>

Рис. 18: 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]).



Рис. 19: Результат запроса

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

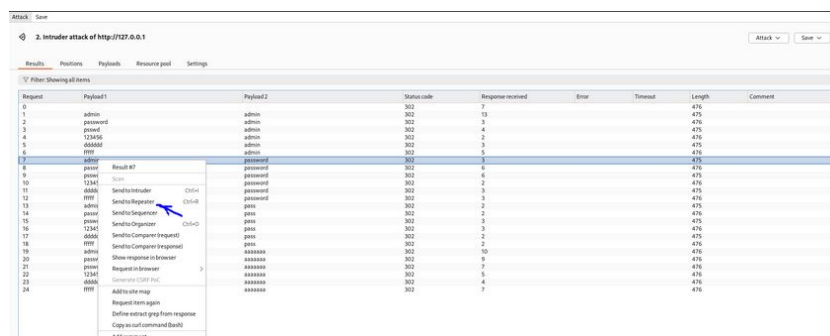


Рис. 20: Дополнительная проверка результата

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

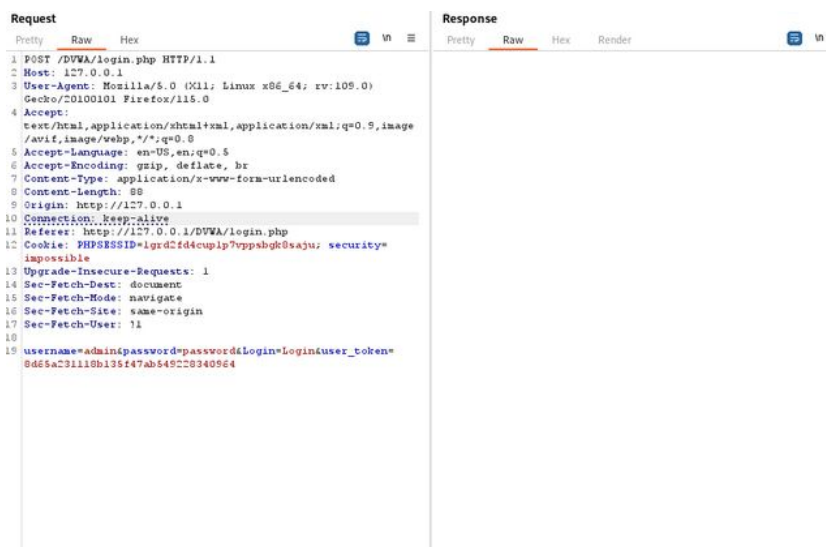


Рис. 21: Вкладка Repeater

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

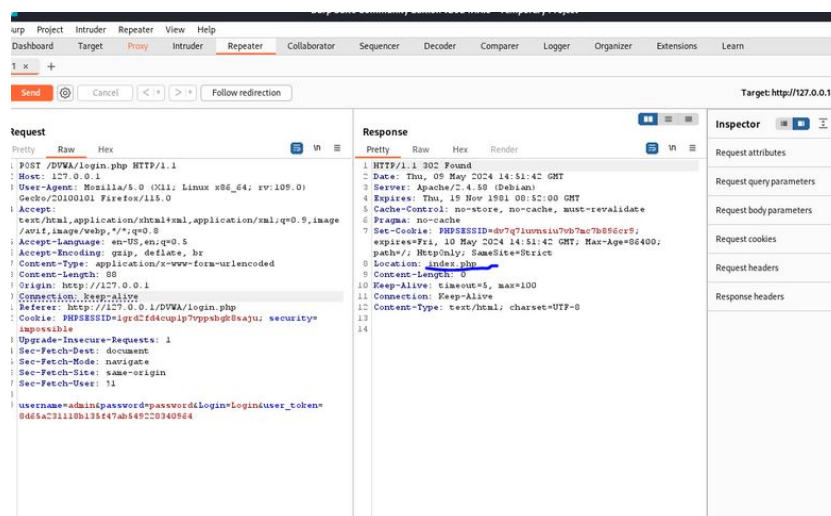


Рис. 22: Окно Response

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

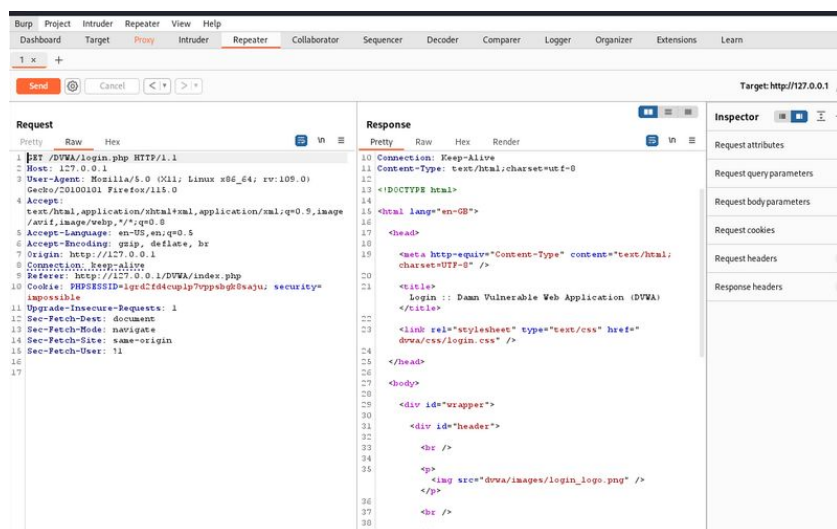


Рис. 23: Изменение в окне Response

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

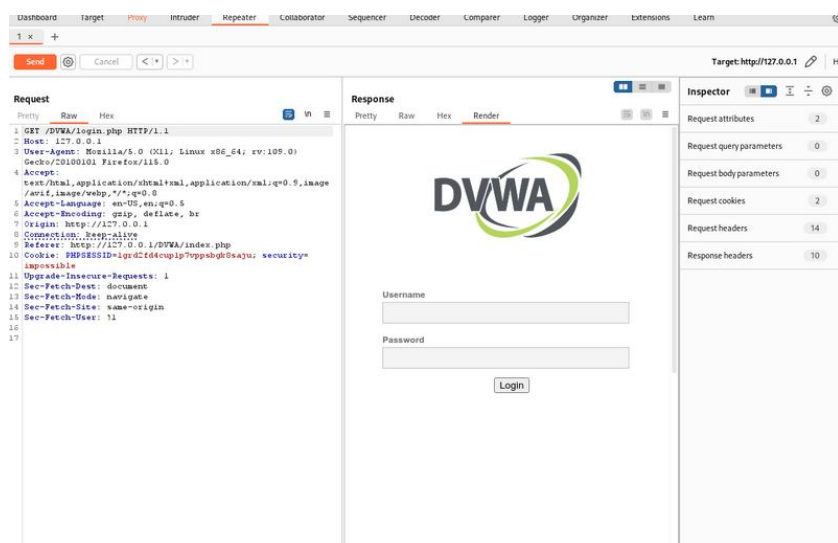


Рис. 24: Полученная страница

Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

Список литературы

- [1] Документация по Virtual Box: <https://www.virtualbox.org/wiki/Documentation>
- [2] Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс