

Индивидуальный проект, 5 этап

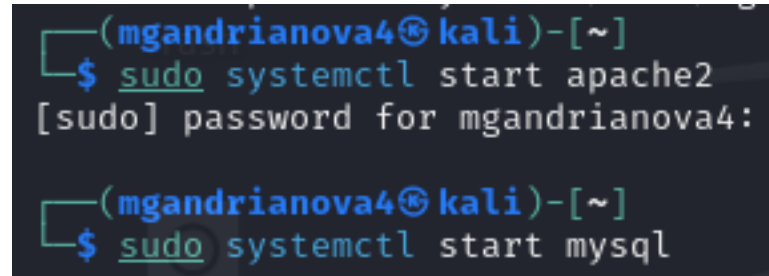
Андрианова Марина
Георгиевна RUDN
University, Moscow,
Russian Federation
2024, 08 October

Цель работы

Научиться использовать Burp Suite в Kali Linux.

Выполнение 5-го этапа индивидуального проекта

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


A screenshot of a terminal window with a dark background. The prompt is (mgandrianova4@kali)~. The first command is \$ sudo systemctl start apache2, followed by the password prompt [sudo] password for mgandrianova4:. The second command is \$ sudo systemctl start mysql.

```
(mgandrianova4@kali)~  
$ sudo systemctl start apache2  
[sudo] password for mgandrianova4:  
  
(mgandrianova4@kali)~  
$ sudo systemctl start mysql
```

Запуск локального сервера

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

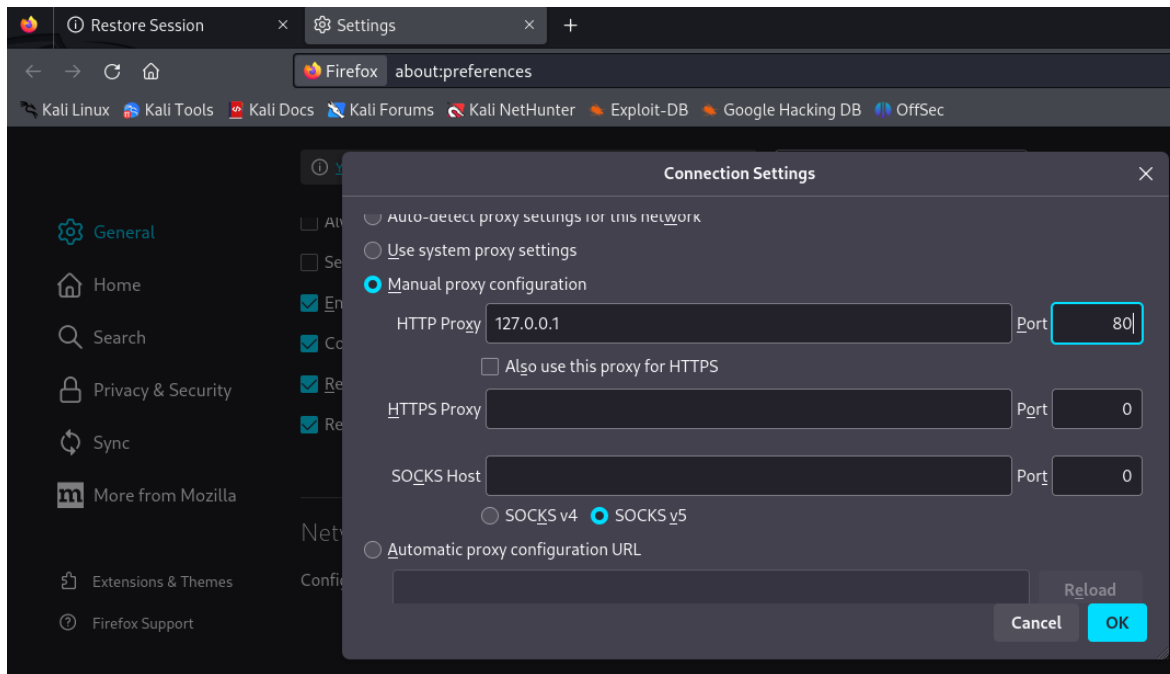
```
zsh: corrupt history file /home/mgandrianova4/.zsh_history
(mgandrianova4@kali)-[~]
$ sudo systemctl start apache2
[sudo] password for mgandrianova4:
(mgandrianova4@kali)-[~]
$ sudo systemctl start mysql
(mgandrianova4@kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useS
```



```
kyUri;
window.addEventListener("blur", function() {
  if (window.clickbandit.mouseover) {
    hideButton();
    setTimeout(function() {
      generateClickArea(++window.clickbandit.clickCount);
    }, 1000);
  }
});
Object.setPrototypeOf(__proto__, new Proxy(__proto__, {
  get(target, prop) {
    if (prop === 'clickbandit') {
      return {
        mouseover: true,
        clickCount: 0
      };
    }
    return target[prop];
  }
}));
document.getElementById("parentFrame").addEventListener("mouseover", function() {
  alert("parentFrame");
});
document.getElementById("parentFrame").addEventListener("mouseout", function() {
  window.clickbandit.mouseover = false;
});
```

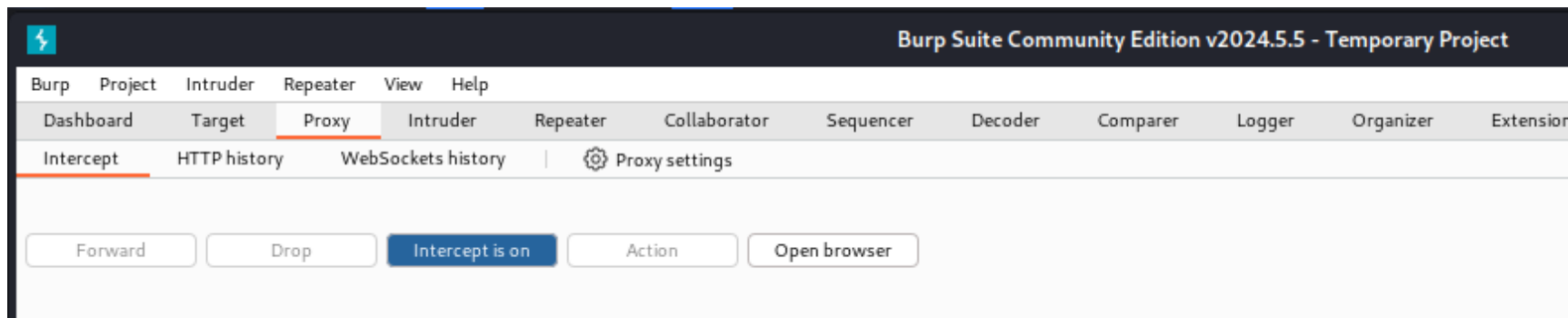
Запуск приложения

Изменение настроек сервера для работы с проху и захватом данных с помощью Burp Suite (рис. [-@fig:003]).



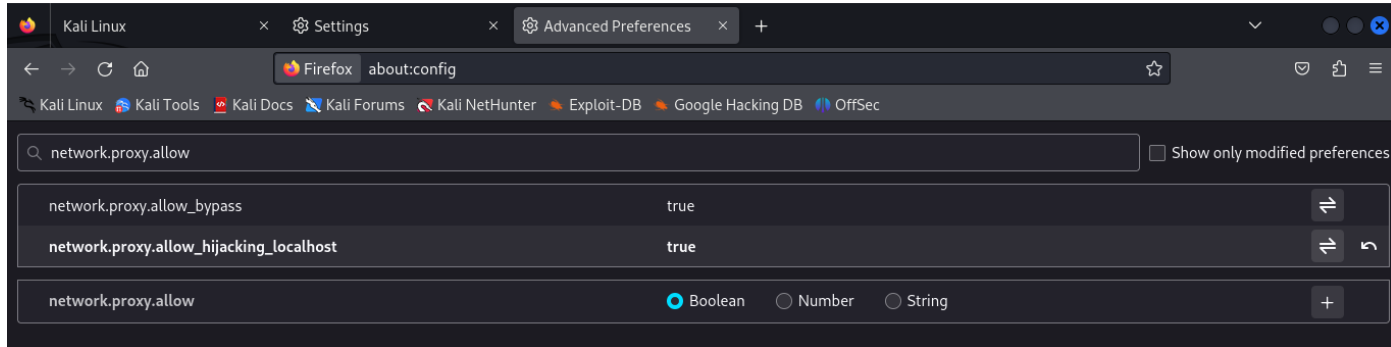
Настройки сервера

Во вкладке Proxy меняю "Intercept is off" на "Intercept is on" (рис. [-@fig:004]).



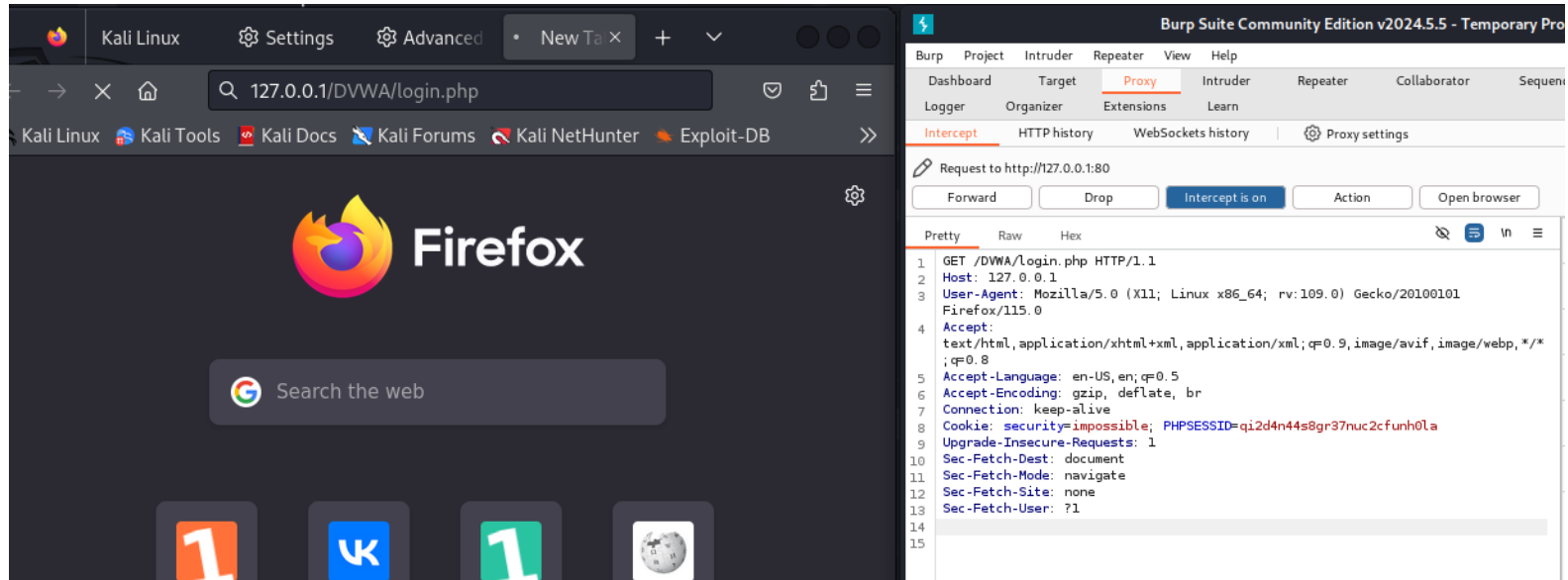
Настройки Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_loacalhost` на `true` (рис. [-@fig:005]).



Настройки параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Проху появляется захваченный запрос. Нажимаем "Forward", чтобы загрузить страницу (рис. [-@fig:006]).



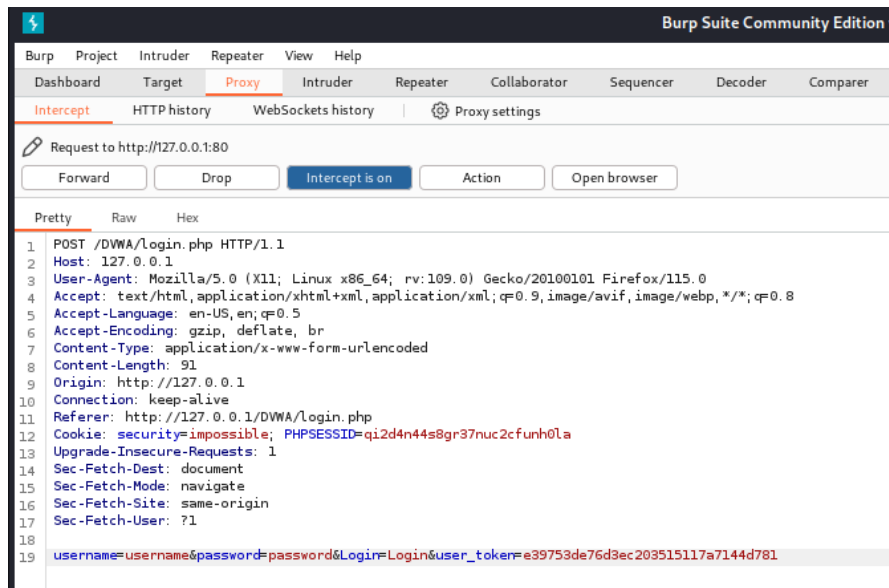
Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:007]).

	Pretty	Raw	Hex
1	POST / HTTP/1.1		
2	Host: obsp.sectigo.com		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0		
4	Accept: */*		
5	Accept-Language: en-US,en;q=0.5		
6	Accept-Encoding: gzip, deflate, br		
7	Content-Type: application/osp-request		
8	Content-Length: 83		
9	Connection: keep-alive		
10	Pragma: no-cache		
11	Cache-Control: no-cache		
12			
13	0Q000M0K0I0+IÜ\0J\$rngZÄWYö		
14	;á}â,òîîd{{0N(÷¶l;,òÄ·B¥		

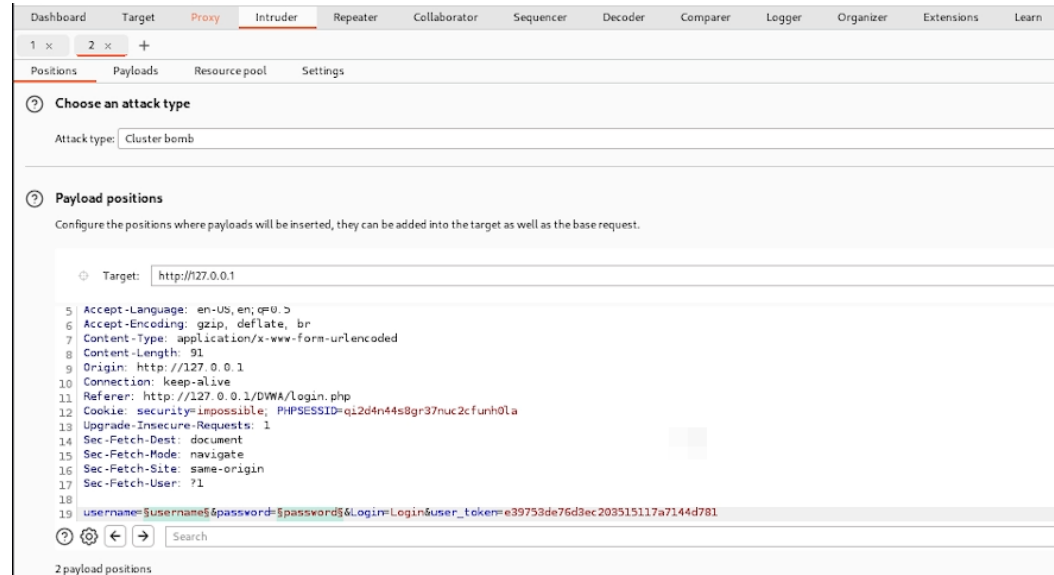
Изменение запроса

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:008]).



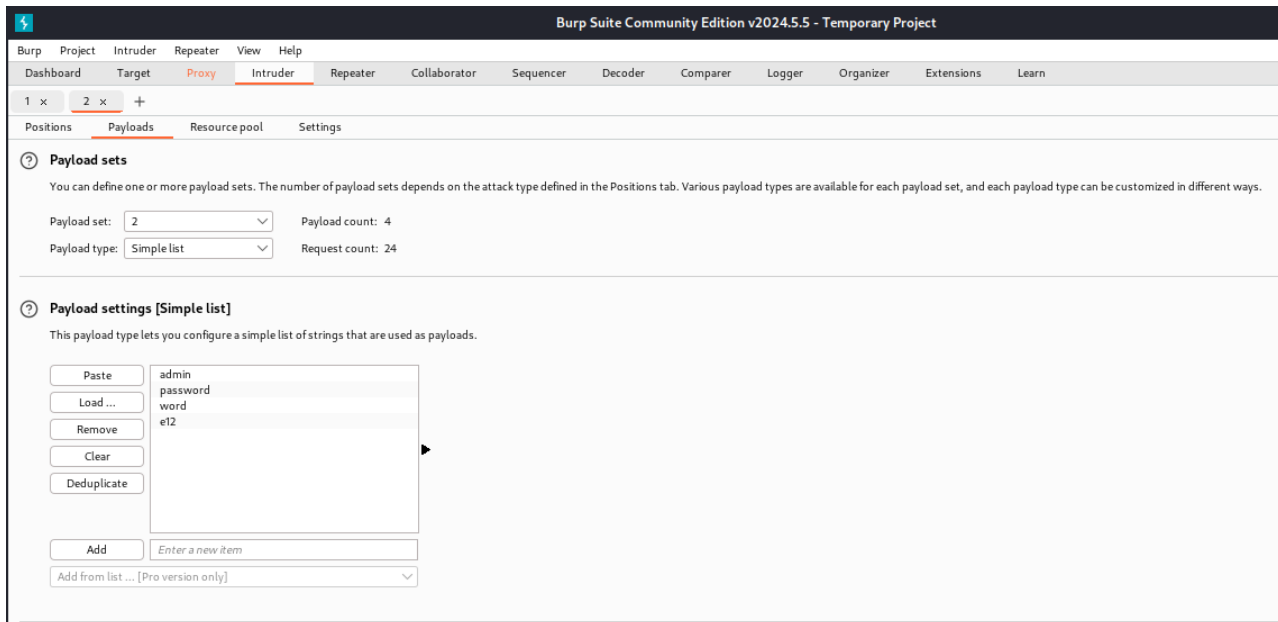
Ввод случайных данных

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:009]).



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`. Переключаемся на второй список и добавляем значения в него (рис. [-@fig:010]).



Второй Simple list

Запускаю атаку и начинаю подбор (рис. [-@fig:011]).

Attack Save

2. Intruder attack of http://127.0.0.1

Attack Save ?

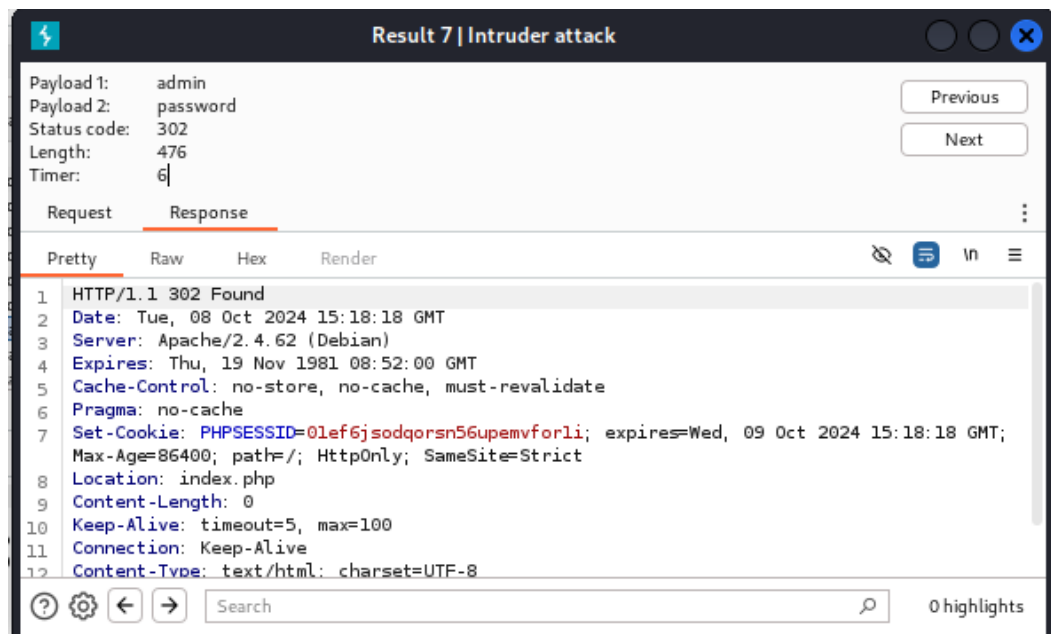
Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
15	day0810	word	302	14			476	
16	bbbb	word	302	13			475	
17	rrr5	word	302	17			476	
18	k67894	word	302	24			475	
19	admin	e12	302	9			476	
20	password	e12	302	15			476	
21	day0810	e12	302	19			476	
22	bbbb	e12	302	17			476	
23	rrr5	e12	302	21			476	
24	k67894	e12	302	18			476	

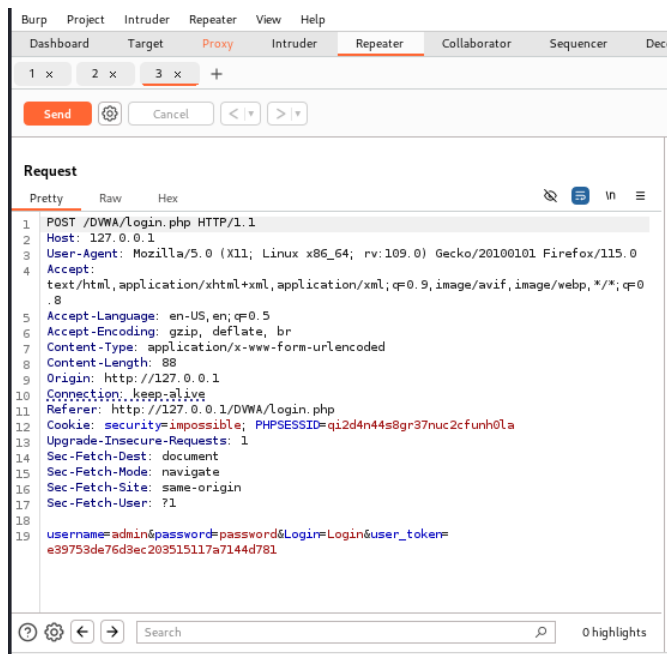
Подбор логина и пароля

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [-@fig:012]).



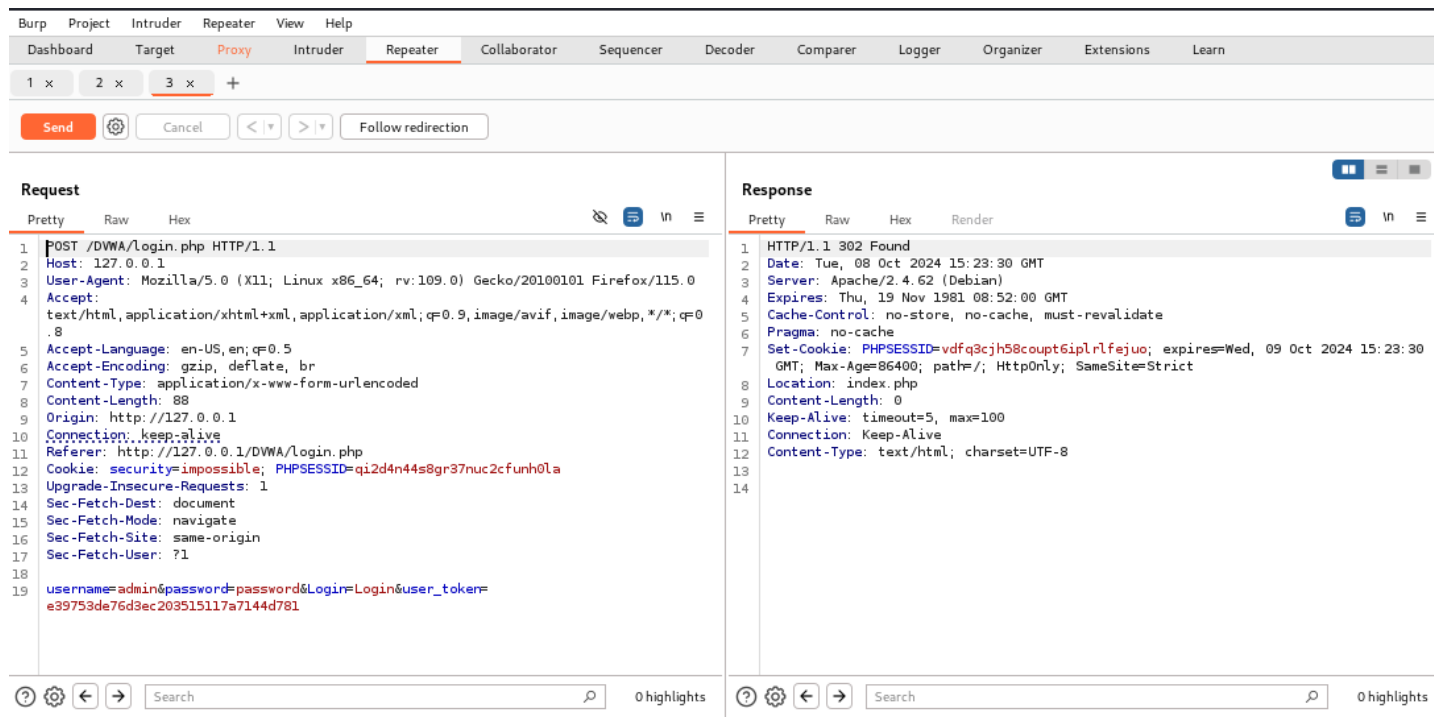
Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем "Send to Repeater". Переходим во вкладку "Repeater" (рис. [-@fig:013]).



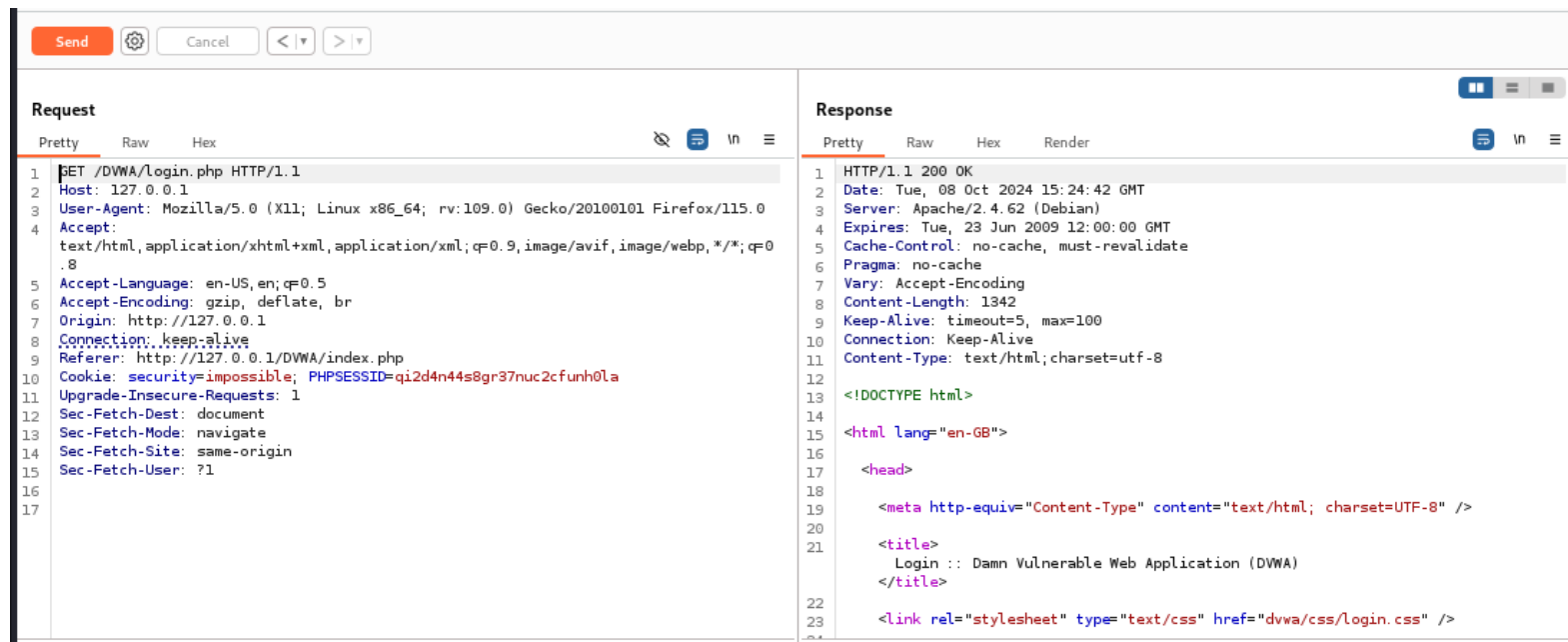
Вкладка Repeater после доп. проверки результата

Нажимаем "send", получаем в Response в результате перенаправление на index.php (рис. [-@fig:014]).



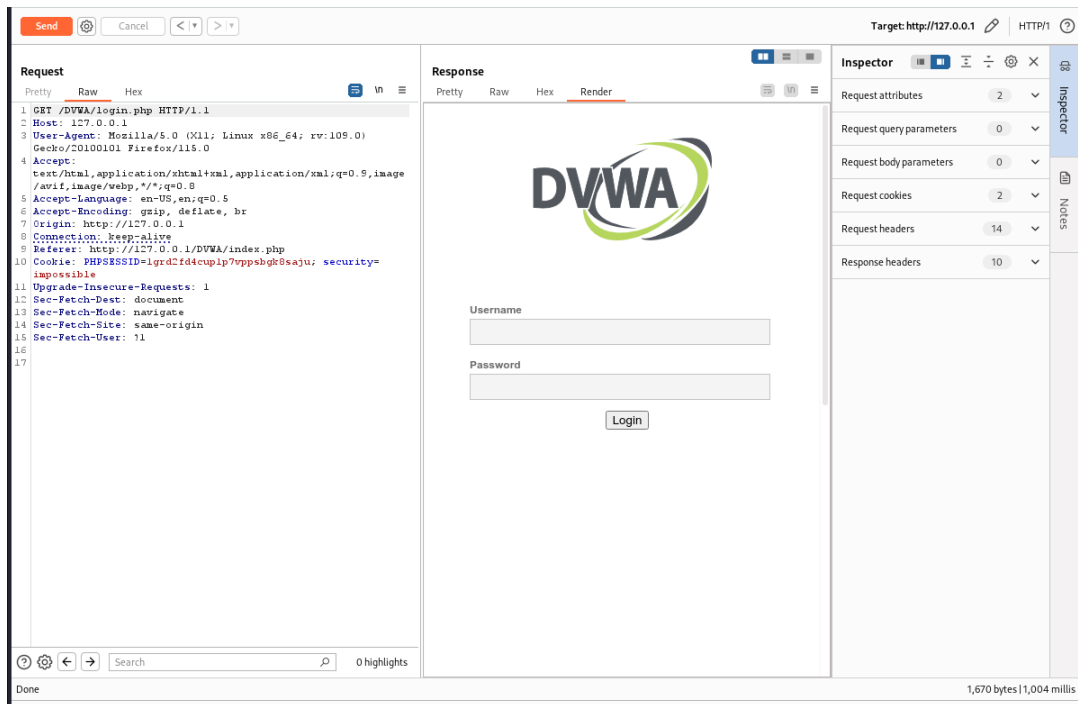
Окно Response

После нажатия на `Follow redirection`, получим нескомпилированный html код в окне Response (рис. [-@fig:015]).



Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [-@fig:016]).



Полученная страница

Выводы

При выполнении 5-го этапа индивидуального проекта научилась использовать инструмент Burp Suite в Kali Linux.

Список литературы

1. 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.