

Индивидуальный проект. Этап 5

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	16
	Список литературы	17

Список иллюстраций

2.1	Запуск mysql и apache2	6
2.2	Запуск burpsuite	7
2.3	Настройки соединения	8
2.4	Настройки приложения	8
2.5	Включение intercept	9
2.6	Параметр network.proxy.allow_hijacking_localhost	9
2.7	Переход на DVWA	10
2.8	Запросы	10
2.9	Попытка авторизации	11
2.10	Перенаправление в Intruder	11
2.11	Cluster bomb attack	12
2.12	Атака	13
2.13	Успешный подбор	14
2.14	Reaper	15

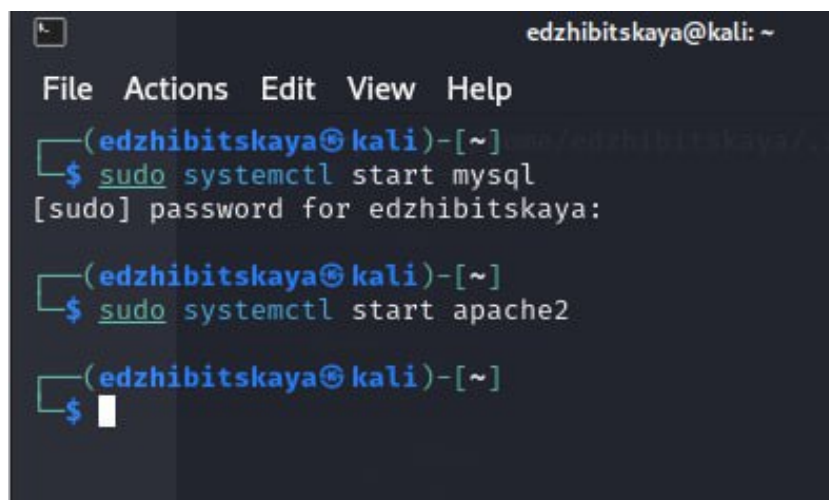
Список таблиц

1 Цель работы

Завершение выполнения индивидуального проекта. Знакомство и освоение Burp Suite.

2 Выполнение лабораторной работы

Запустим сервер для работы с DVWA (рис. 2.1).



```
edzhibitskaya@kali: ~  
File Actions Edit View Help  
(edzhibitskaya@kali)-[~]  
$ sudo systemctl start mysql  
[sudo] password for edzhibitskaya:  
(edzhibitskaya@kali)-[~]  
$ sudo systemctl start apache2  
(edzhibitskaya@kali)-[~]  
$
```

Рис. 2.1: Запуск mysql и apache2

Далее запускаем сам burpsuite.

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения(рис. 2.2).

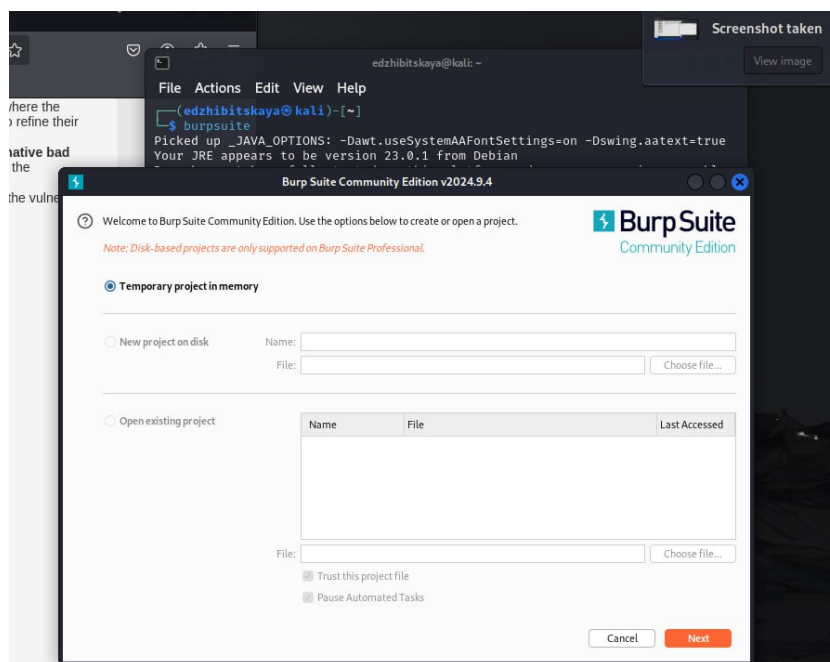


Рис. 2.2: Запуск burpsuite

После необходимо его настроить. Для этого в настройках соединения указываем 127.0.0.1 - наш сервер в http проху(рис. 2.3), проверяем настройки приложения(рис. 2.4), ставим интерсепт в режим on(рис. 2.5).

Также устанавливаем на true параметр network.proxy.allow_hijacking_localhost(рис. 2.6).

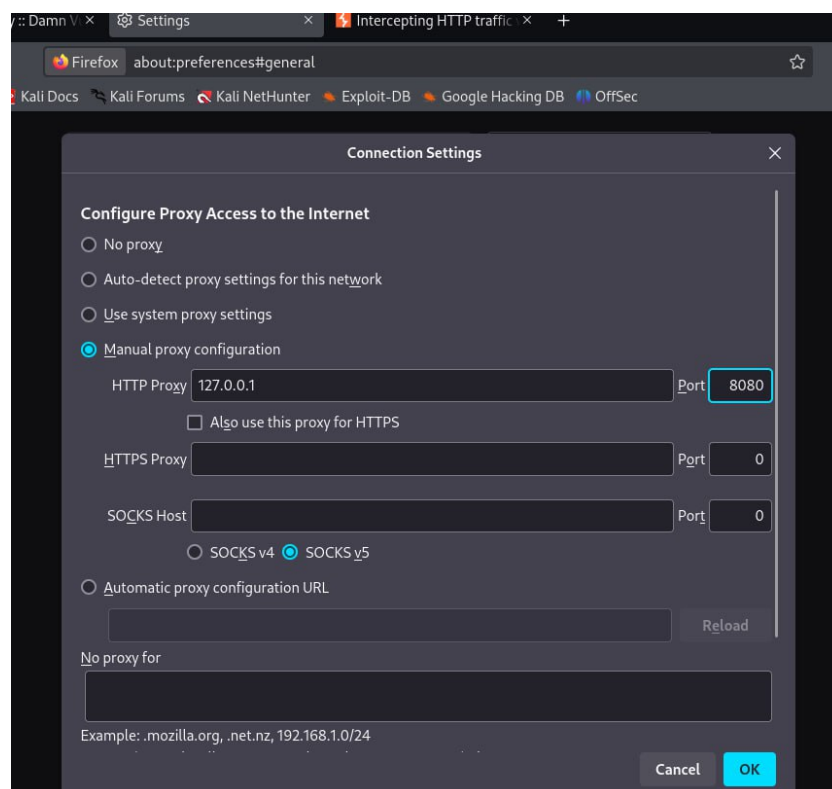


Рис. 2.3: Настройки соединения

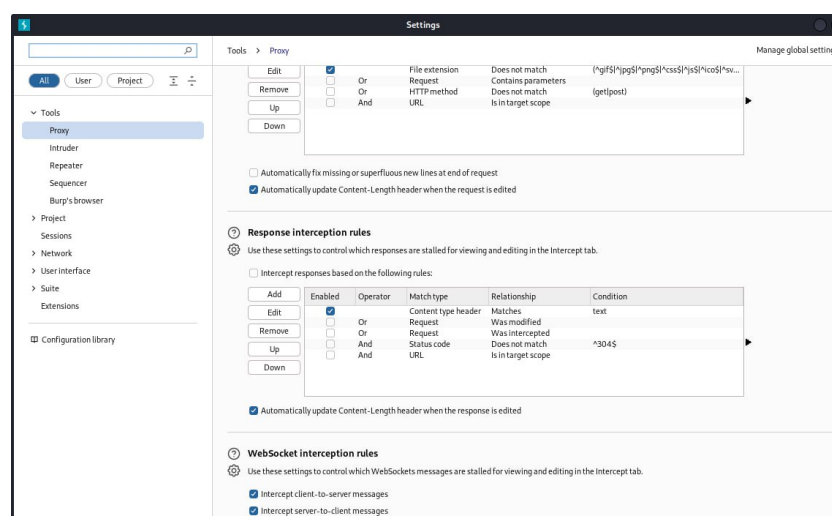


Рис. 2.4: Настройки приложения

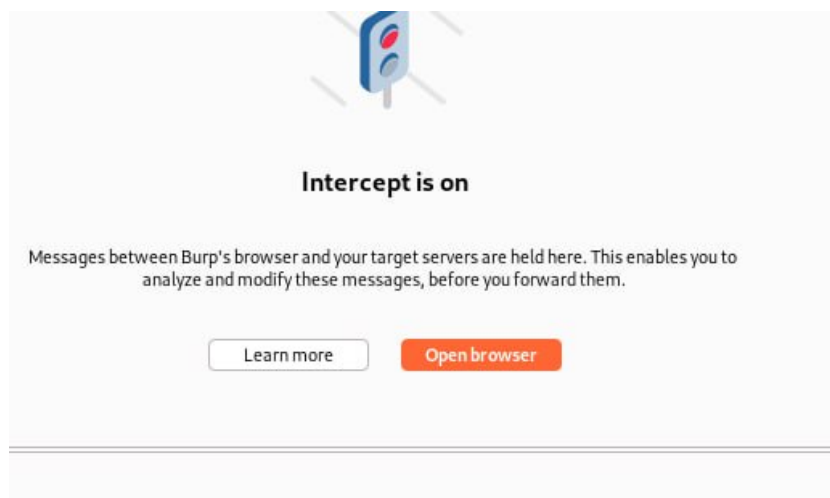


Рис. 2.5: Включение intercept

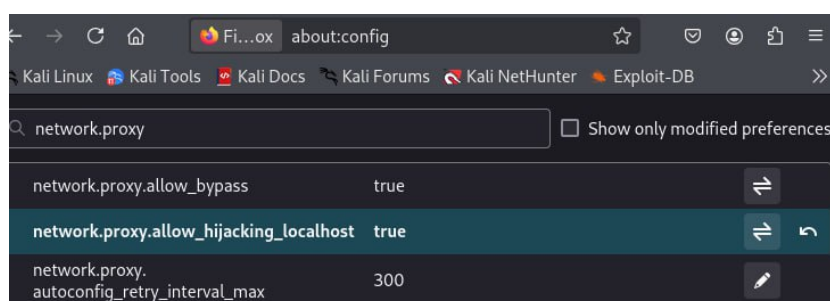


Рис. 2.6: Параметр network.proxy.allow_hijacking_localhost

Переходим непосредственно к работе.

Заходим на DVWA и смотрим, что появляется во вкладке Proxy (рис. 2.7). Видим, что запросы обновляются (также используем forward) (рис. 2.8).

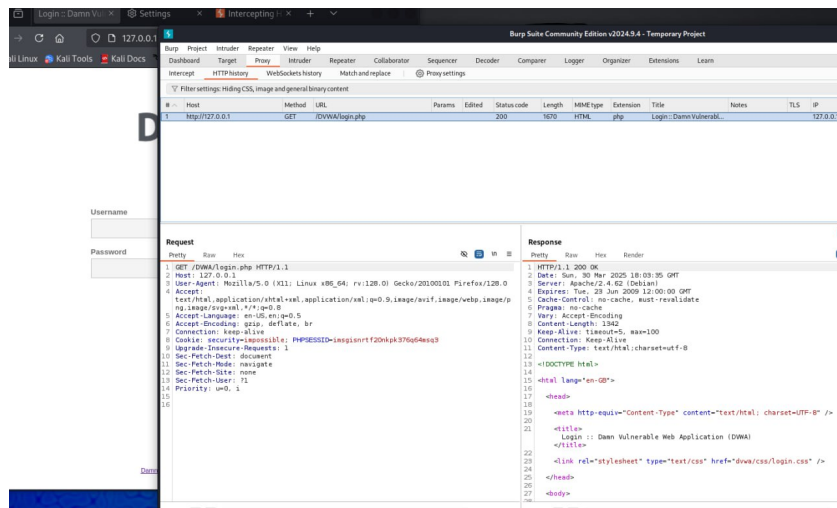


Рис. 2.7: Переход на DVWA

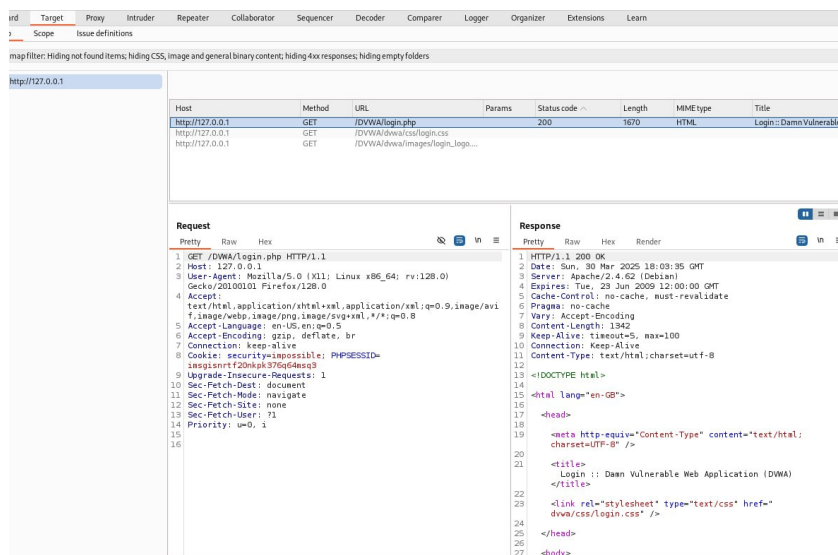


Рис. 2.8: Запросы

Пытаемся авторизоваться и видим внизу появляются введенные данные(рис. 2.9).

```
Request
Pretty Raw Hex
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,
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: 85
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DWA/login.php
12 Cookie: security=impossible; PHPSESSID=msgisnrtf20nkp376q64msq3
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 Priority: u=0, i
19
20 username=root&password=fhkanf&Login=Login&user_token=2795346fec0c648e25bf6eb6c6255965
```

Рис. 2.9: Попытка авторизации

Отправляем запрос в Intruder(рис. 2.10).

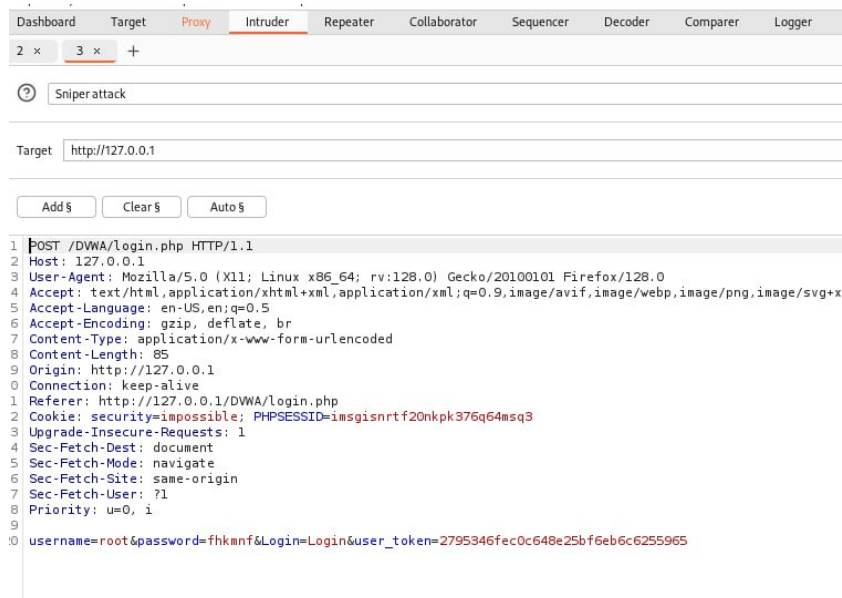


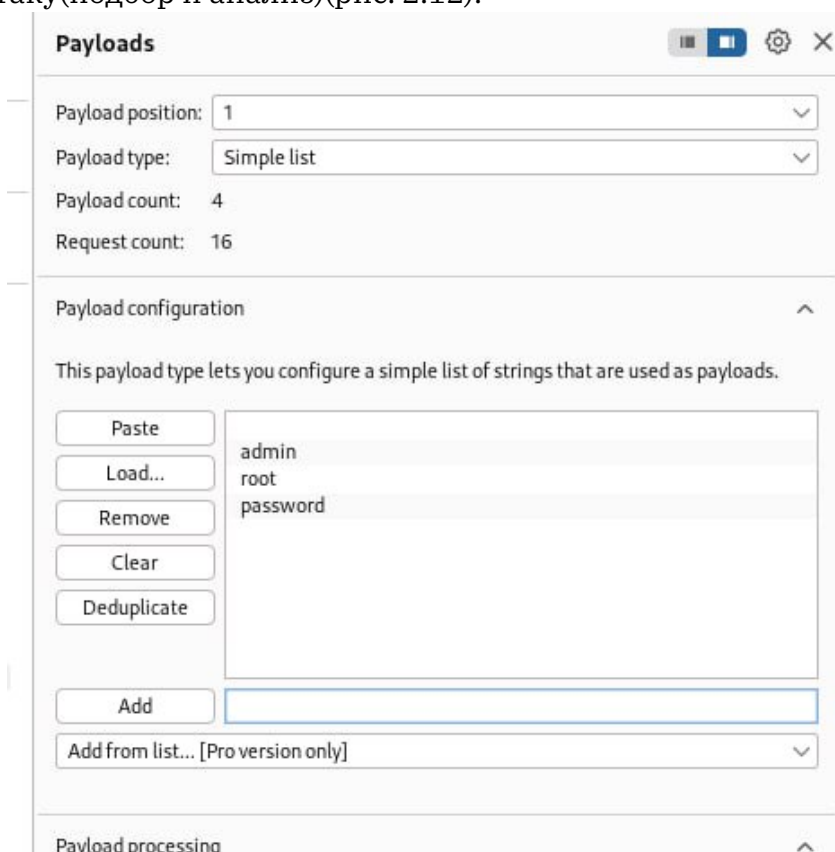
Рис. 2.10: Перенаправление в Intruder

Далее меняю тип атаки на Cluster bomb, меняю(убираю) данные о логине и пароле для дальнейшего подбора(рис. 2.11).



Рис. 2.11: Cluster bomb attack

Заполняем данными таблицы 1 и 2 - для логина и пароля(рис. ??) и запускаем атаку(подбор и анализ)(рис. 2.12).



3. Intruder attack of http://127.0.0.1

Results

Positions

▼ Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Com
7	root	root	302	23			475	
8	password	root	302	7			475	
9		password	302	90			476	
10	admin	password	302	26			475	
11		root	302	12			475	
12	password	password	302	8			475	
13		admin	12345	302	17		475	
14		root	12345	302	15		475	
15		password	12345	302	10		475	
16		password	12345	302	7		475	

Request

Response

Pretty

Raw

Hex

Render

1 HTTP/1.1 302 Found

2 Date: Sun, 30 Mar 2025 18:26:00 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=fh08vkvun7L4h0o9shhtgovapc; expires=Mon, 31 Mar 2025 18:26:00 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict

8 Location: login.php

9 Content-Length: 0

10 Keep-Alive: timeout=5, max=96

11 Connection: Keep-Alive

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

13

14

Рис. 2.12: Атака

На предыдщем рисунке видно, что местоположение не меняется при неверных вариантах, а вот если посмотреть ниже, на подходящем наборе данных местоположение(location) уже меняется - происходит авторизация - вход успешный(рис. 2.13).

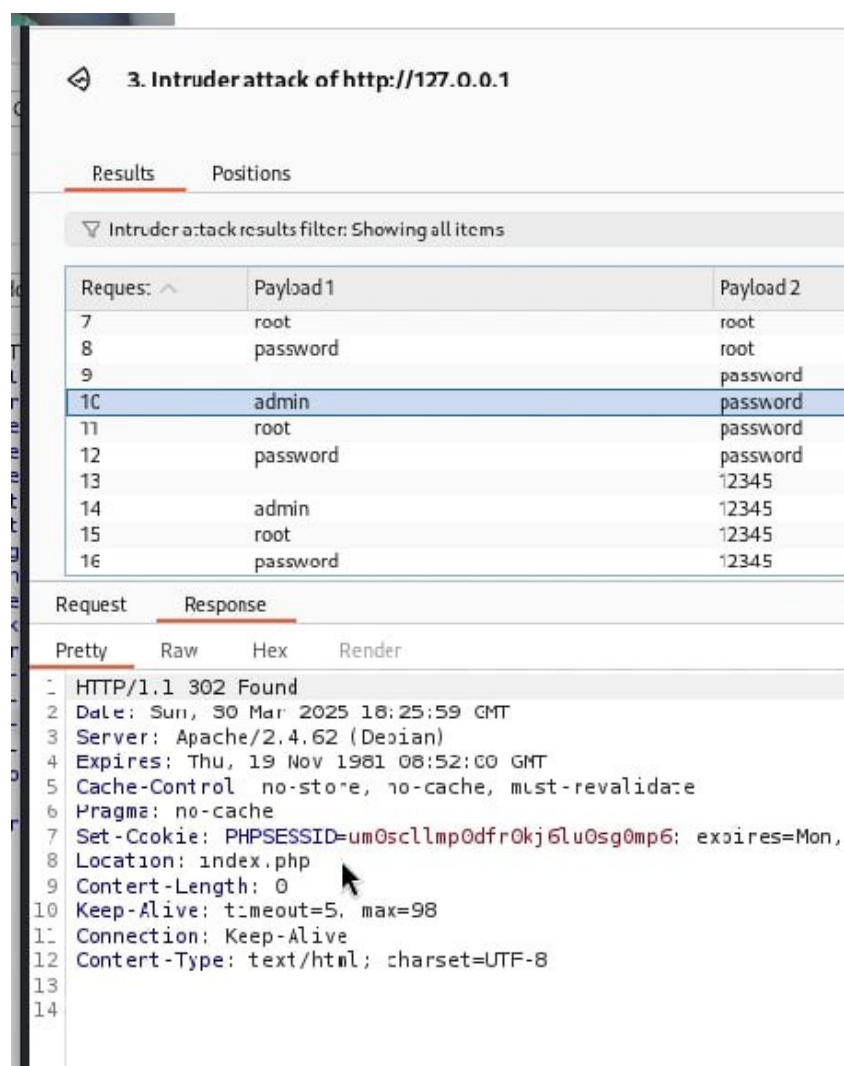


Рис. 2.13: Успешный подбор

Изучим также работы repeater. Перенаправим туда любой результат, посмотрим на его ответ в виде render - увидим страницу входа(рис. 2.14).

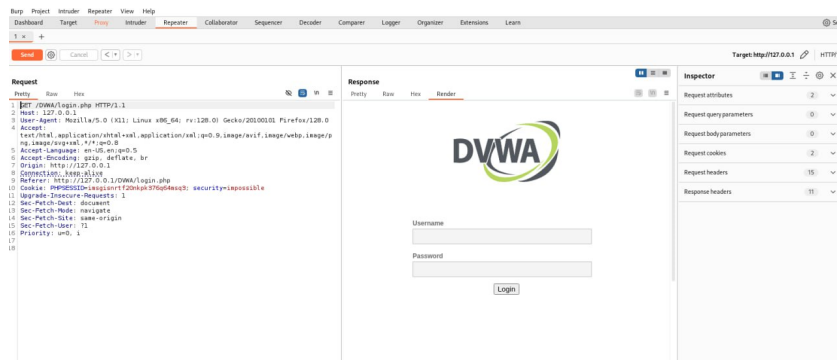


Рис. 2.14: Repeater

3 Выводы

В ходе работы было произведена знакомство с Burp Suite, произведен анализ работы и принцип атаки подбора данных для входа

Список литературы

- 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.