

# **Индивидуальный проект. Этап 5**

**Использование Burp Suite**

Лебедева Ольга Андреевна

# Содержание

<b>Цель работы</b>	<b>4</b>
<b>Теоретическое введение</b>	<b>5</b>
<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>Заключение</b>	<b>11</b>
<b>Библиографическая справка</b>	<b>12</b>

## Список иллюстраций

1	Запуск локального сервера . . . . .	6
2	Запуск Burp Suite . . . . .	7
3	Настройки браузера . . . . .	7
4	Network settings . . . . .	8
5	Settings в Burp Suite . . . . .	8
6	Настройки проху . . . . .	9
7	Установка параметра network.proxy.allow_hijacking_localhost . . . . .	9
8	Захваченный запрос . . . . .	9
9	Изменение запроса . . . . .	10
10	История запросов . . . . .	10

## **Цель работы**

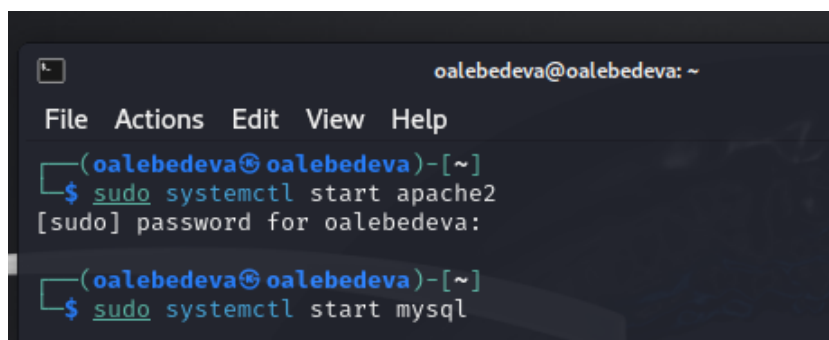
Научиться использовать Burp Suite.

# Теоретическое введение

Burp Suite — это набор инструментов для проведения аудита безопасности веб-приложений. Он позволяет анализировать трафик между клиентом и сервером, обнаруживать уязвимости в приложениях и автоматически создавать эксплойты для их использования. Burp Suite также может использоваться для тестирования на проникновение и мониторинга безопасности сетей[1].

# Выполнение лабораторной работы

Подготовим открытие приложения DVWA. Для этого запустим локальный сервер: См. рис. 1



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

Рис. 1: Запуск локального сервера

Через консоль запускаем инструмент Burp Suite: См. рис. 2

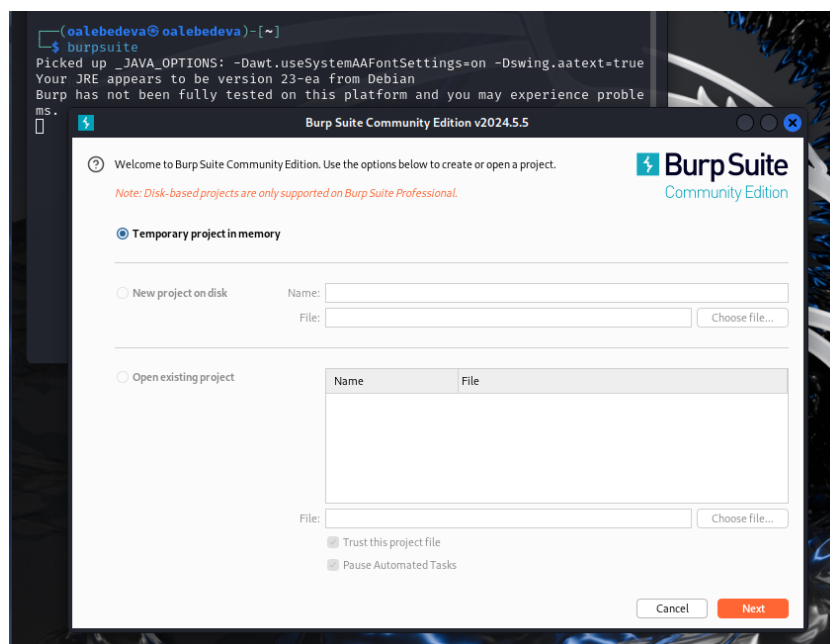


Рис. 2: Запуск Burp Suite

Заходим в настройки браузера в раздел network settings: См. рис. 3

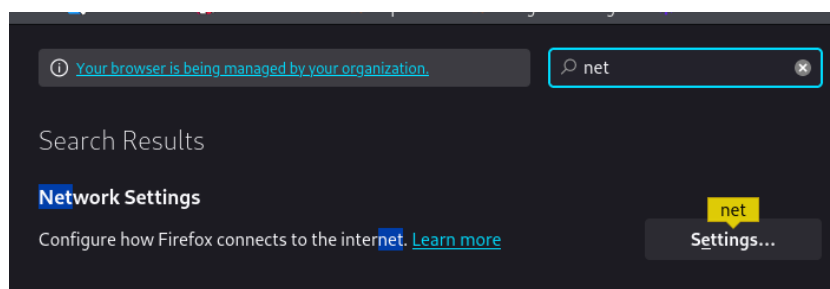


Рис. 3: Настройки браузера

Меняем настройки сервера для возможности работы с проху и захватом данных при помощи Burp Suite: См. рис. 4





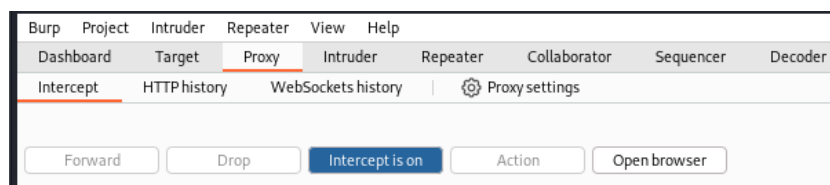


Рис. 6: Настройки проху

В настройках браузера необходимо установить параметр `network.proxy.allow_hijacking_localhost` на значение `true`: См. рис. 7

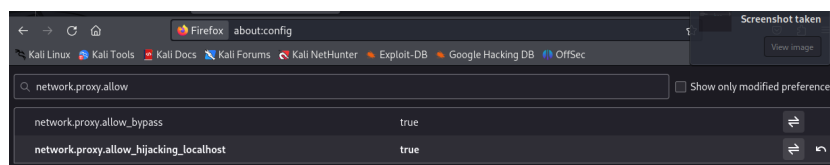


Рис. 7: Установка параметра `network.proxy.allow_hijacking_localhost`

Пробуем зайти на сайт DVWA, и нас сразу перенаправляет в приложение Burp Suite: См. рис. 8

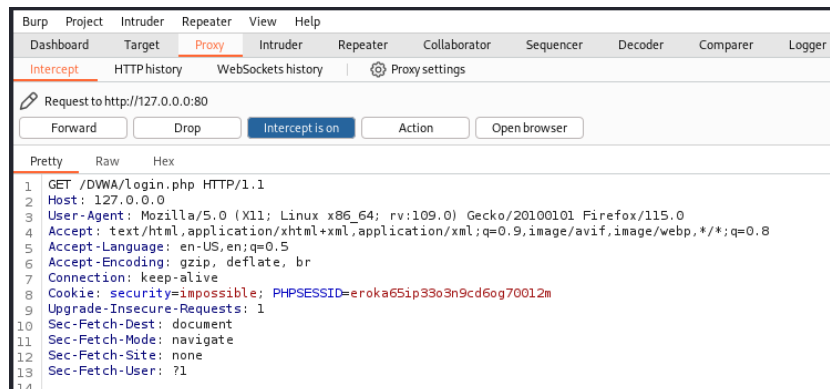


Рис. 8: Захваченный запрос

Нажимаем клавишу `forward`, и скрипт запроса в разделе проху меняется. Теперь загружается и страница авторизации: См. рис. 9



Рис. 9: Изменение запроса

Переходим во вкладку target, там мы можем увидеть историю запросов: См. рис. 10

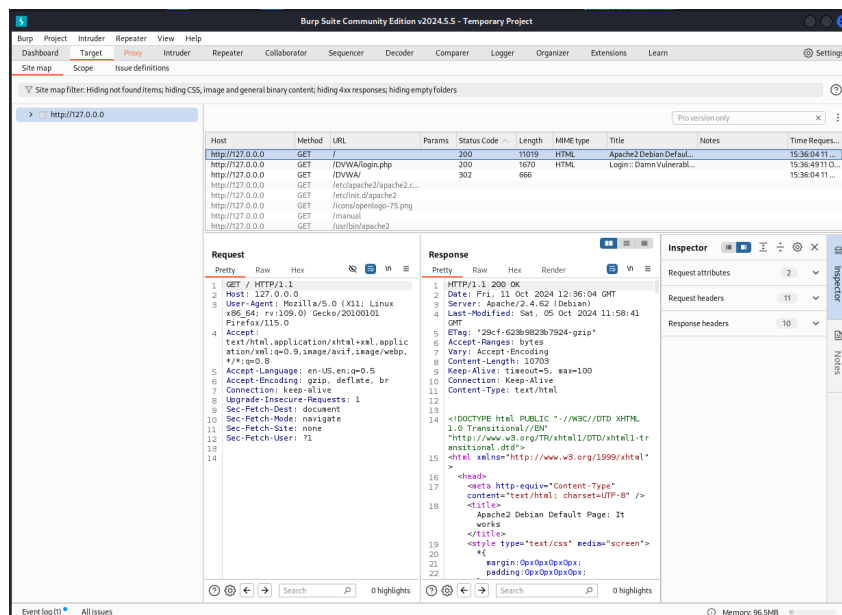


Рис. 10: История запросов

# **Заключение**

Приобрели навыки использования набора инструментов Burp Suite.

## **Библиографическая справка**

[1] Burp Suite: <https://ru.hexlet.io/qna/glossary/questions/что-такое-burp-suite>