

Отчет к 5 этапу индивидуального проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

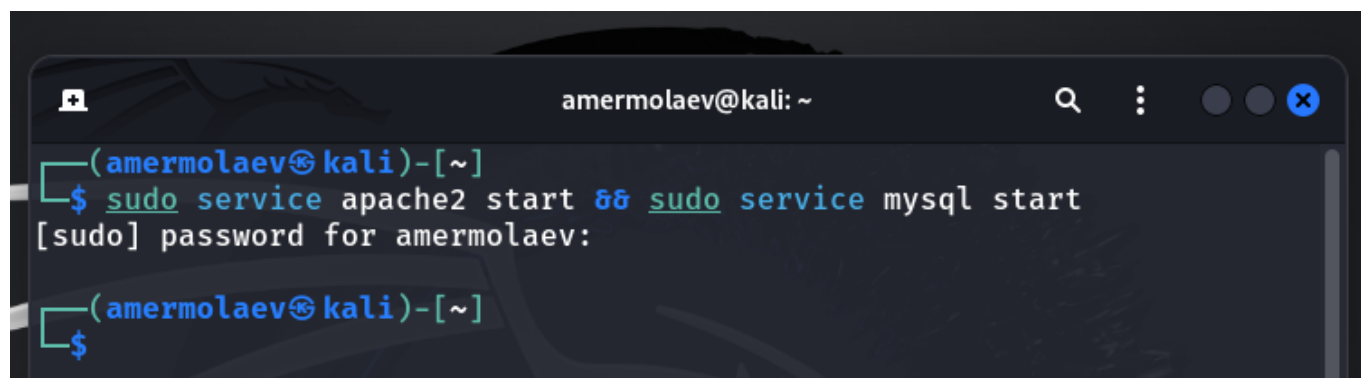
author: Ермолаев А.М.

Цель работы

Приобретение практических навыков по использованию инструмента Burp Suite - набором мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения.

Выполнение работы

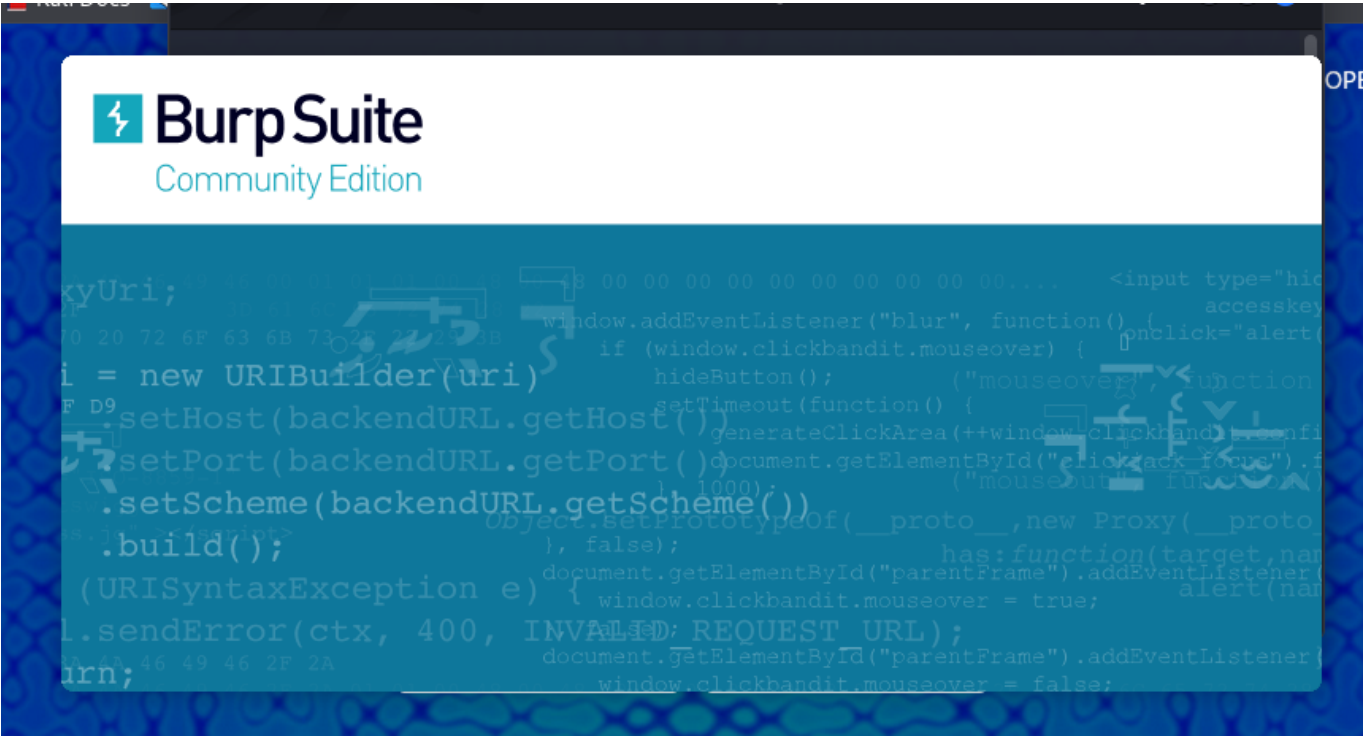
Для работы приложения запустим сервисы Apache2 и MySQL:



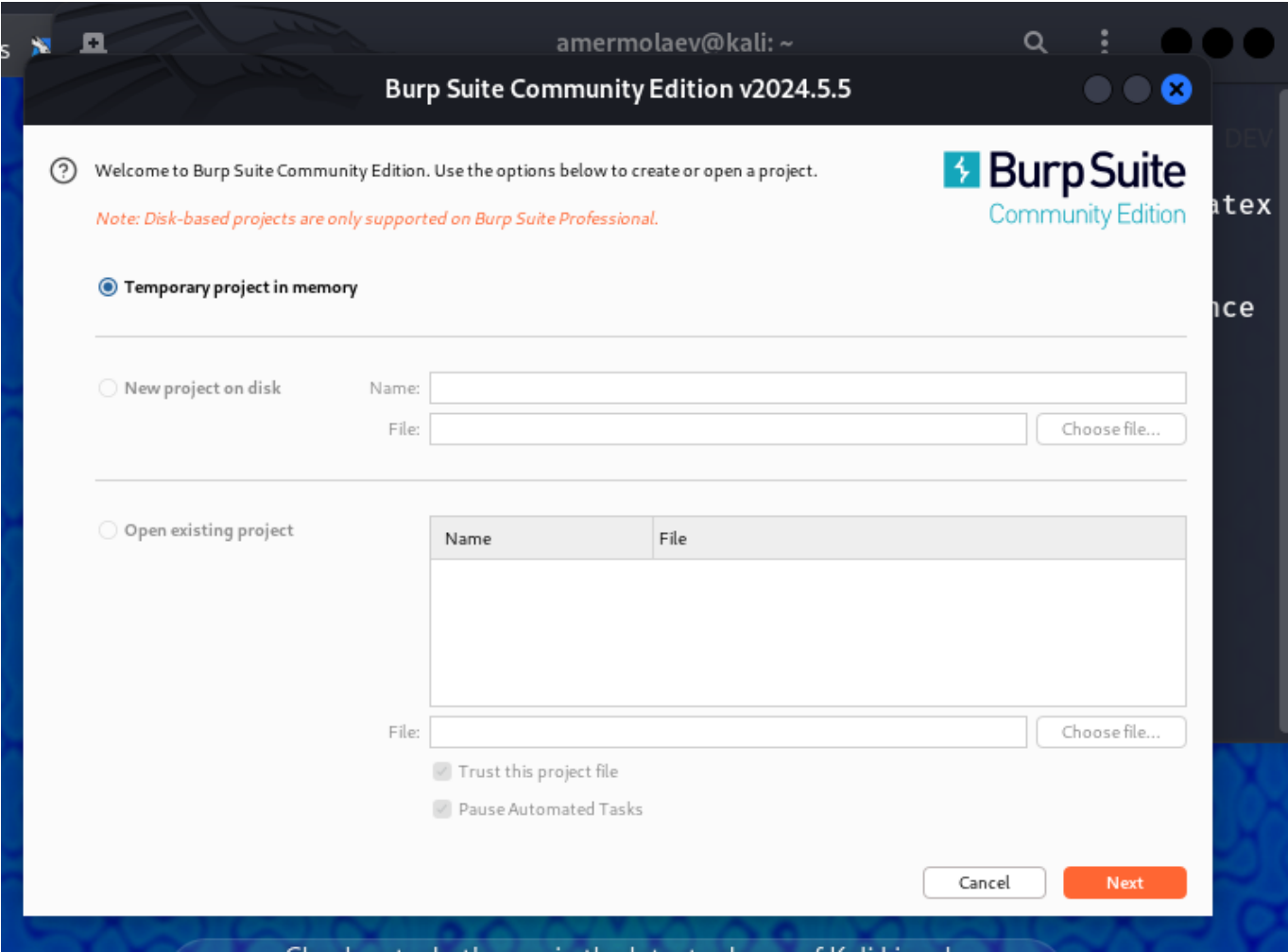
```
amermolaev@kali: ~  
[amermolaev@kali]~  
$ sudo service apache2 start && sudo service mysql start  
[sudo] password for amermolaev:  
[amermolaev@kali]~  
$
```

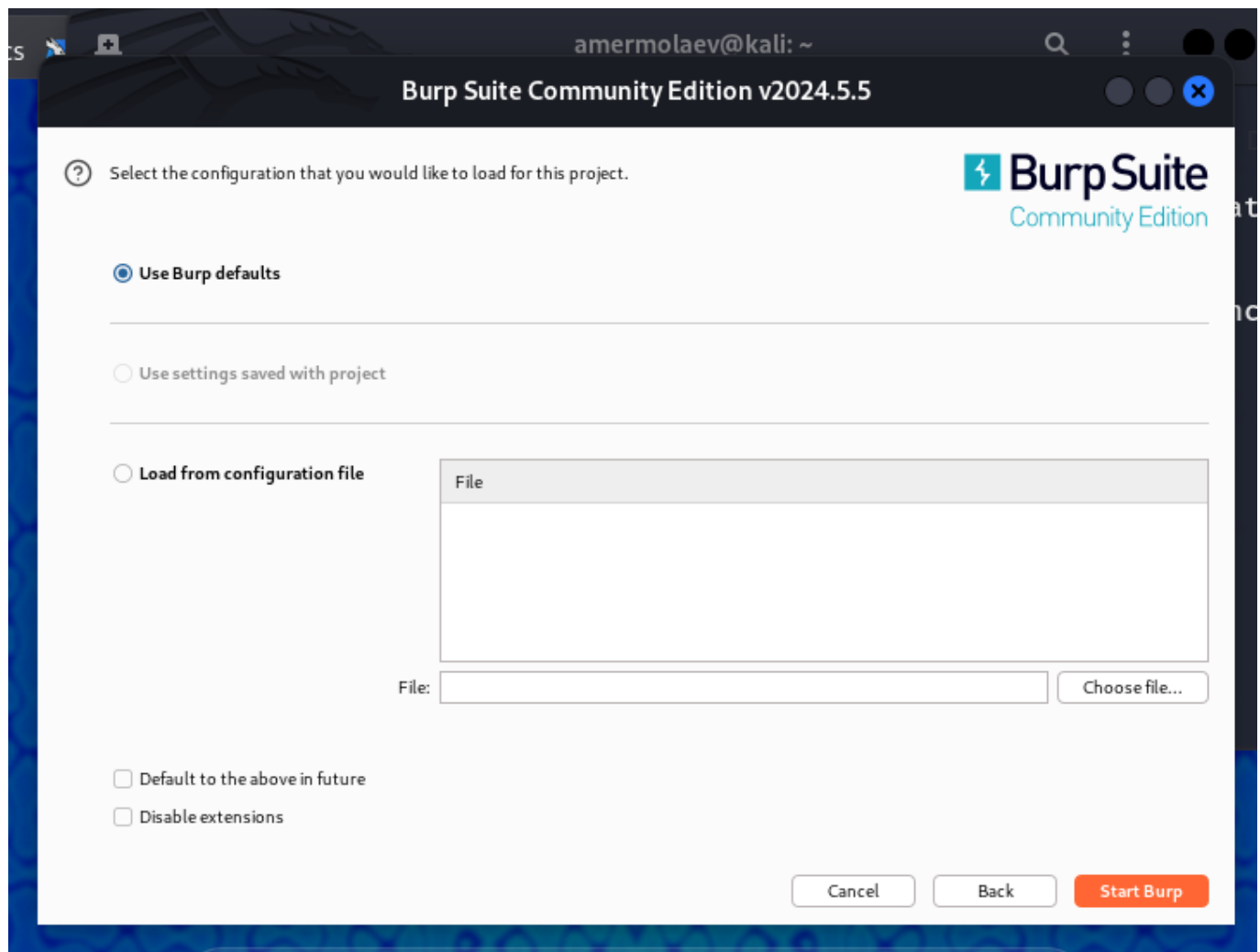
Теперь запустим Burp Suite командой

```
barpsuit
```

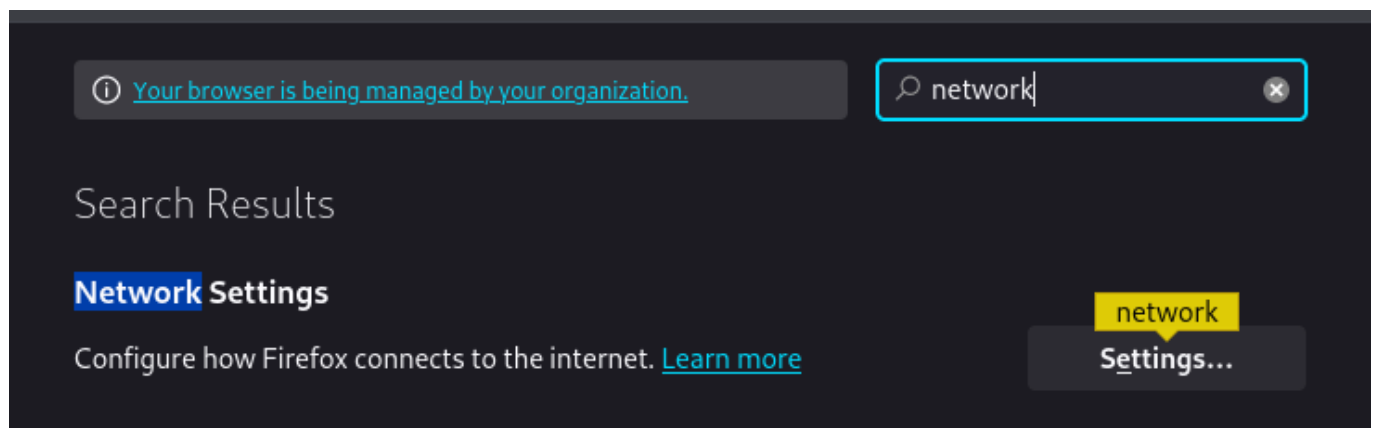


Создадим проект в оперативной памяти и выберем настройки по умолчанию:

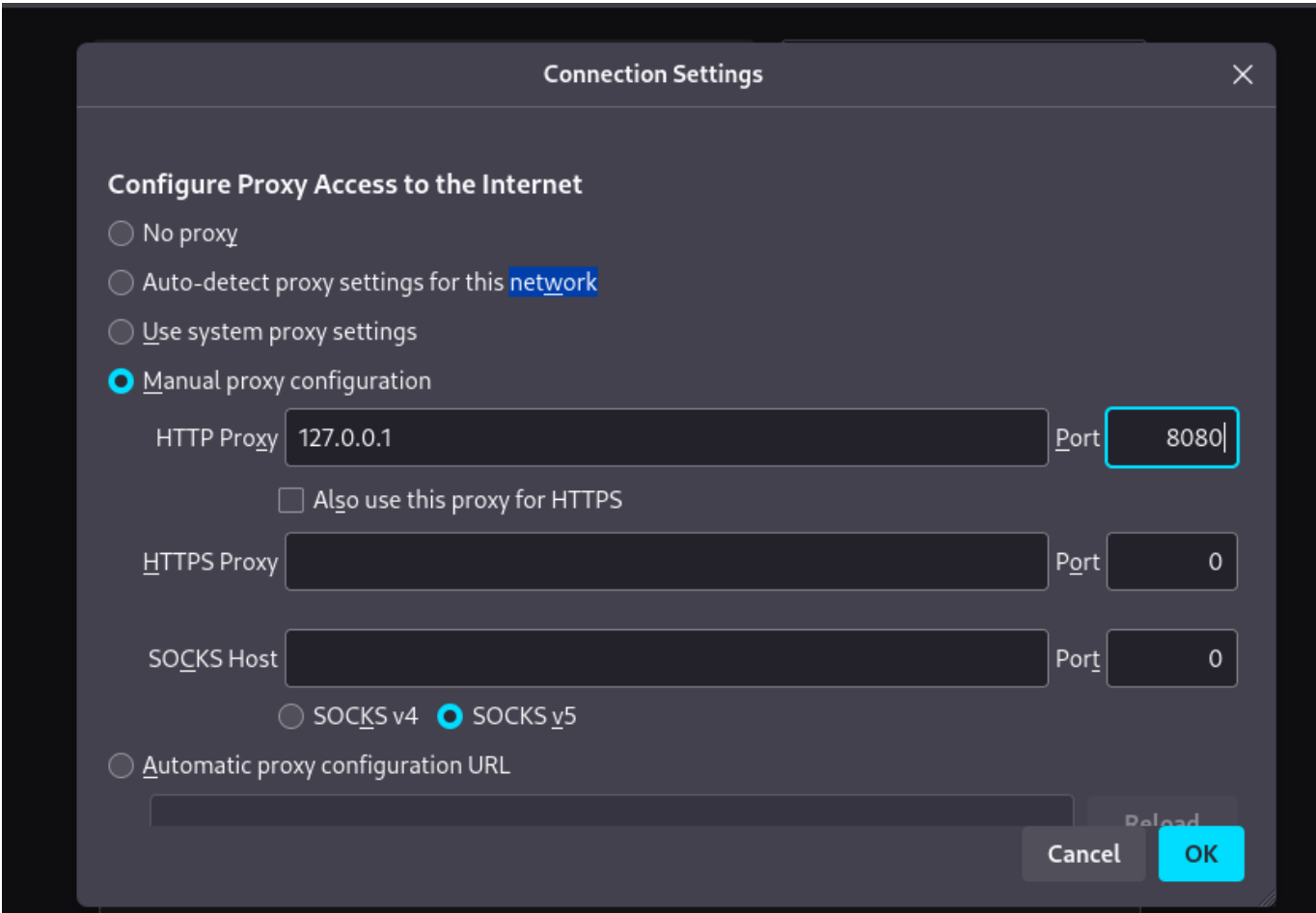




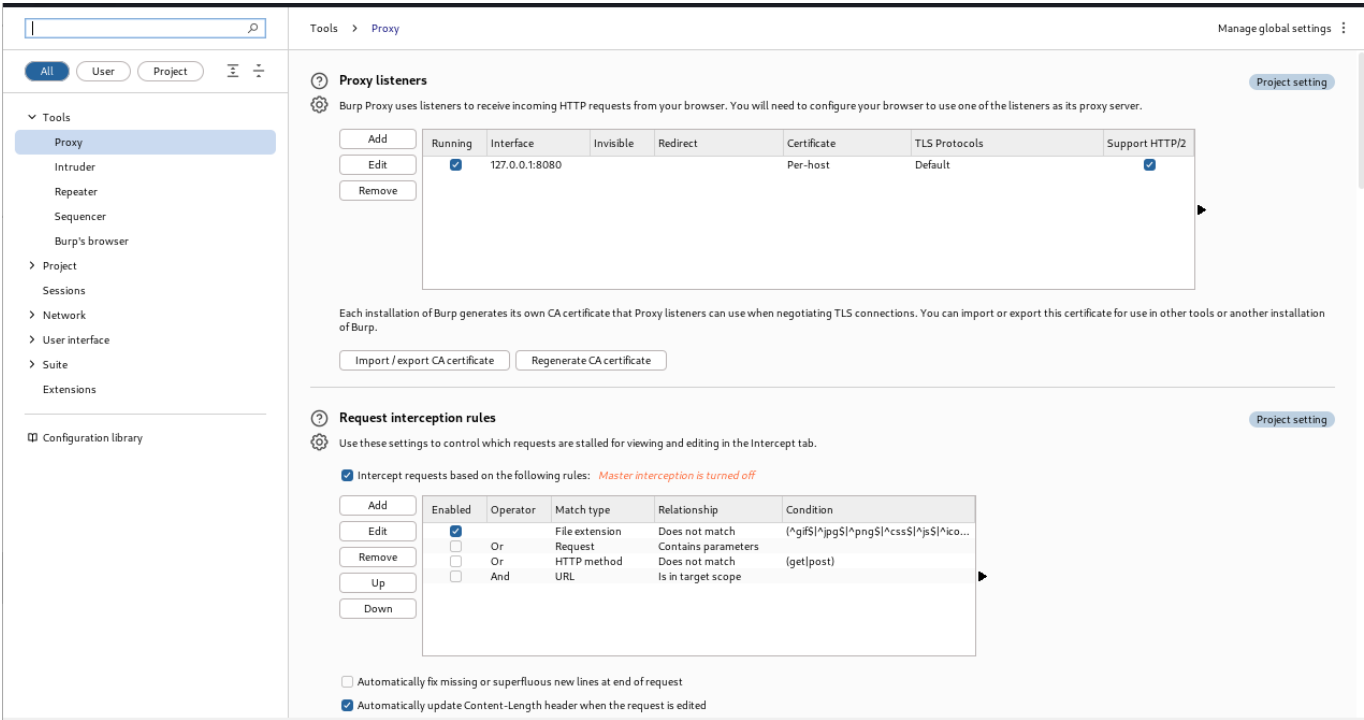
Теперь для интеграции с браузером произведем его настройки в разделе **Settings**



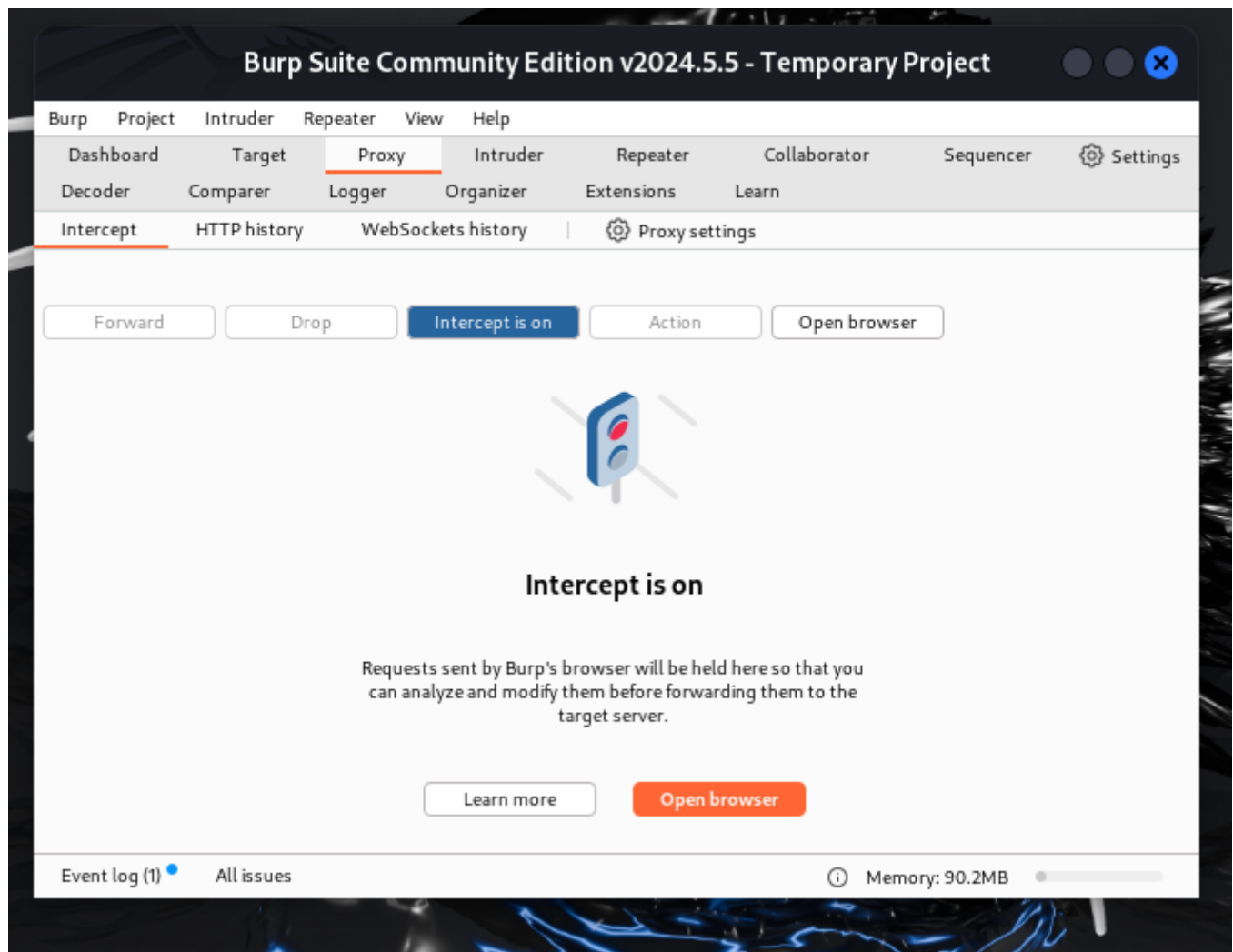
Настроим прокси:



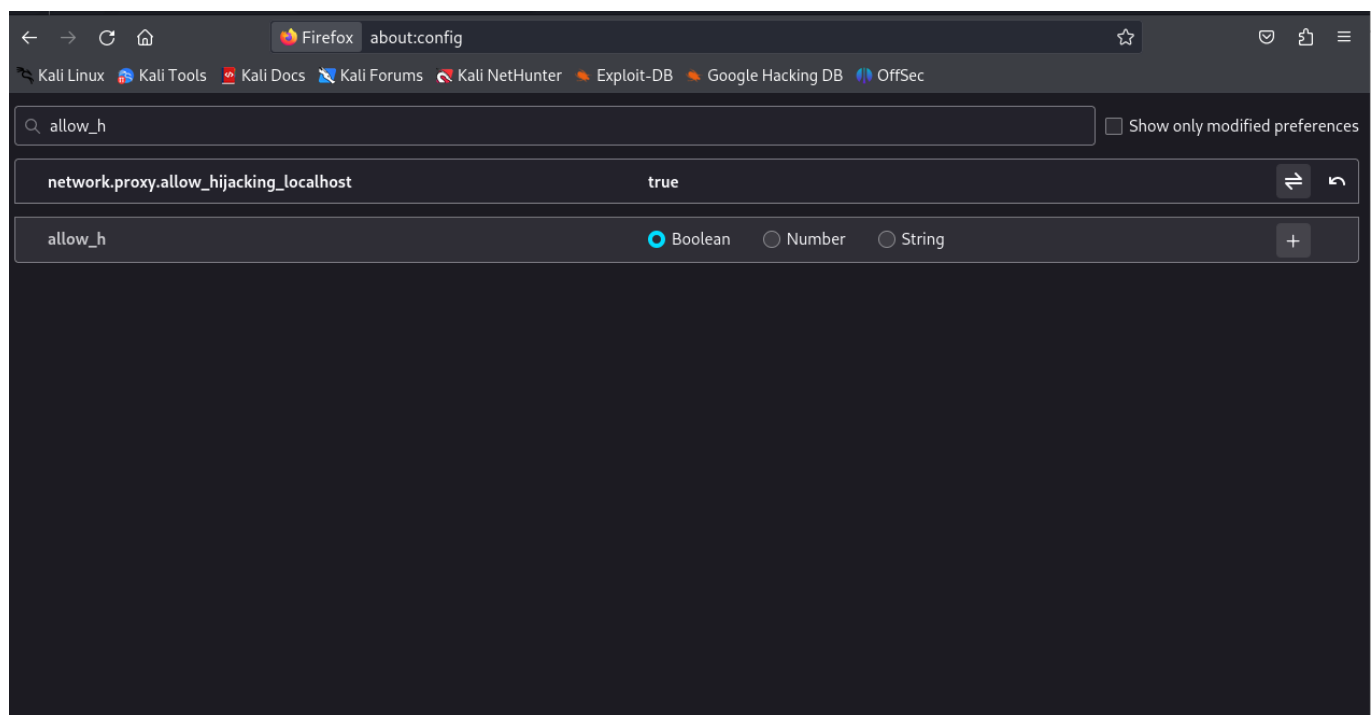
Теперь перейдем в Burp Suite и проверим настройки страницы и прокси:



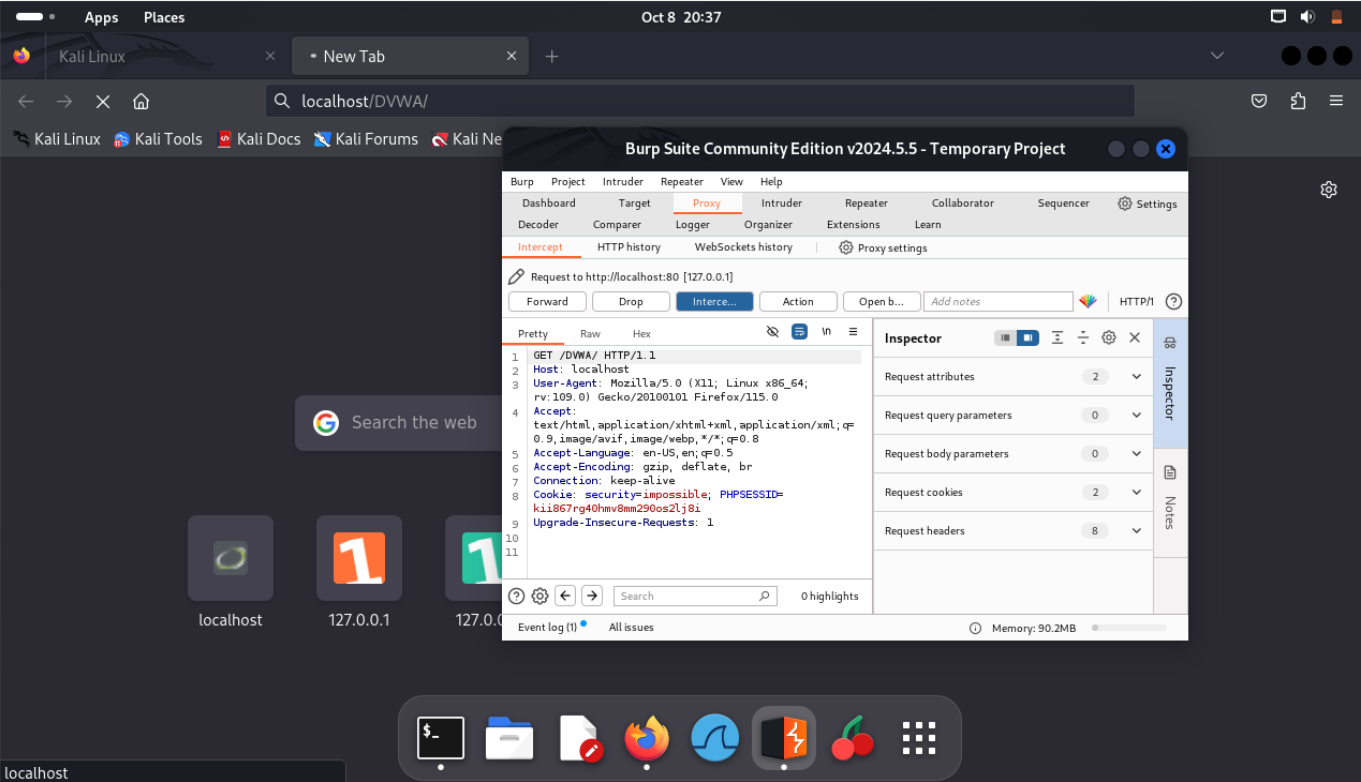
Перейдем во вкладку **Proxu** и включим внедрение Burp Suite:



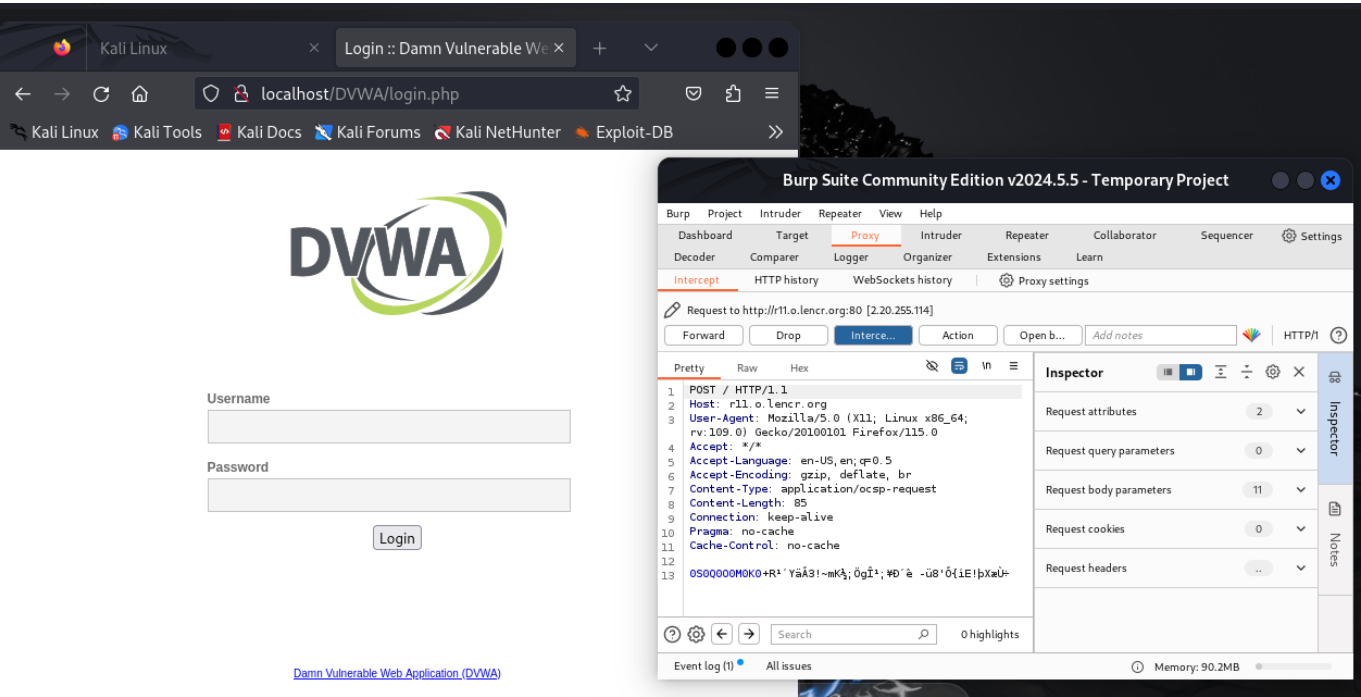
Также не забудем задать переменной `network.allow_hijacking_localhost` значение `true`:



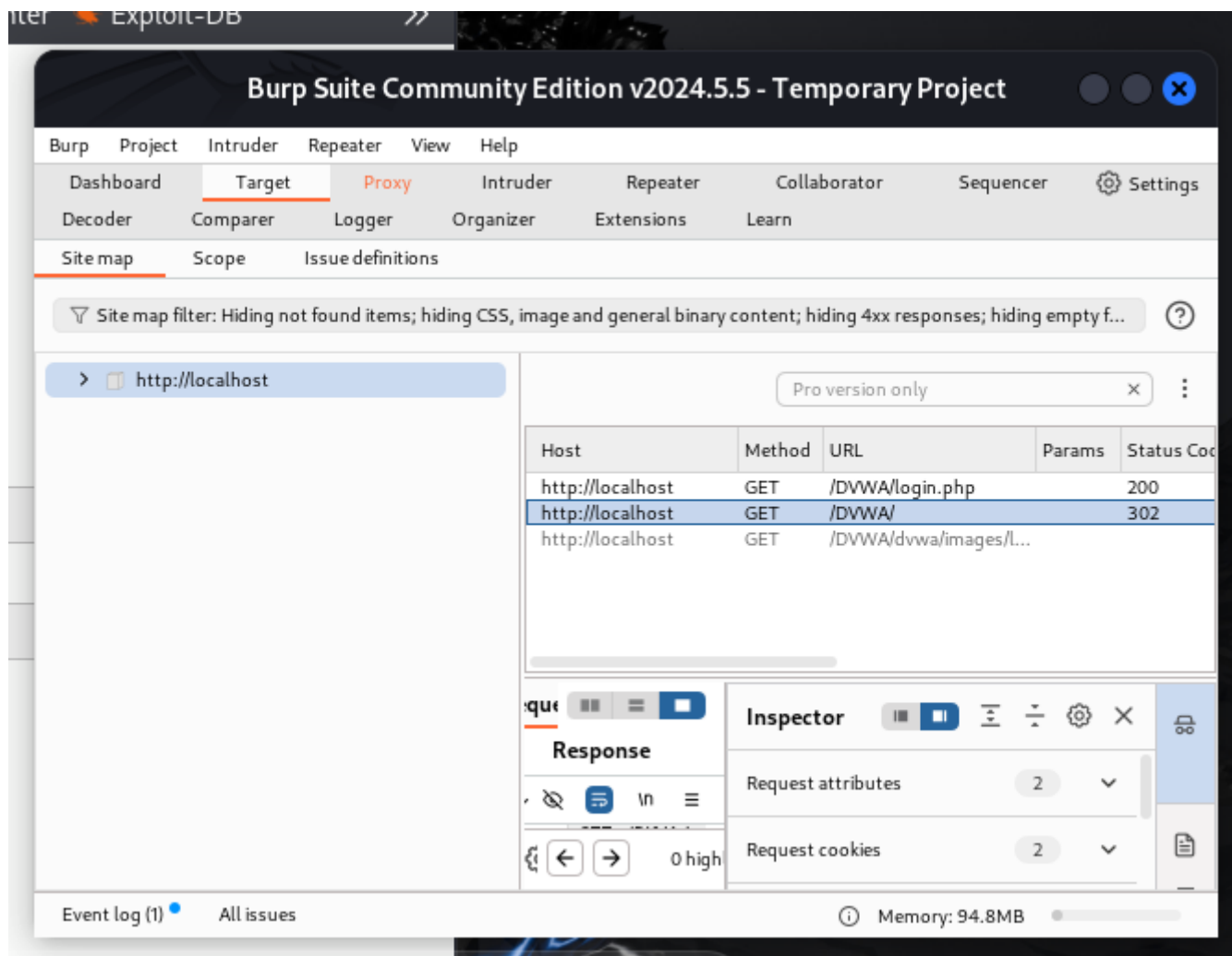
Перейдем по адресу `http://localhost/DWVA/`. Страница загружается, а во вкладке **Proxy** появляется захваченный запрос:



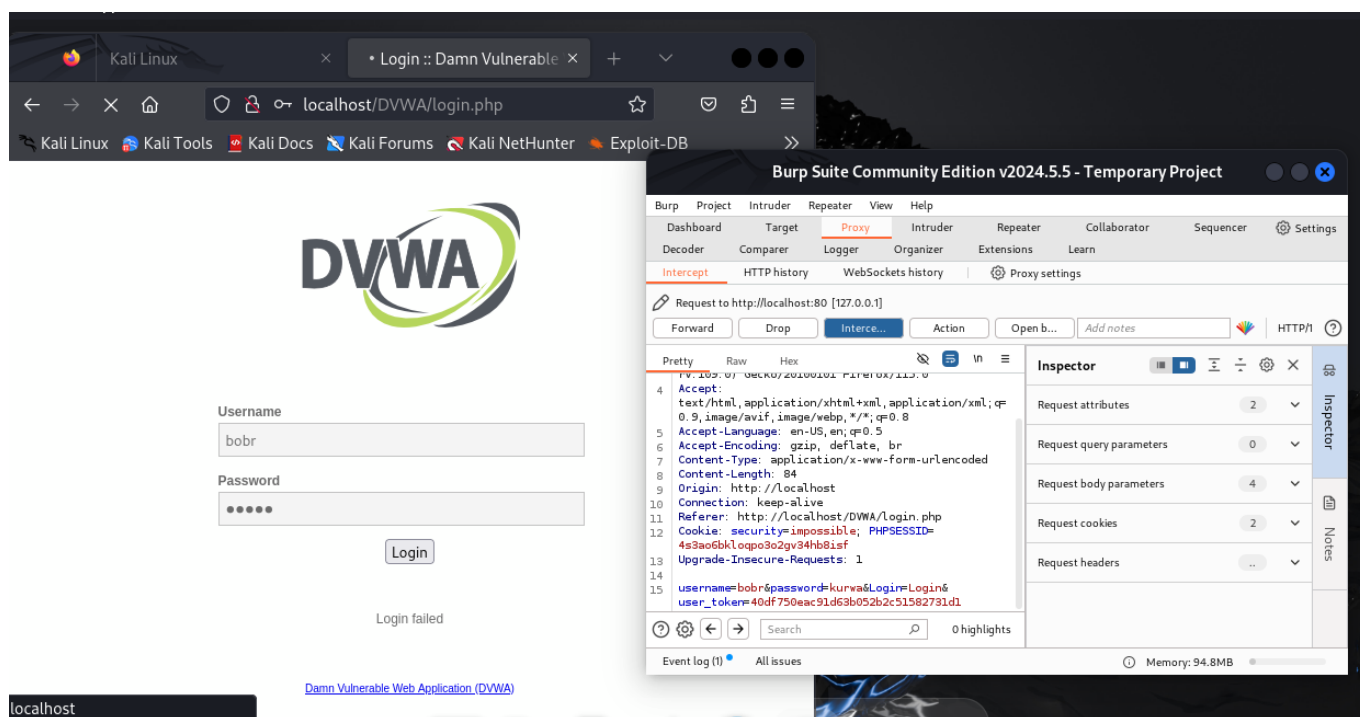
Нажмем кнопку **Forward**, чтобы загрузить страницу:



Все запросы можно найти в разделе **Target**:

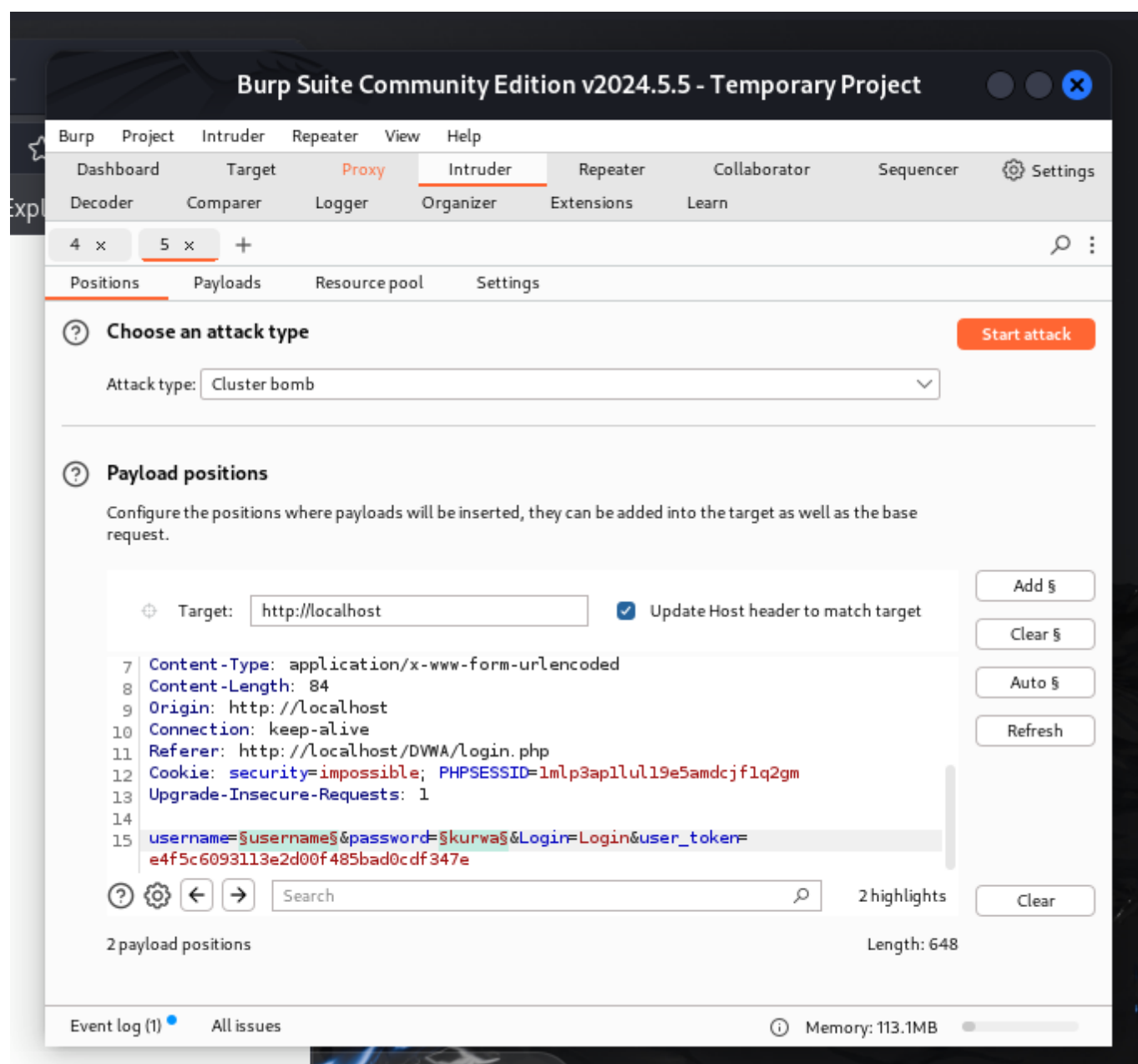


Попробуем ввести невалидные данные в форму нажмем кнопку **Login**. В окне Burp Suite появятся введенные в поля формы значения:

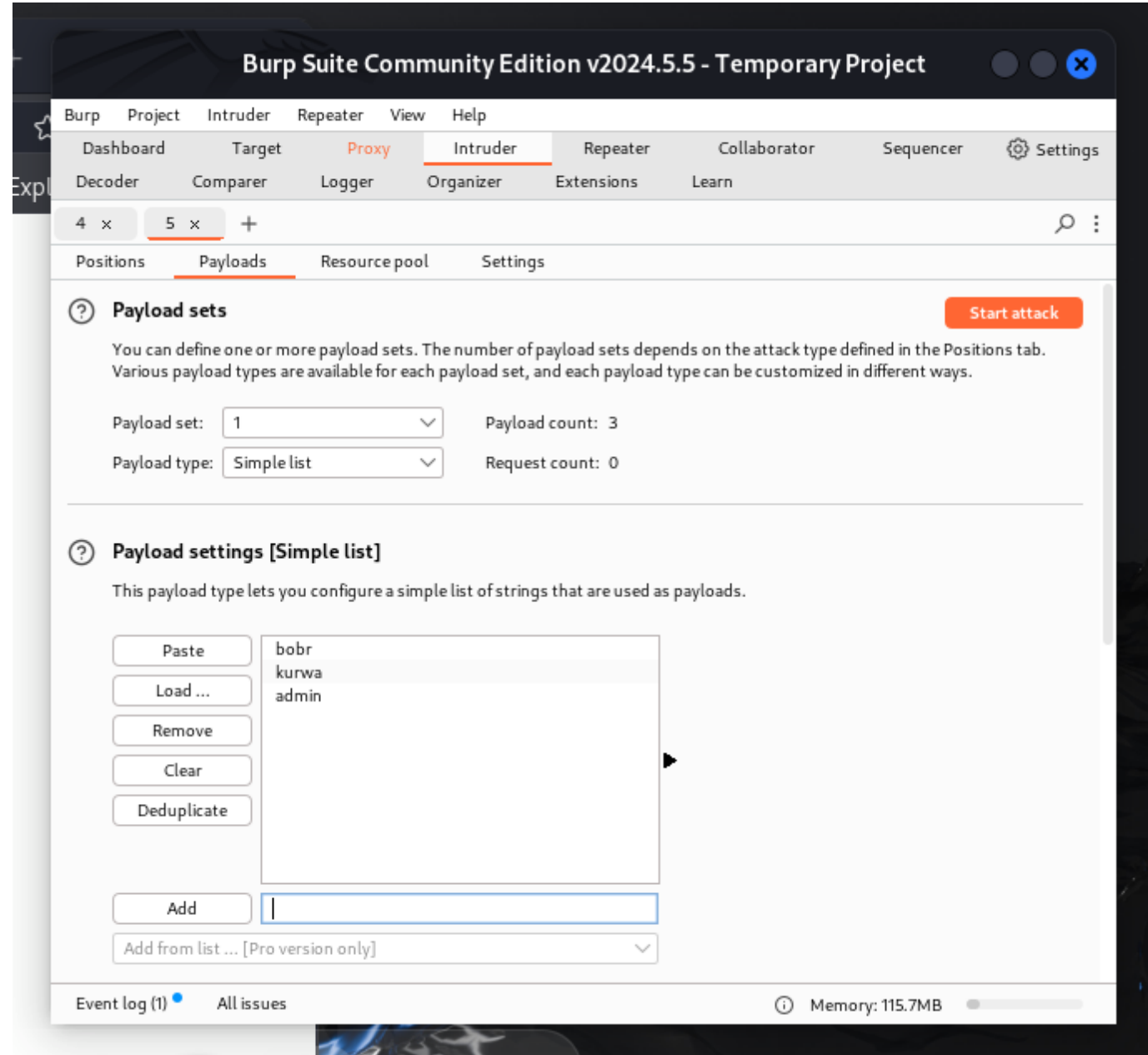


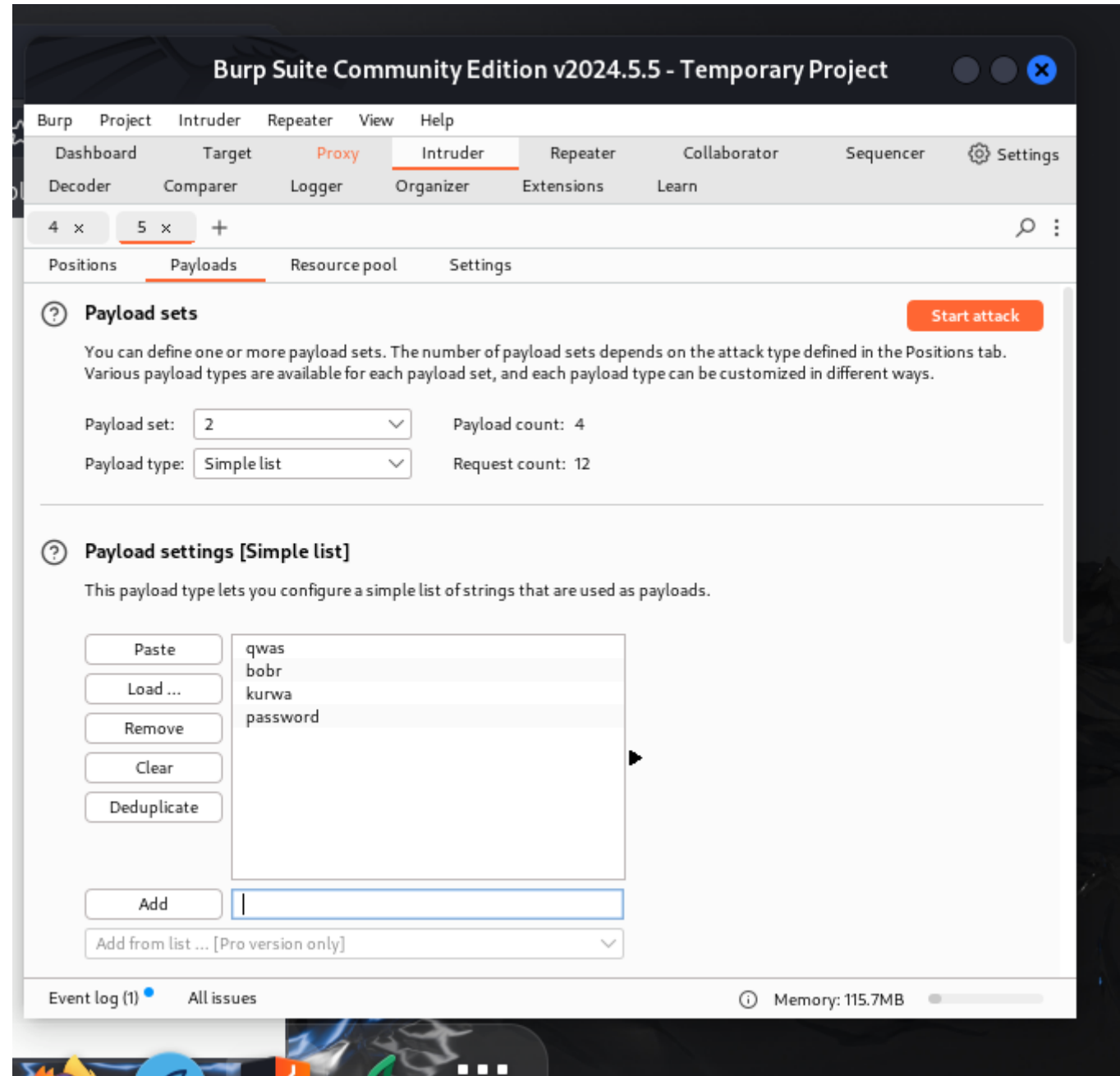
Попробуем подобрать логин пароль для аутентификации. Для этого в разделе **Target** нажмем на запрос правой кнопкой мыши и в меню выберем **Send to intruder**.

Во вкладке **Intruder** выберим тип атаки и **Cluster Bomb** и выделим значения специальным символом:



Заполним произвольные значения логинов и паролей в двух списках:

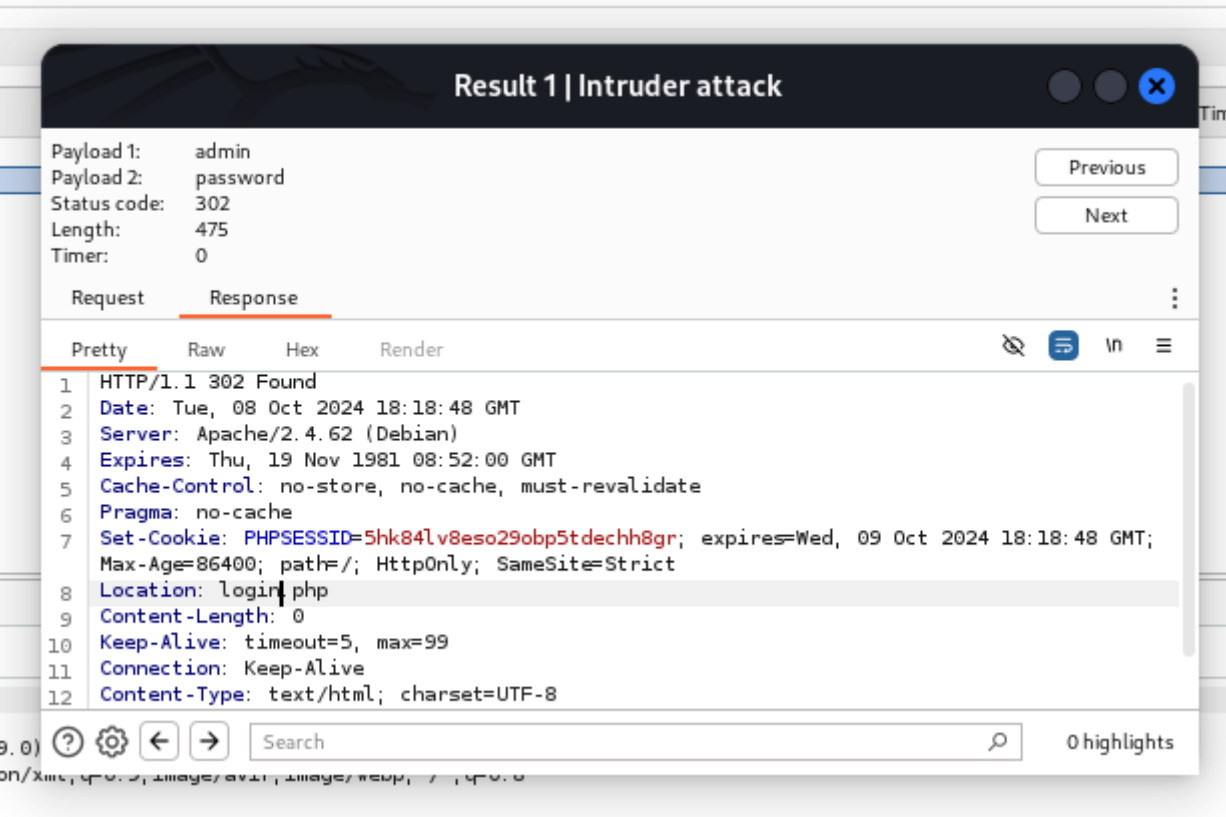




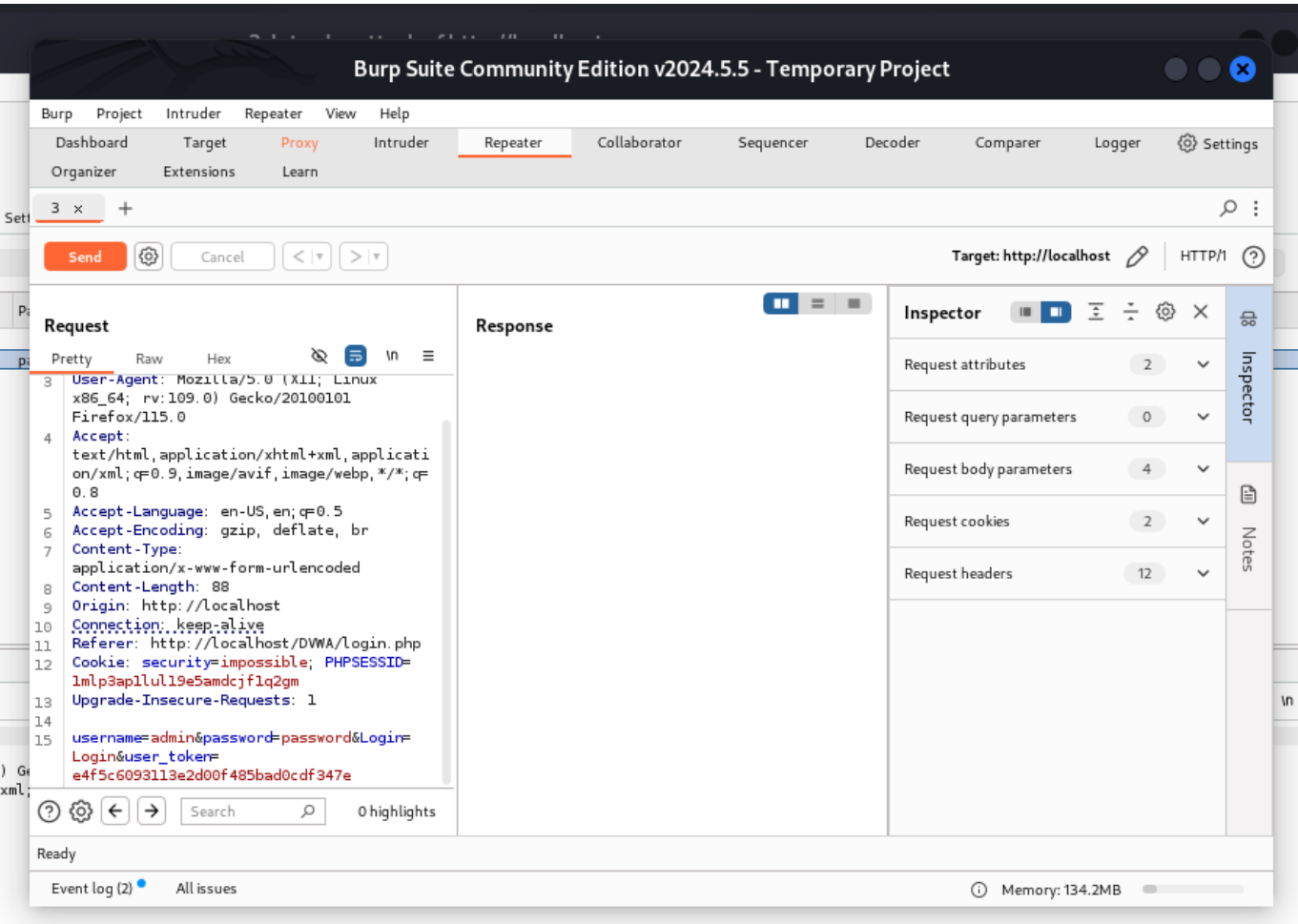
и нажмем кнопку **Start attack**:

2. Intruder attack of http://localhost									
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	
0			302	0			476		
1	bobr	qwas	302	0			475		
2	kurwa	qwas	302	0			476		
3	admin	qwas	302	22			475		
4	bobr	bobr	302	11			476		
5	kurwa	bobr	302	2			475		
6	admin	bobr	302	0			476		
7	bobr	kurwa	302	0			475		
8	kurwa	kurwa	302	2			476		
9	admin	kurwa	302	13			475		
10	bobr	password	302	1			476		
11	kurwa	password	302	0			475		
12	admin	password	302	3			476		

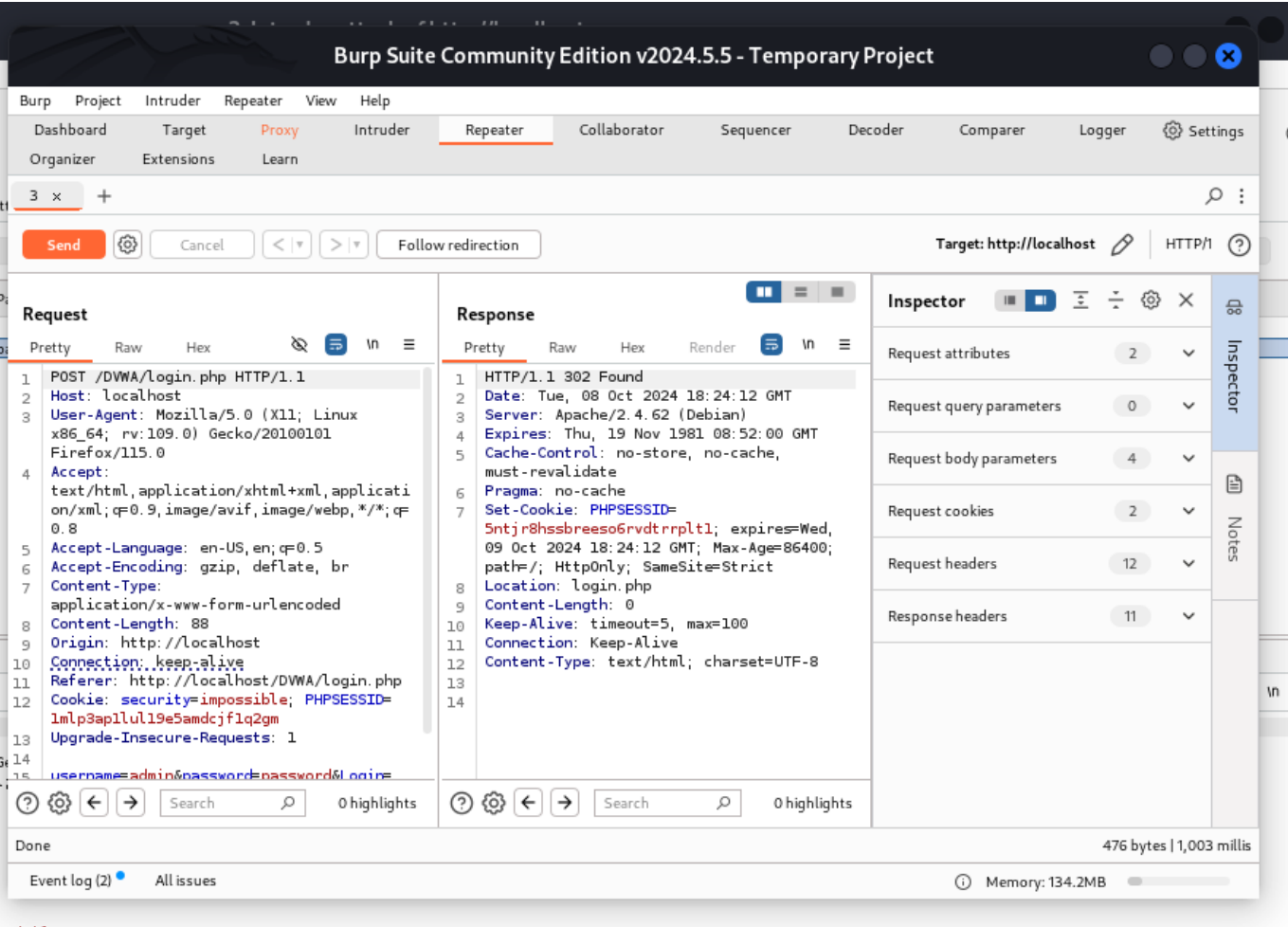
Выберем верную пару логина и и пароля (admin и password), увидев имя скрипта, отработываемый при отправке формы:

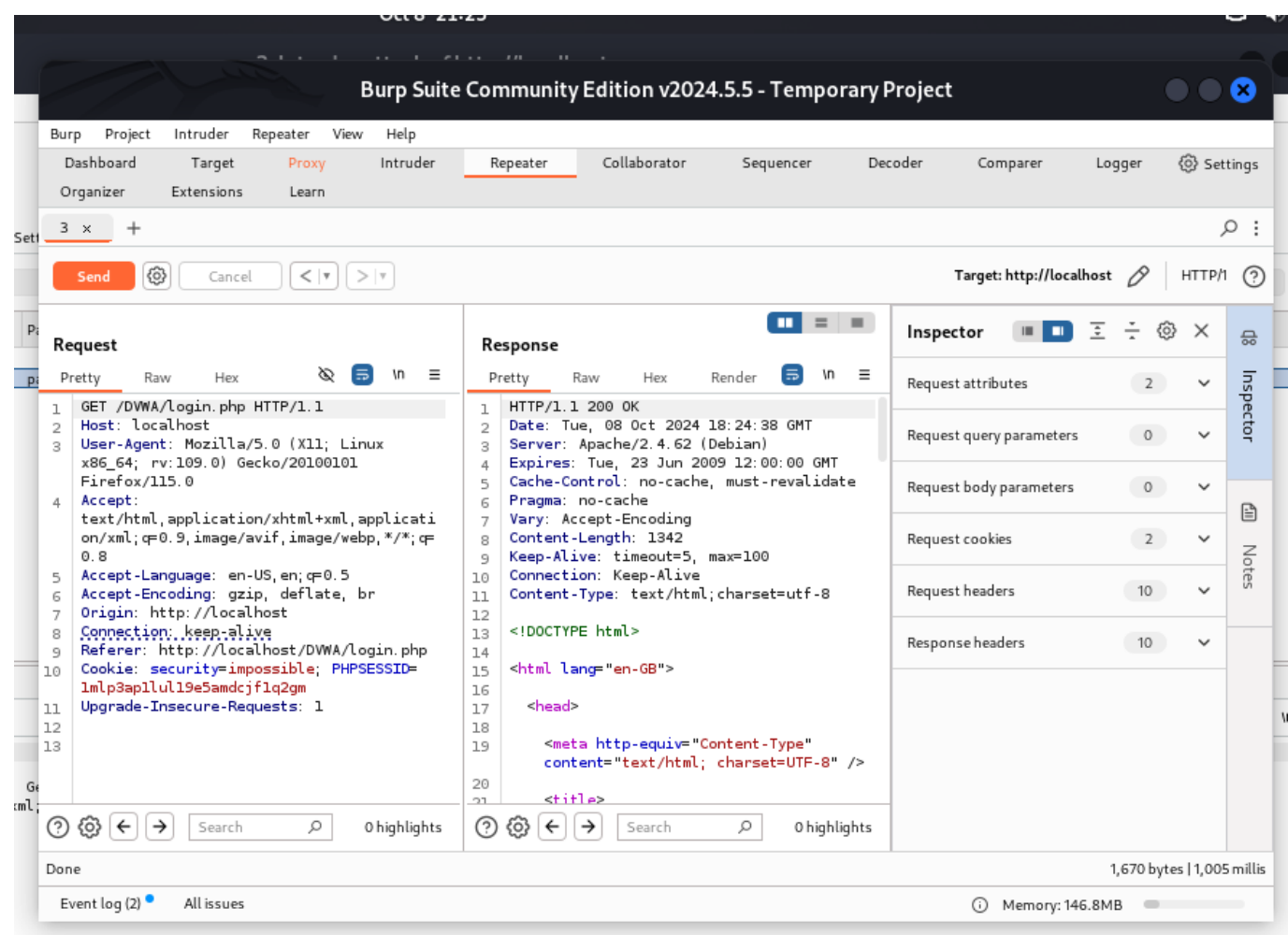


Откроем данный запрос в разделе **Repeater** и нажмем кнопку **Send**:

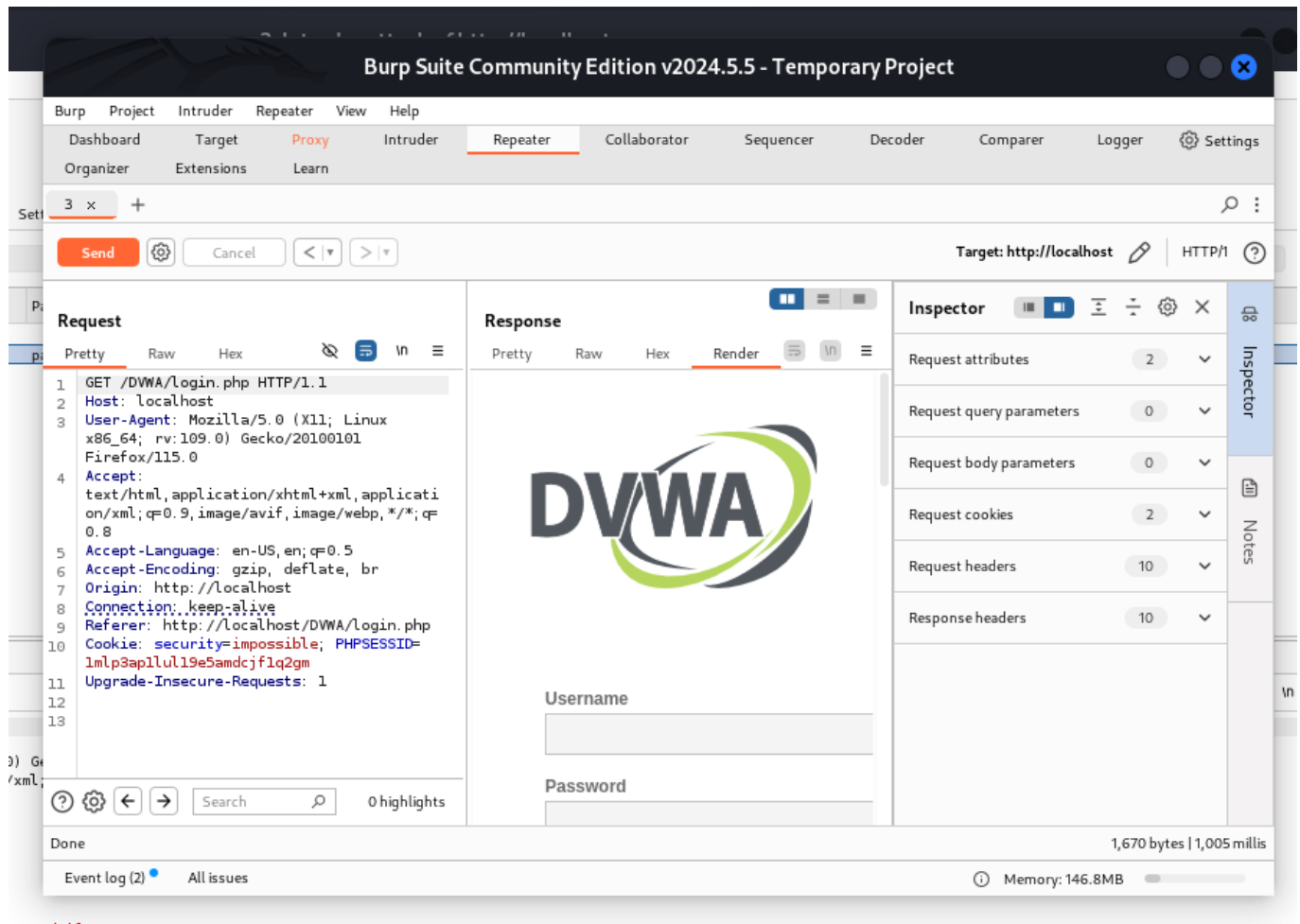


В правом окне увидим знакомый нам вывод, однако, нажав кнопку **Follow redirections**, получим ответ с разметкой страницы с формой авторизации:





Отобразим ее в разделе **Render**:



Вывод

В рамках выполнения работы я приобрел практические навыки по использованию инструмента Burp Suite - набора мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения.

Список литературы

- <https://github.com/digininja/DVWA?tab=readme-ov-file>
- <https://www.kali.org/>
- https://habr.com/ru/companies/yandex_praktikum/articles/770668/
- <https://blog.eldernode.com/configure-burp-suite-on-kali-linux/>