

Отчёт по 5 этапу индивидуального проекта

Дисциплина: Информационная безопасность

Андрианова Марина Георгиевна

Содержание

Цель работы	1
Задание.....	1
Выполнение 5-го этапа индивидуального проекта.....	1
Выводы.....	10
Список литературы.....	10

Цель работы

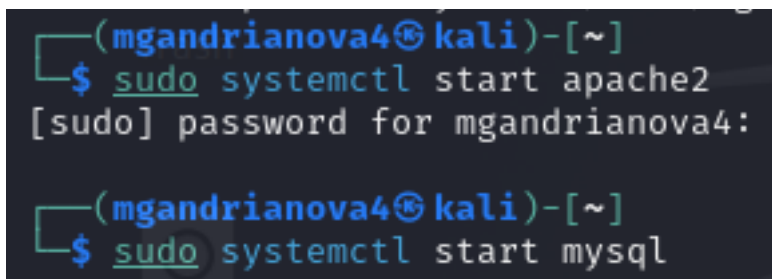
Научиться использовать Burp Suite в Kali Linux.

Задание

Использование Burp Suite.

Выполнение 5-го этапа индивидуального проекта

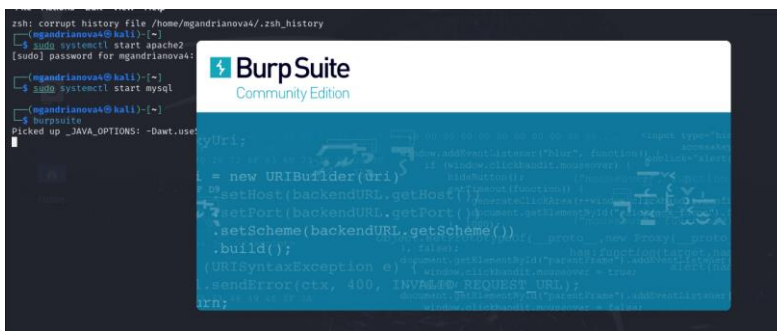
Запускаю локальный сервер, на котором открываю веб-приложение DVWA для тестирования инструмента Burp Suite (рис. [-@fig:001]).



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

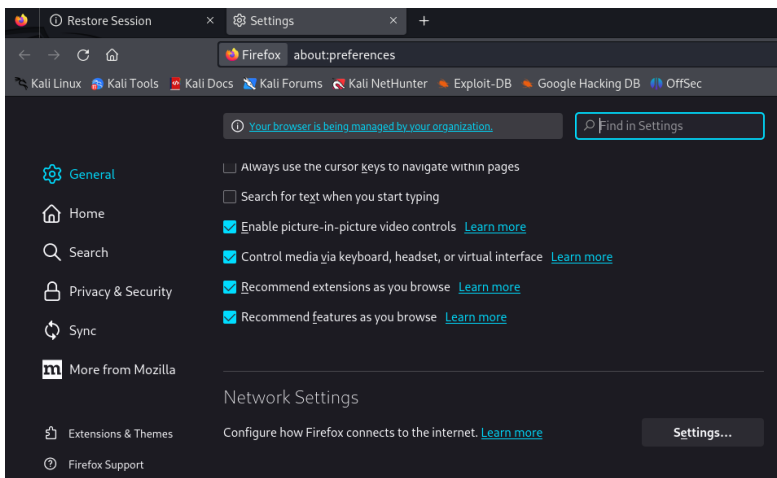
Запуск локального сервера

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



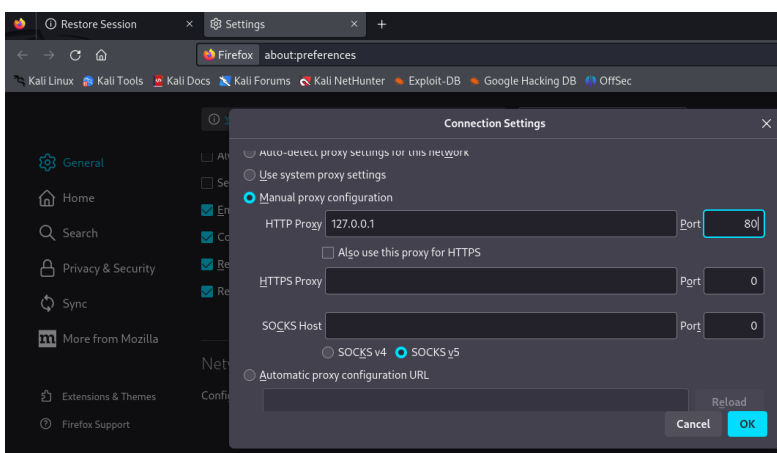
Запуск приложения

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



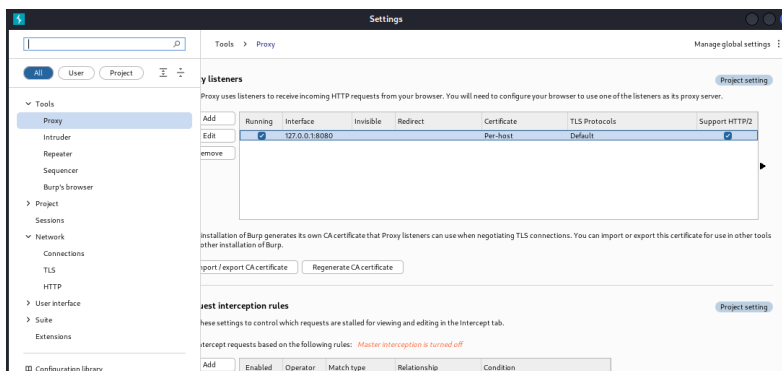
Сетевые настройки браузера

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



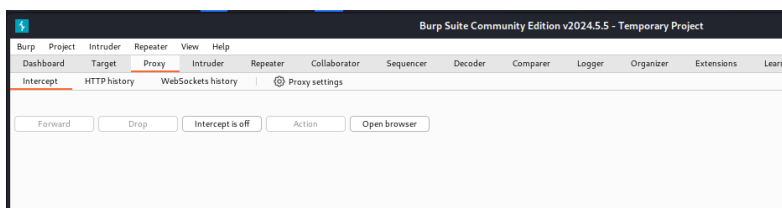
Настройки сервера

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

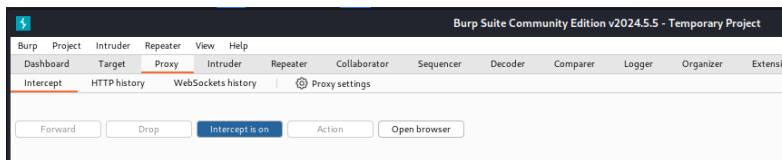


Настройка Burp Suite

Во вкладке Proxy меняю “Intercept is off” на “Intercept is on” (рис. [-@fig:006] и [-@fig:007]).

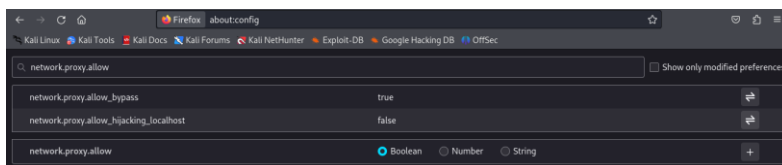


Настройка Proxy

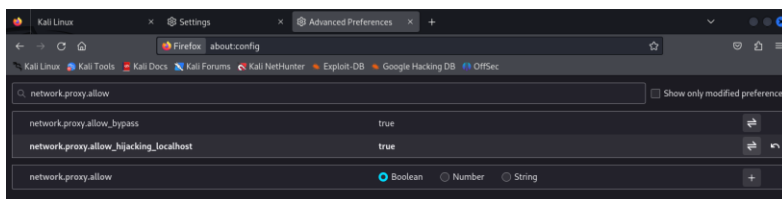


Настройка Proxy

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_localhost` на `true` (рис. [-@fig:008] и [-@fig:009]).

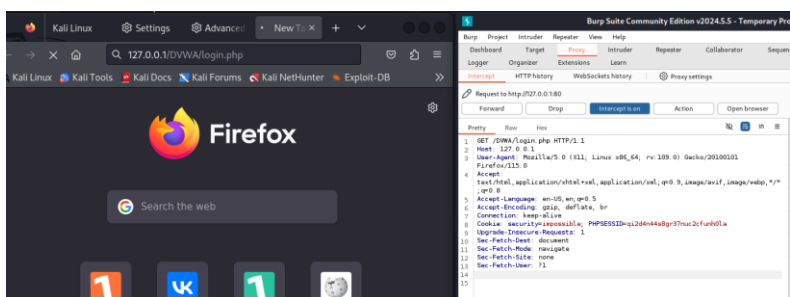


Настройка параметров



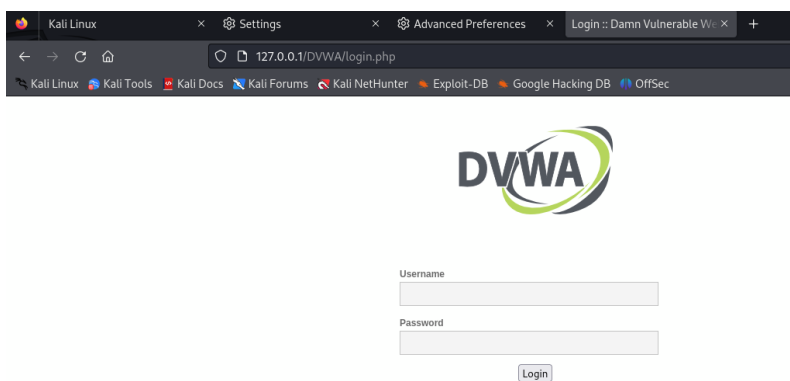
Настройка параметров

Пытаюсь зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:010]).



Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:011] и [-@fig:012]).

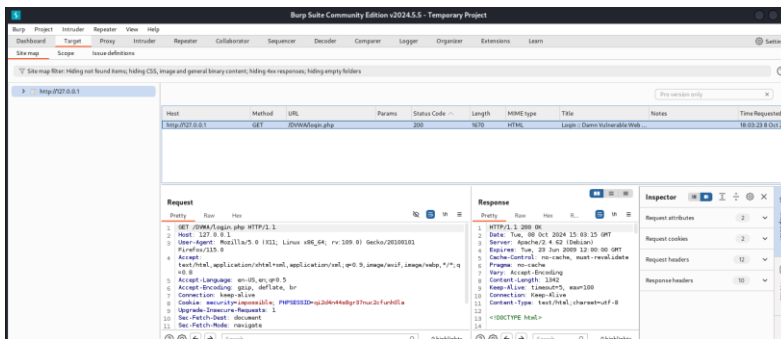


Страница авторизации



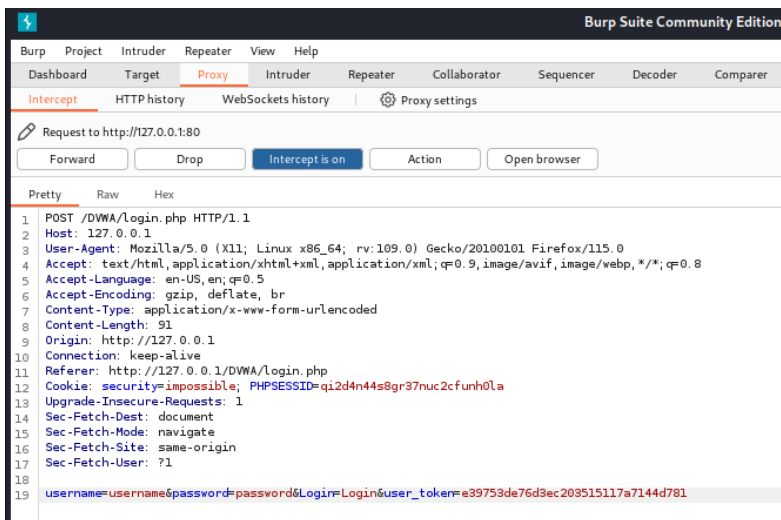
Изменение запроса

История запросов хранится во вкладке Target (рис. [-@fig:013]).



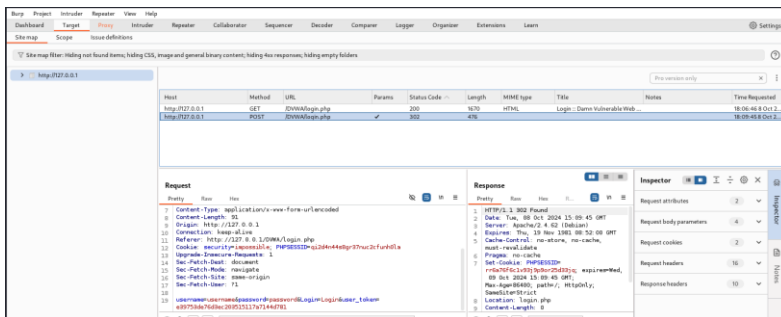
История запросов

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:014]).



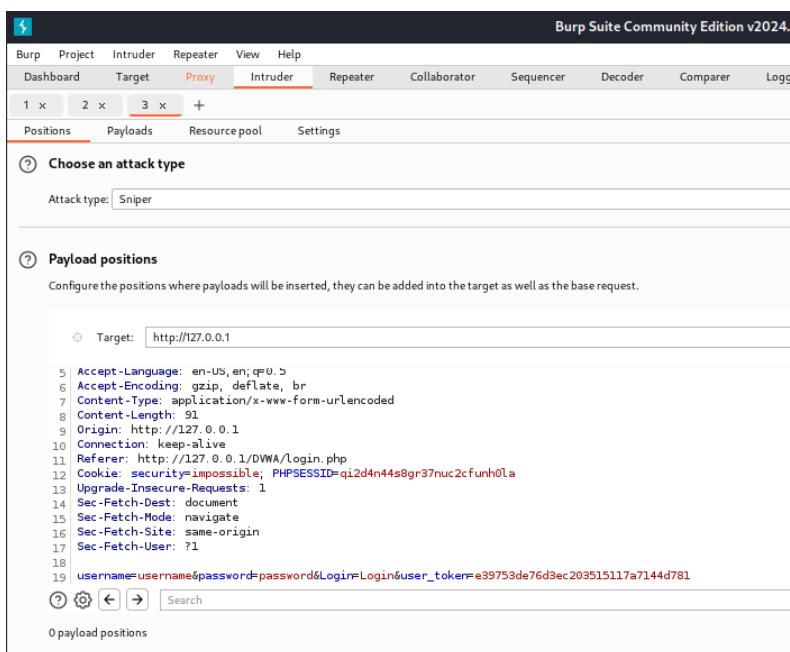
Ввод случайных данных

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:015]).



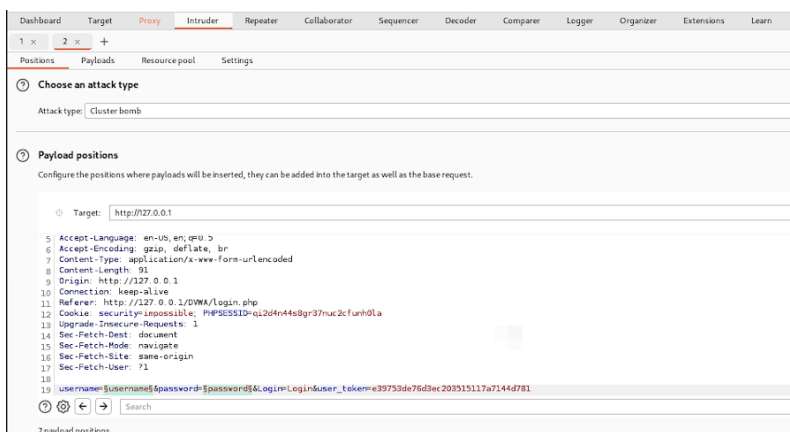
POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:016]).



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:017]).



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:018]).

① Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 6
Payload type: Simple list Request count: 24

① Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste admin
Load ... password
Remove day0810
Clear bbbb
Deduplicate v15
Add 447694

Add from list ... (Pro version only)

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:019]).

Burp Suite Community Edition v2024.5.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

1 x 2 x +

Positions Payloads Resource pool Settings

① Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 4
Payload type: Simple list Request count: 24

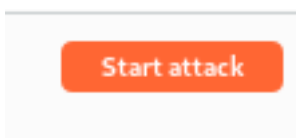
① Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste admin
Load ... password
Remove word
Clear v12
Deduplicate

Add Enter a new item
Add from list ... (Pro version only)

Второй Simple list

Запускаю атаку (рис. [-@fig:020]) и начинаю подбор (рис. [-@fig:021]).



Запуск атаки

Attack - Save

2. Intruder attack of http://127.0.0.1

Attack Save

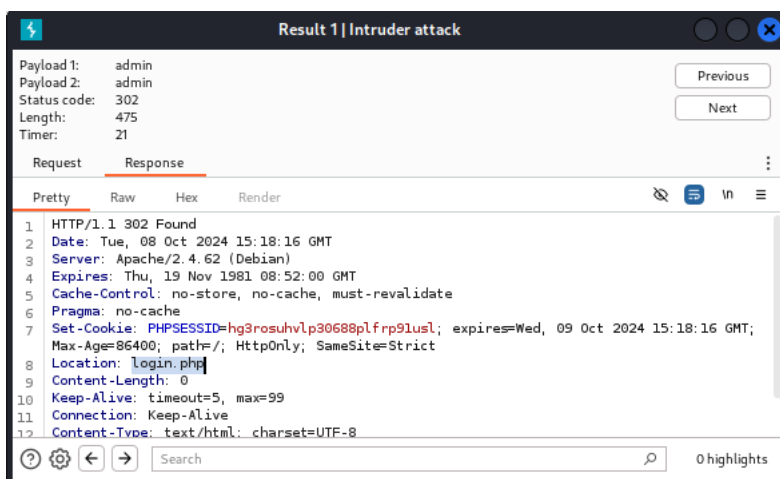
Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
16	day0810	word	202	14			476	
17	bbbb	word	202	13			476	
18	v15	word	202	17			476	
19	447694	word	202	24			476	
20	admin	v12	202	9			476	
21	password	v12	202	15			476	
22	day0810	v12	202	16			476	
23	bbbb	v12	202	17			476	
24	v15	v12	202	21			476	
25	447694	v12	202	18			476	

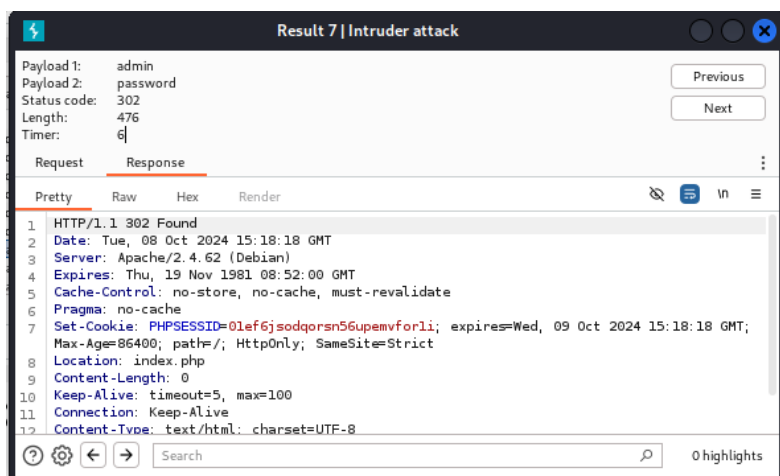
Подбор логина и пароля

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит (рис. [-@fig:022]).



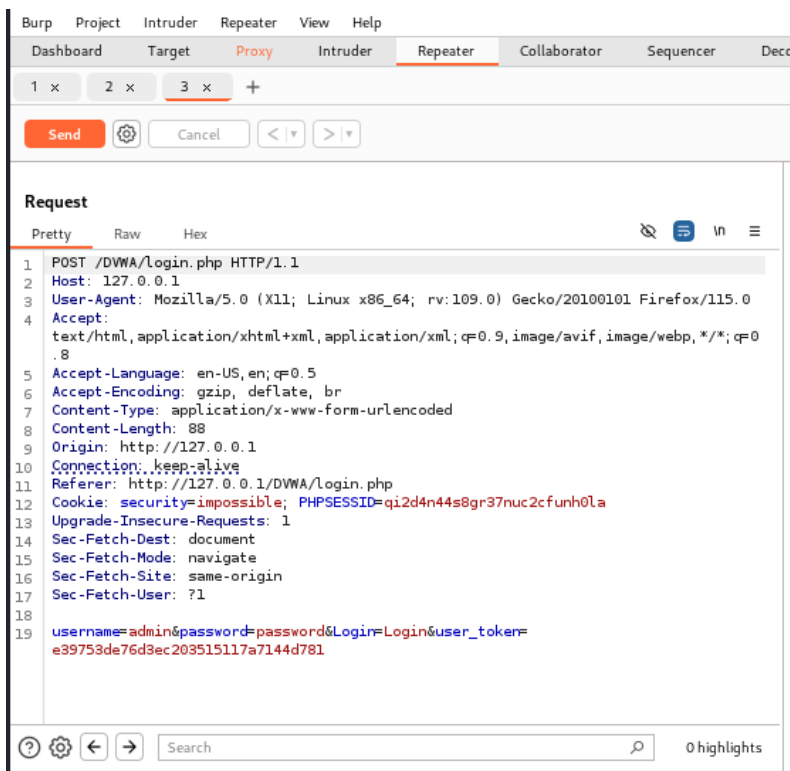
Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [-@fig:023]).



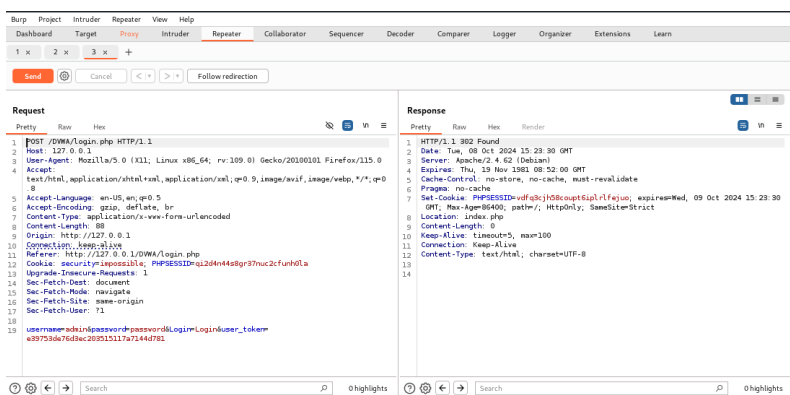
Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater”. Переходим во вкладку “Repeater” (рис. [-@fig:024]).



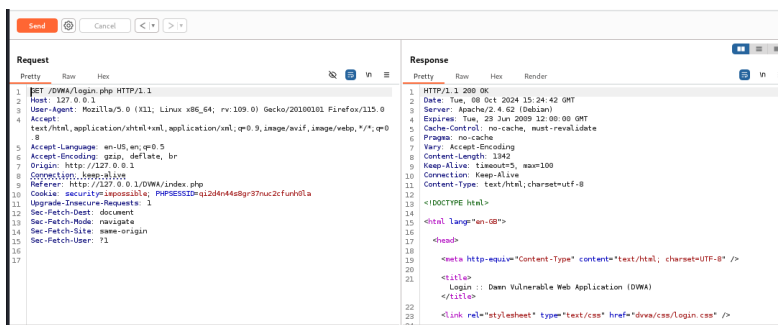
Вкладка Repeater после доп. проверки результата

Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. [-@fig:025]).



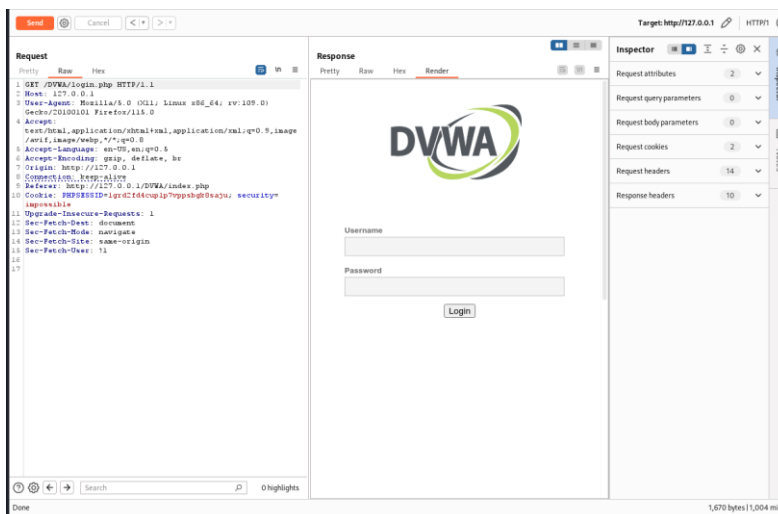
Окно Response

После нажатия на Follow redirection, получим неcompiled html код в окне Response (рис. [-@fig:026]).



Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [-@fig:027]).



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.