Отчет по этапу №5

Использование Burp Suite

Галацан Николай, НПИбд-01-22

Содержание

Список иллюстраций

1 Цель работы

Научиться использовать Burp Suite для демонстрации реальных возможностей злоумышленника, проникающего в веб-приложения.

2 Выполнение лабораторной работы

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. [1]

Для запуска Burn Suite выбираю команду меню *Applications -> Web Application Analysis -> burpsuite* В нашем примере мы будем использовать Burp для взлома учетных данных, чтобы 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. Открываю вкладку *Proxy*. Нажимаю *Intercept is on* (рис. 2.1).

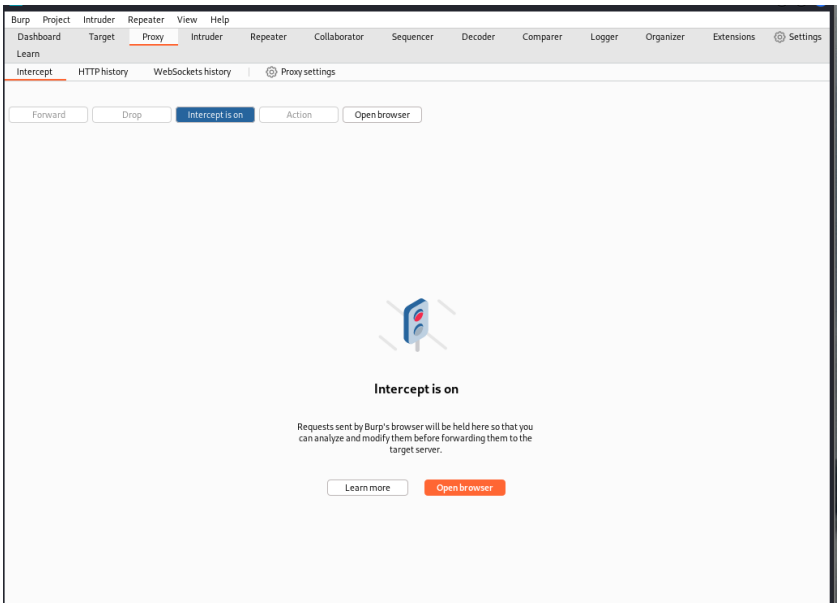

Рис. 2.1: Включение перехвата в Прокси

После этого открываю браузер и выбираю *Settinfs -> Preferences -> Advanced -> Network -> Connection Settings* и настраиваю свой прокси-сервер. После этого запускаю и открываю DVWA (рис. 2.2).

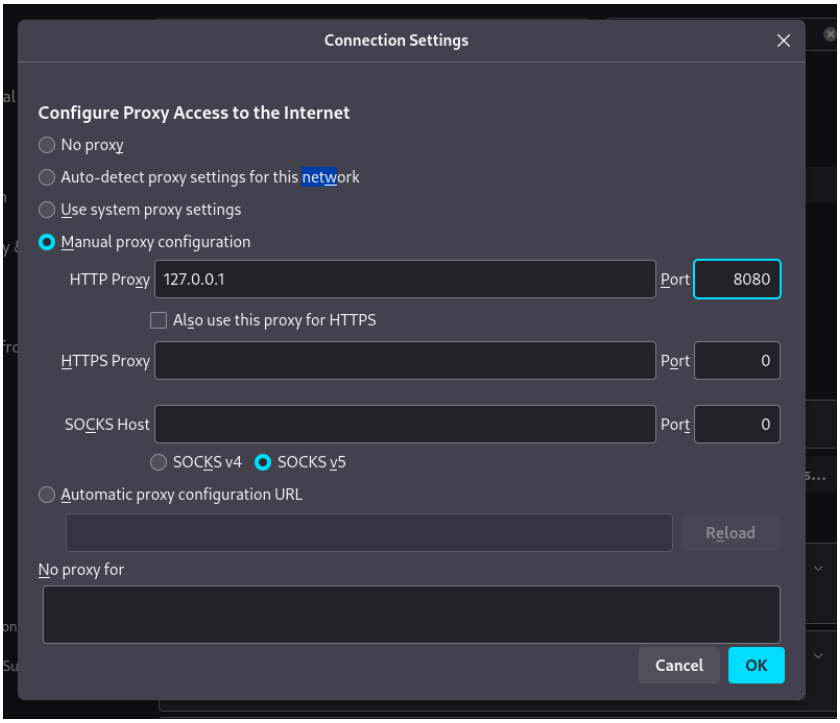

Рис. 2.2: Настройка прокси-сервера

Перейдя в интерфейс Burp Suite, уже видны данные, которые программа смогла получить (рис. 2.3).

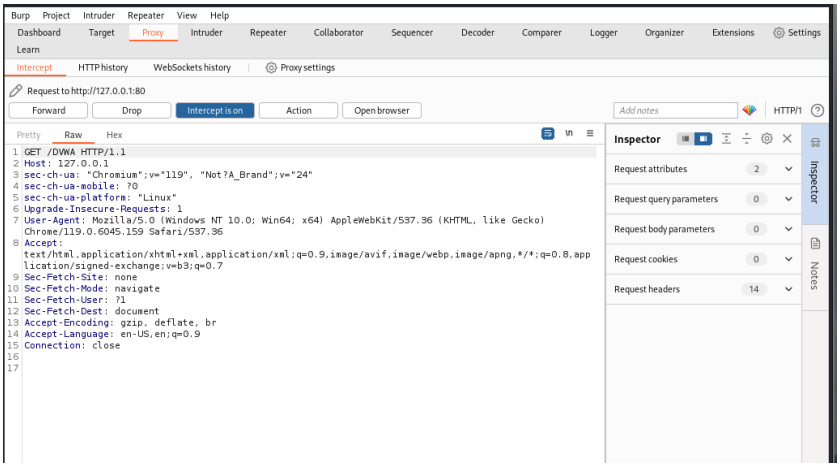

Рис. 2.3: Перехват данных веб-приложения

После нескольких нажатий кнопки *Forward* браузер загружает веб-страницу. В Burp Suite на вкладке *Target* (Цель) теперь видны некоторые данные на внутренней вкладке *Site map* (Карта сайта) (рис. 2.4).

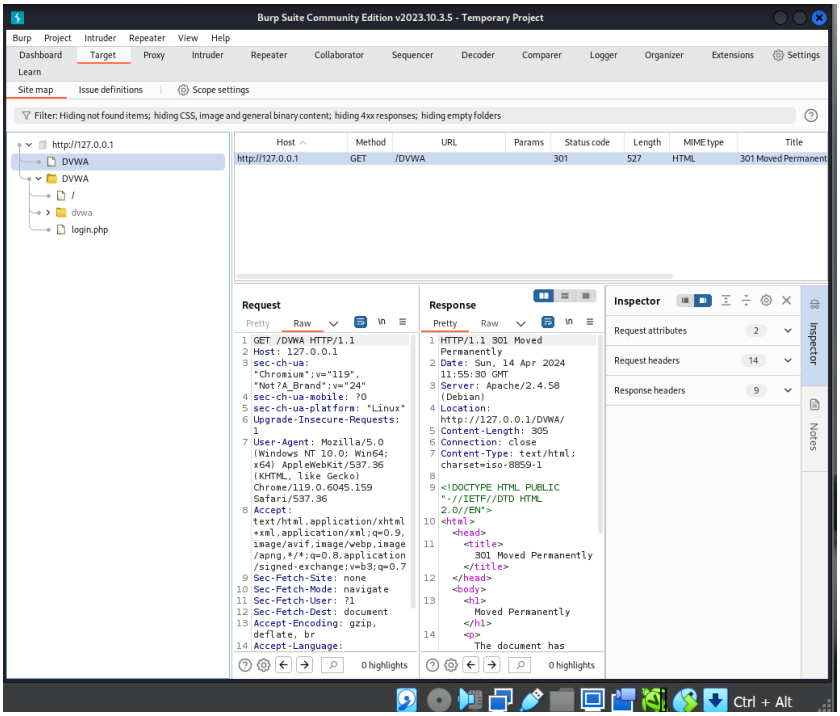

Рис. 2.4: Вкладка Target

В браузере ввожу любые логин и пароль для входа. Во вкладке *Intercept* вижу перехваченный запрос, где на последней строке видны введенные логин и пароль (рис. 2.5).

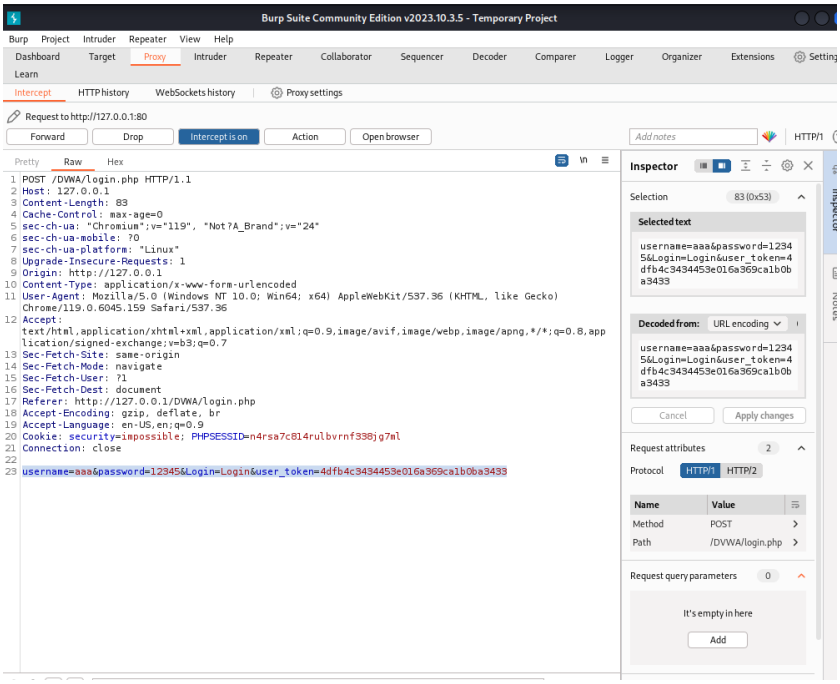

Рис. 2.5: Запрос для входа в веб-приложение

Во вкладке *HTTP-history* так же можно увидеть попытку входа. Нажимаю правой кнопкой мыши на запрос и выбираю *Send to Intruder* (рис. 2.6)

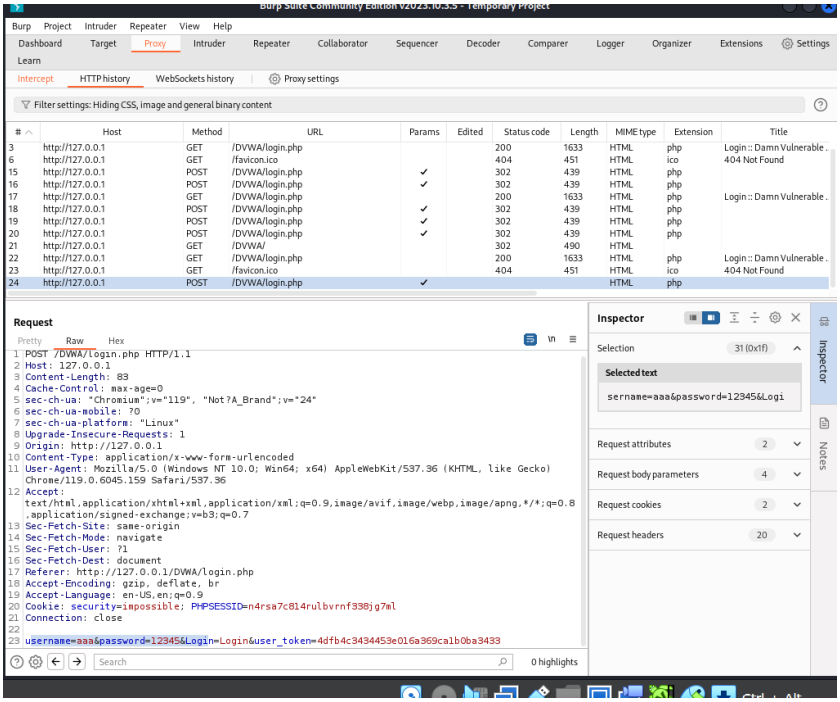

Рис. 2.6: HTTP-history

В разделе *Intruder* выбираю вкладку *Positions* и выделяю поля со введенными логином и паролем на последней строке, нажимаю *Add* (рис. 2.7)

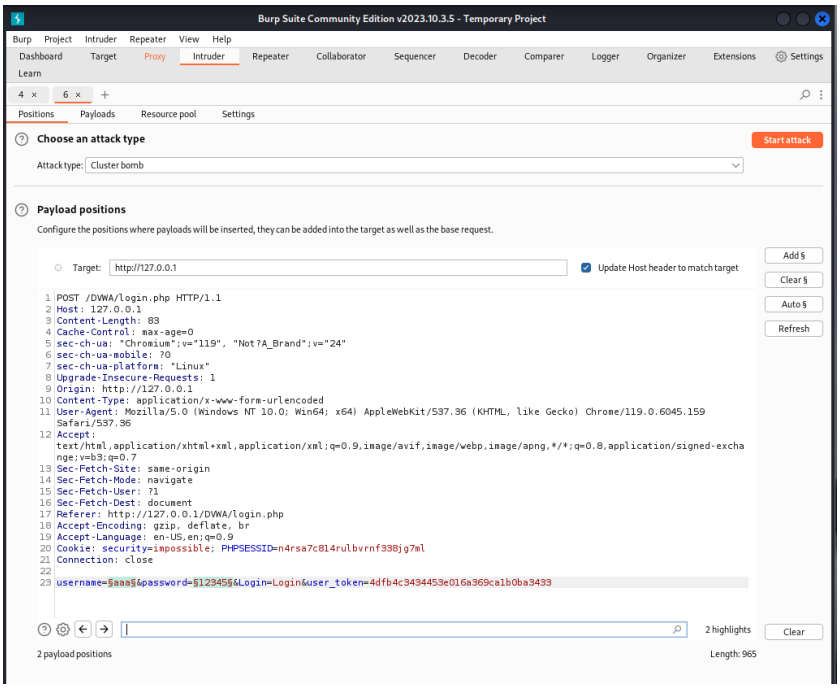

Рис. 2.7: Выбор позиций в Intruder

Выбираю тип атаки *Cluster bomb* и перехожу на вкладку *Payloads*. В *Payload sets* выбираю 1 и заполняю: в *Payload settings* прописываю возможные имена пользователя для подбора (рис. 2.8)

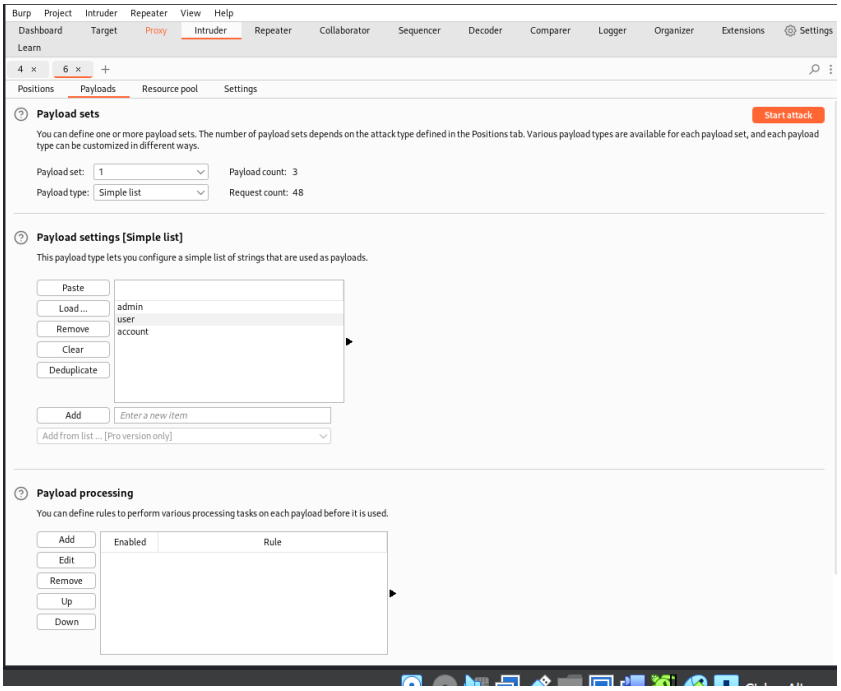

Рис. 2.8: Заполнение нагрузки username

В *Payload sets* выбираю 2 и заполняю: в *Payload settings* добавляю возможные пароли (рис. 2.9)

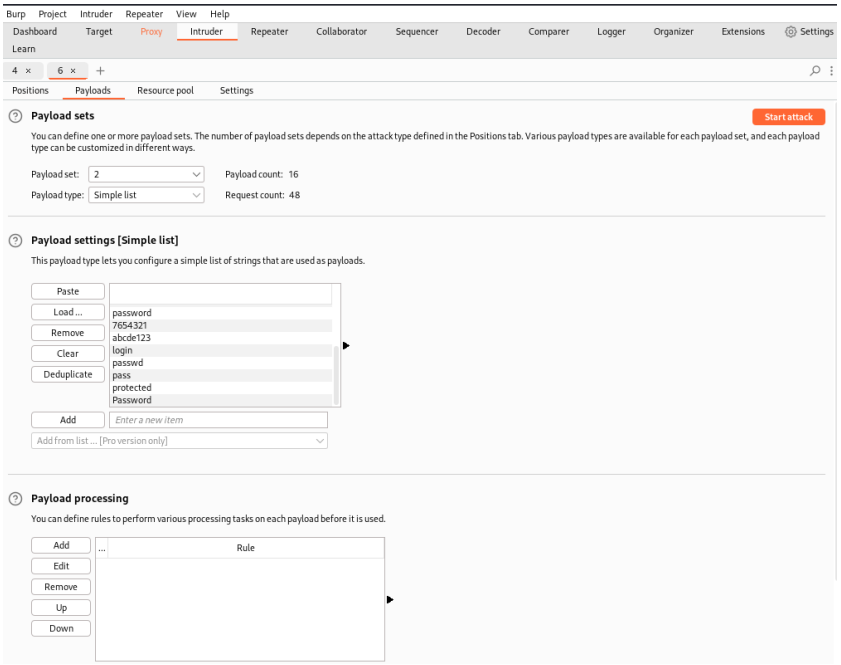

Рис. 2.9: Заполнение нагрузки password

Нажимаю *Start attack* и дожидаюсь результатов (рис. 2.10)

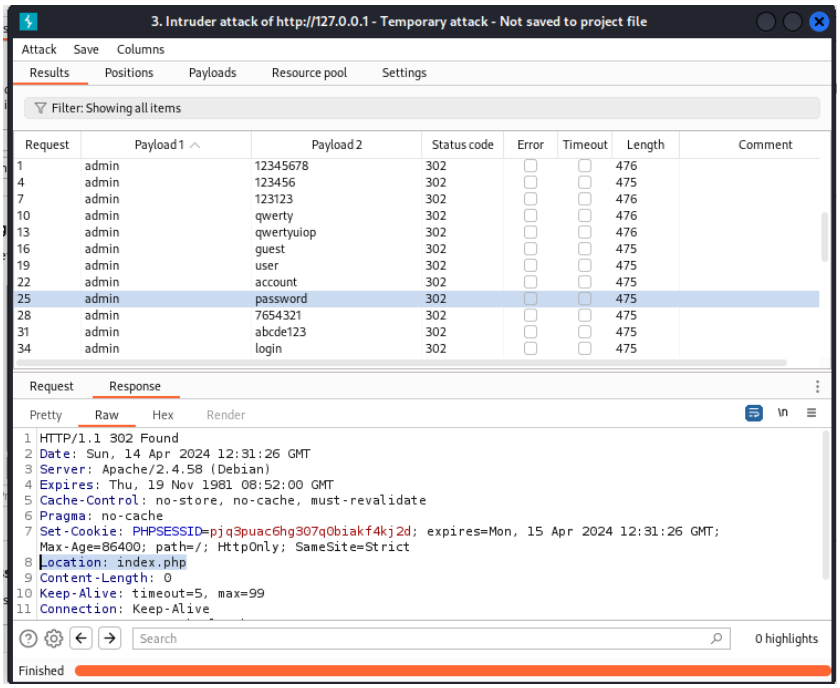

Рис. 2.10: Результаты атаки

Все попытки атаки получили статус (код ответа HTTP) 302 - Перенаправление. Если нажать кнопкой мыши на результате, а затем выбрать вкладку *Response* (Ответ), то можно увидеть, что все запросы перенаправляются на `login.php`, кроме одного. Это комбинация `admin:password`, который перенаправляется на `index.php`. Это и есть верные логин и пароль.

Нажав на запрос и выбрав *Send to Repeater*, можно проверить эти результаты в Burp Suite. Ретранслятор предназначен для ручного изменения HTTP-запросов и данных, отправляемых в этих запросах. Во влкадке *Repeater* можно изменять данные в запросе, нажать *Send* и получить ответ (рис. 2.11) [1]

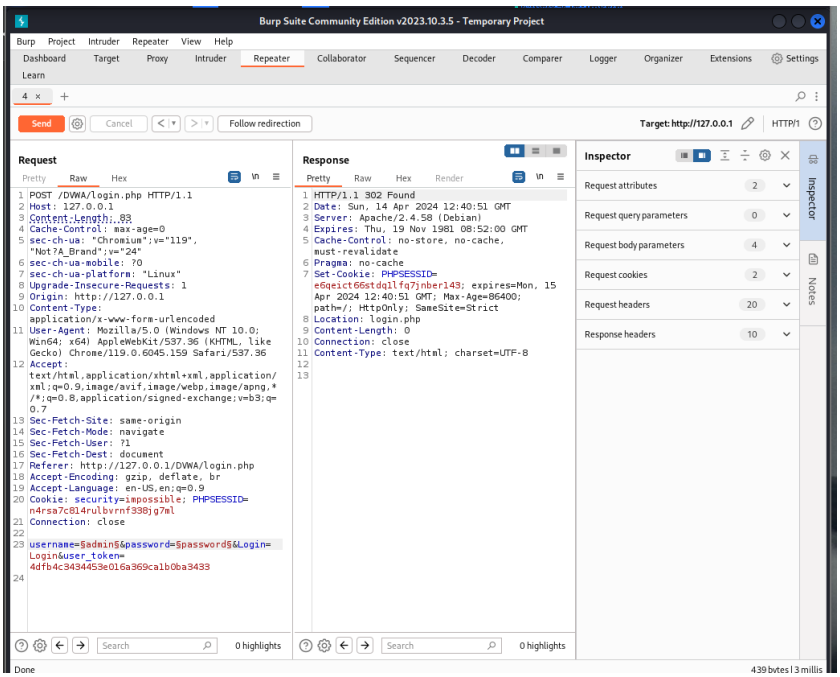

Рис. 2.11: Использование Repeater

3 Выводы

В ходе работы были изучены и использованы несколько инструментов, которые входят в состав Burp Suite. Этот набор инструментов безопасности приложений является мощной платформой для атаки веб-приложений. [1]

Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.