Индивидуальный проект. Этап №5

Основы инфомационной безопасности

Астраханцева А. А.

Содержание

Список иллюстраций

1 Цель работы

Знакомство с инструментами Burp Suite и их применение.

2 Теоретическое введение

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений.

3 Выполнение

Находим Burp Suite среди встроенных приложения и открываем его (рис. 3.1).

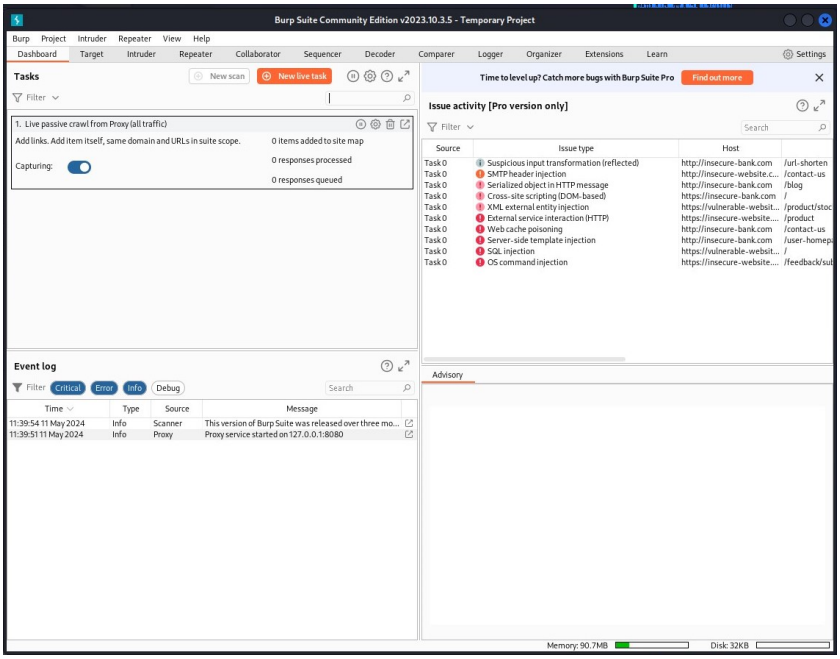

Рис. 3.1: Окно Burp Suite

В качестве знакомства работы с Burp, я буду использовать его для взлома учетных данных, что-бы получить доступ к приложению DVWA. Для этого нам сначала потребуется настроить прокси-сервер и убедиться, что для IP установлено значение localhost IP, а.номер порта — 8080.Откроем вкладку Proxy (Прокси). На нейбудет несколько вложенных вкладок.

Откроем вкладку Intercept (Перехват) и в первую очередь убедимся, что функция перехвата включена (нажата кнопка Intercept is on (Перехват.на))(рис. 3.2).

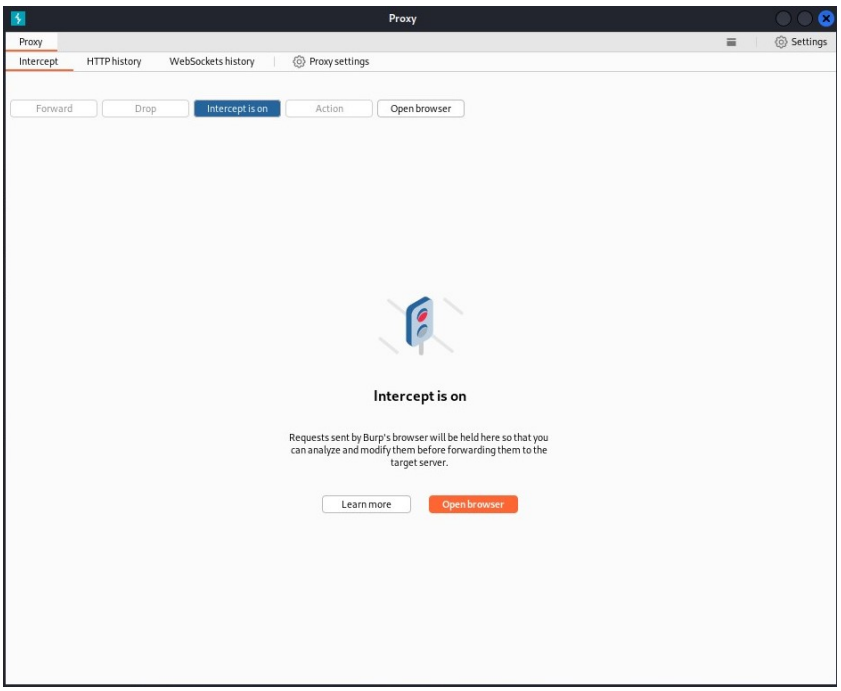

Рис. 3.2: Вкладка прокси

Открываем браузер и переходим в раздел настройек подключения. Теперь нужно настроить браузер для своего прокси-сервера (рис. 3.3).

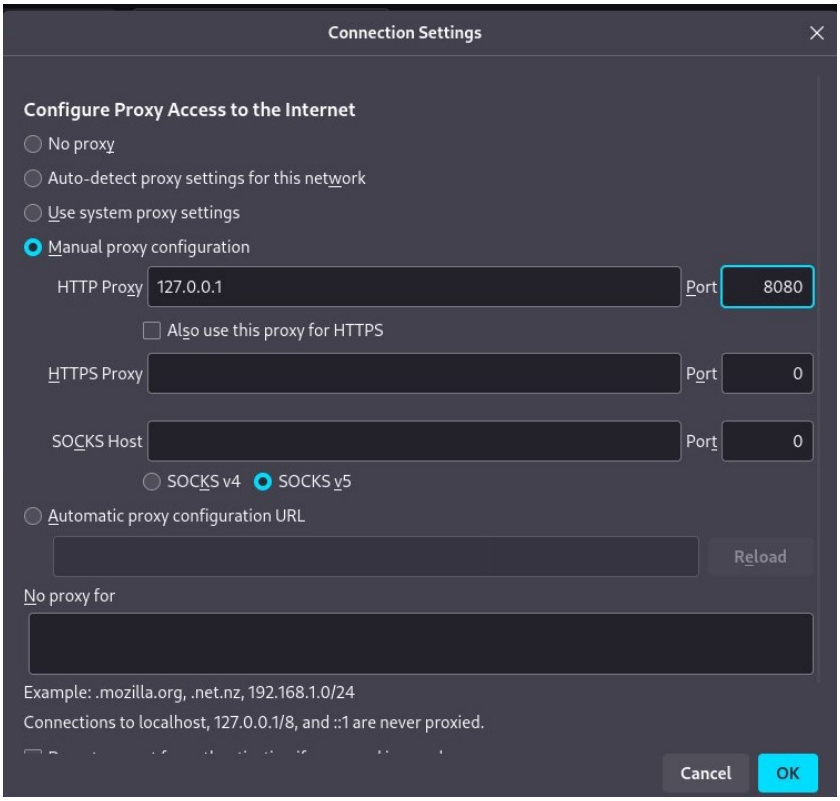

Рис. 3.3: Настройка прокси в браузере

Теперь нужно посетить целевой сайт. В нашем случае целевым сайтом будет http://localhost/DVWA Браузер должен оставаться в режиме подключения. Но если посмотреть на интерфейс Burp Suite, мы уже увидим данные, которые программа смогла получить (рис. 3.4).

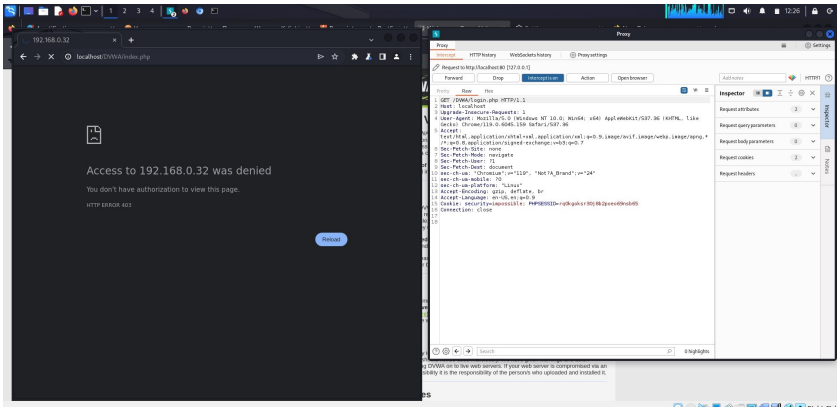

Рис. 3.4: Получение первых данных

После нескольких нажатий кнопки Forward (Вперед) браузер загрузит веб-страницу. В Burp Suite на вкладке Target (Цель) теперь будут некоторые данные на внутренней вкладке Site map (Карта сайта) (рис. 3.5).

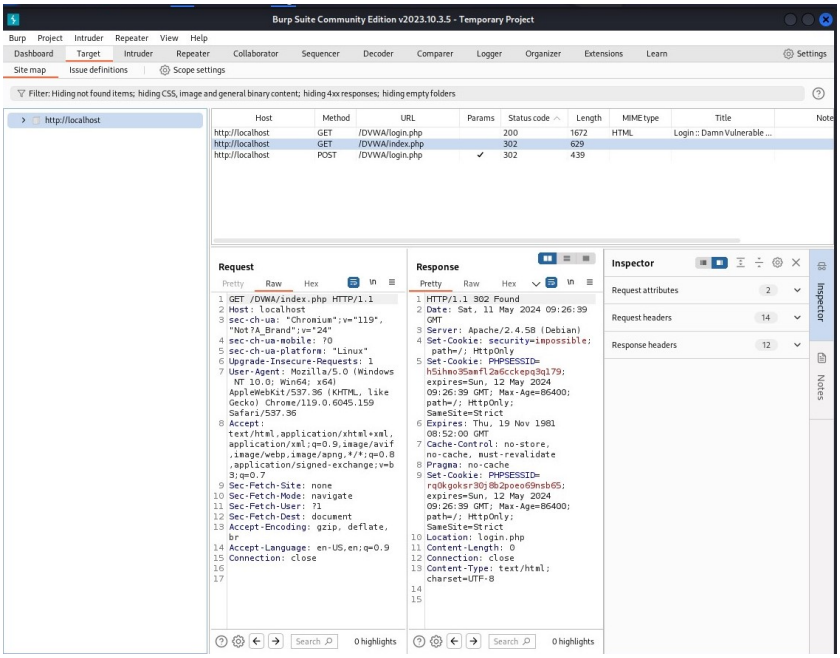

Рис. 3.5: Карта сайта

Вернемся на нашу страницу, открытую на целевом сайте. Сгенерируем трафик, которым воспользуется инструмент — нарушитель Burp Suite. Для этого в форме входа на странице введем случайные учетные данные. После ввода учетных данных увидим, какие сведения смог захватить перехватчик (логин и пароль) (рис. 3.6).

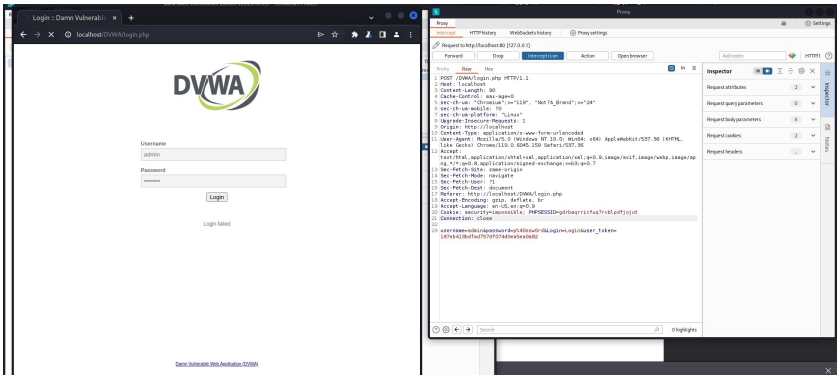

Рис. 3.6: Заполучение перехватчиком данных

Теперь щелкаем правой кнопкой мыши на целевом хосте и выбераем в появившемся контекстном меню команду Send to Intruder (Отправить злоумышленнику). На вкладке Intruder (Злоумышленник) переходим на вкладку Positions (Позиции). Прежде чем продолжить, необходимо убедиться, что выбран тип атаки Cluster bomb (рис. 3.7).

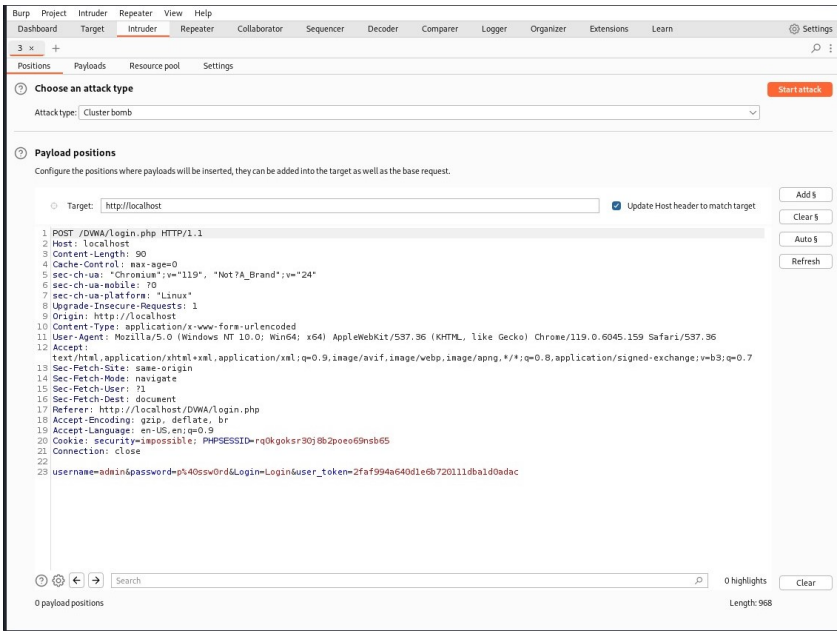

Рис. 3.7: Вкладка Intruder Positions

Если щелкнутьна Payload set (Набор полезных нагрузок), мы увидим количество позиций полезных нагрузок. Выбераем значение 1. Оно будет соответствовать полю username. В раскрывающемся списке Playload type выбераем Simple list. Ниже, в разделе Payload Options (Параметры полезной нагрузки) вводим в поле ввода имя пользователя и нажмимаем ткнопку Add (Добавить). Это имя будет использоваться злоумышленником в качестве имени пользователя.

Теперь в поле ввода Payload set выбераем полезную нагрузку 2, отвечающую за поле пароля. После того, как все настройки будут выполнены, нажмиаем кнопку Start attack (Начало.атаки) (рис. 3.8 - 3.9).

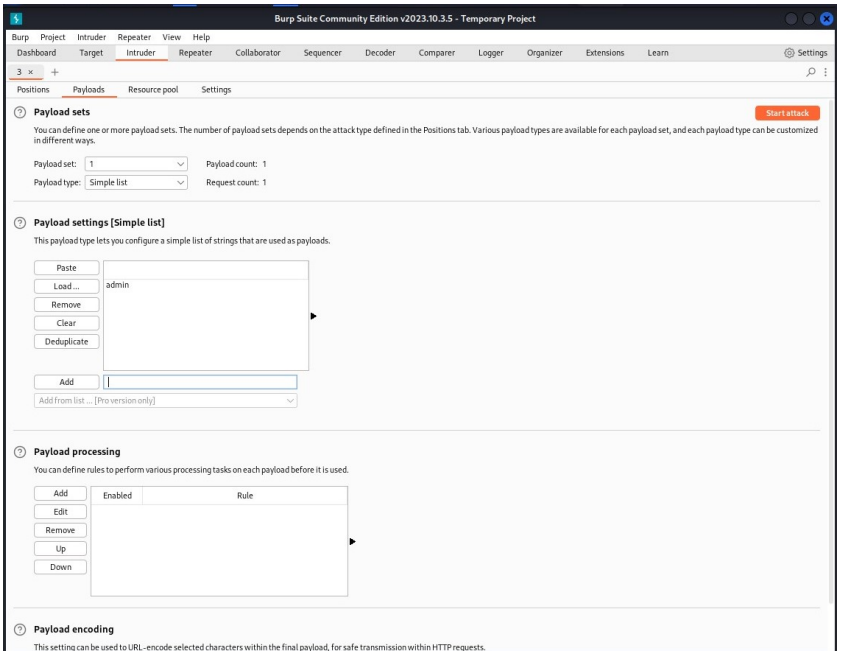

Рис. 3.8: Вкладка Intruder Positions

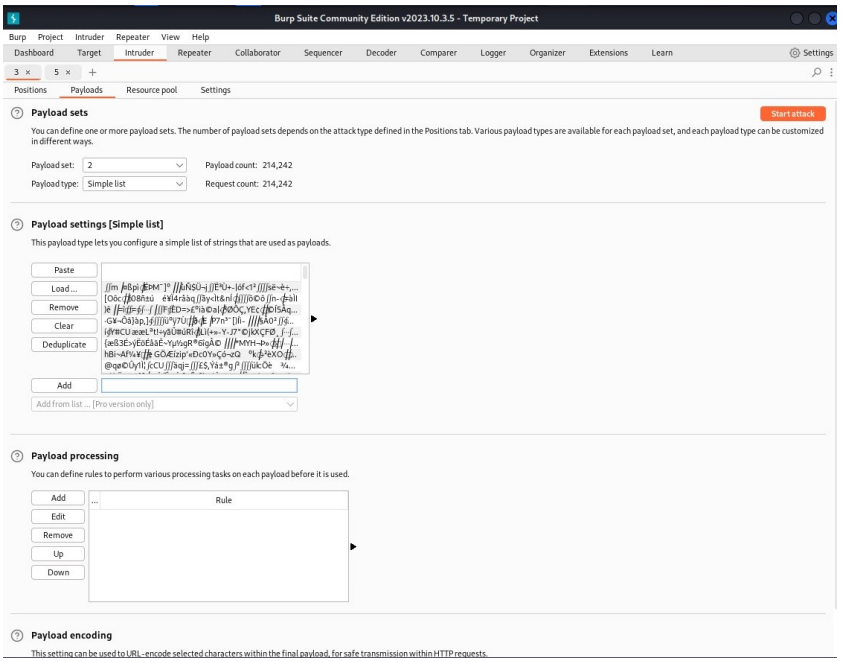

Рис. 3.9: Вкладка Intruder Positions

После этого появится окно с результатами (Results). Глядя на эти результаты, мы видим, что все попытки атаки получили статус (код ответа HTTP) 302, это код

перенаправления. Если щеокнуть на результат, а затем выбрать вкладку Response (Ответ), то увидим, что все запросы перенаправляются на index.php (рис. 3.10).

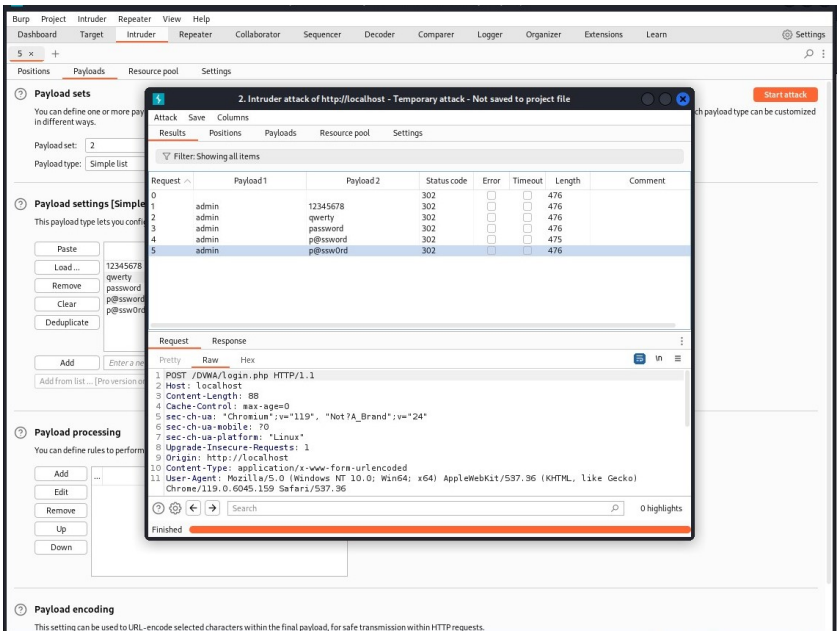

Рис. 3.10: Результаты атаки

Теперь мы можем перейти на страницу входа DVWA и предоставить доступ к сайту. Для этого нам потребуется ввести учетные данные Кроме того, используя инструмент Repeater, мы можем проверить эти результаты в Burp Suite. Ретранслятор предназначен для ручного изменения HTTP-запросов и данных, отправляемых в этих запросах. Вернемся на вкладку Target, выберем для входа в login.php запрос.POST. Это форма запроса, в которой отправляется имя пользователя и пароль. Отправим данный запром в ретранслятор. перейдем в данную папку. После password= удаляем неверный пароль и вводим тот, который перенаправит нас на index.php. И нажимаем кнопку Go. В результате этих действий мы должны во вкладке response увидеть, что локация теперь будет index.php. После нажатия на кнопку Follow redirection (Переадресация) во вкладке Rendermы увидим, как должна выглядеть страница (у меня это почему-то не получилось, хотя я вводила правильный пароль и логин) (рис. 3.11 - 3.12).

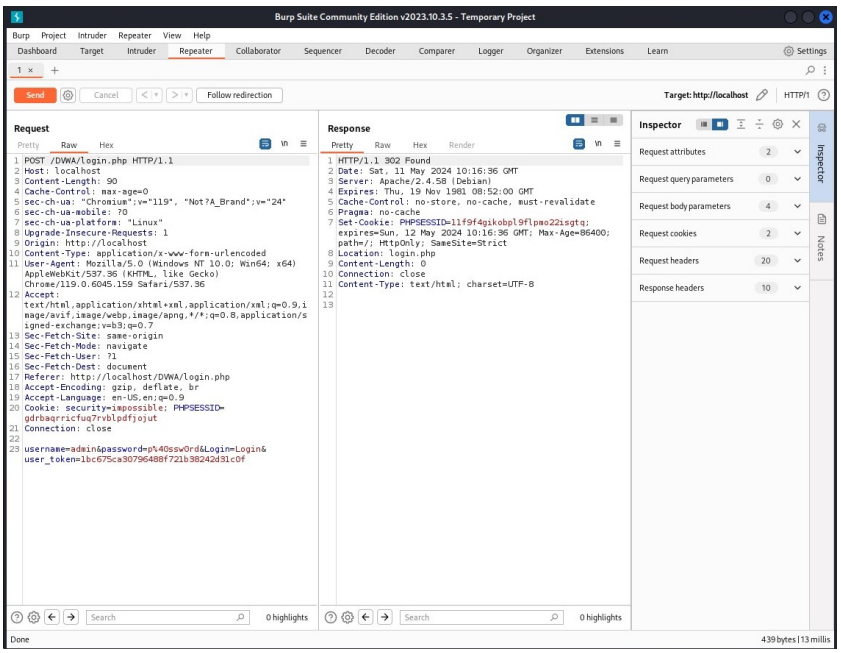

Рис. 3.11: Вкладка Repeater

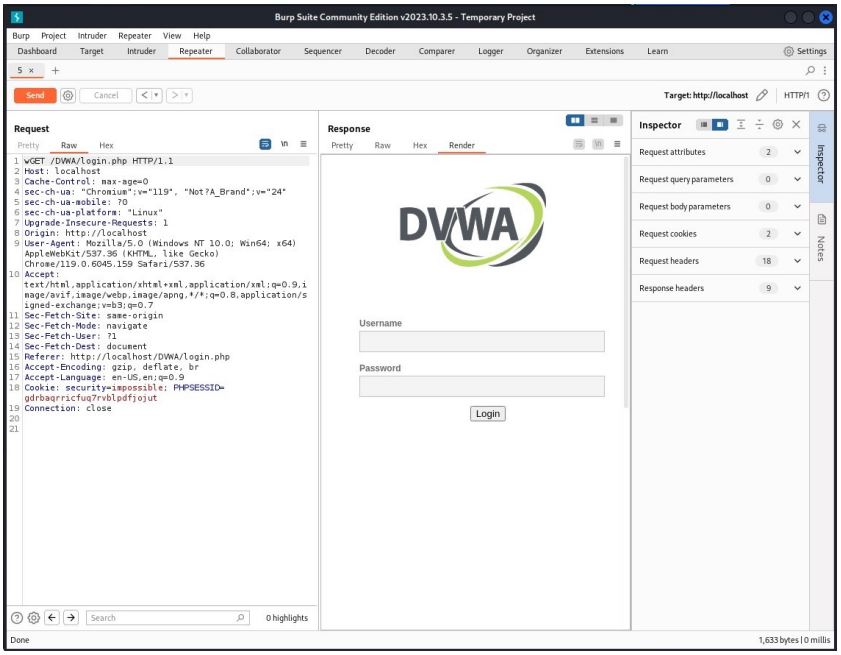

Рис. 3.12: Вкладка Repeater Render

4 Выводы

Познакомилась с инструментами Burp Suite и применила их для атаки на целевой сайт.

5 Список литературы. Библиография

[1] Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. П18 Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. — 448 с.: ил. — (Серия «Для профессионалов»). ISBN 978-5-4461-1252-4