

# Индивидуальный проект. Этап 5

## Использование Burp Suite

Петрова Мария Евгеньевна

### Содержание

#### 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

1. Подготовим открытие приложения DVWA. Для этого запустим локальный сервер
2. Через консоль запускаем инструмент Burp Suite
3. Заходим в настройки браузера в раздел network settings
4. Меняем настройки сервера для возможности работы с прокси и захватом данных при помощи Burp Suite
5. Заходим в раздел settings в Burp Suite и настраиваем параметры
6. Для последующей работы изменяем настройки в разделе proxy. Ставим “intercept is on”

7. В настройках браузера необходимо установить параметр `network.proxy.allow_hijacking_localhost` на значение `true`
8. Пробуем зайти на сайт DVWA, и нас сразу перенаправляет в приложение Burp Suite
9. Нажимаем клавишу `forward`, и скрипт запроса в разделе `proxy` меняется. Теперь загружается и страница авторизации
10. Переходим во вкладку `target`, там мы можем увидеть историю 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>