Отчёт по индивидуальному проекту этап №5

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

# 1 Цель работы

Научиться использовать на практике Burp Suite.

# 2 Выполнение лабораторной работы

1. Запускаем локальный сервер, на котором откроем веб-приложение DVWA для тестирования инструмента Burp Suite. (рис. 1)

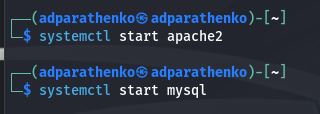


Рис. 1: Запуск Apache2

1. Запускаем Burp Suite. (рис. 2)

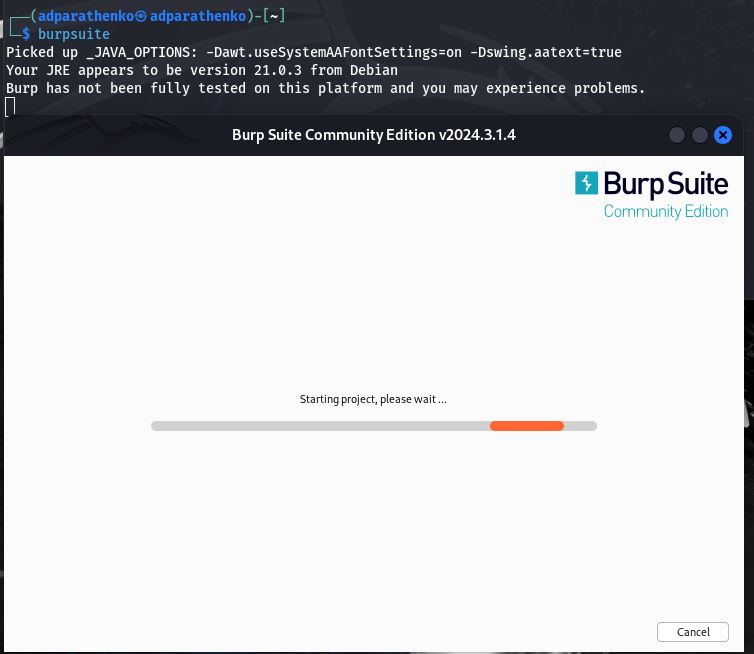


Рис. 2: Запуск Burp Suite

1. Изменяем настройки в Proxy на *Intercept is on*. рис. 3)

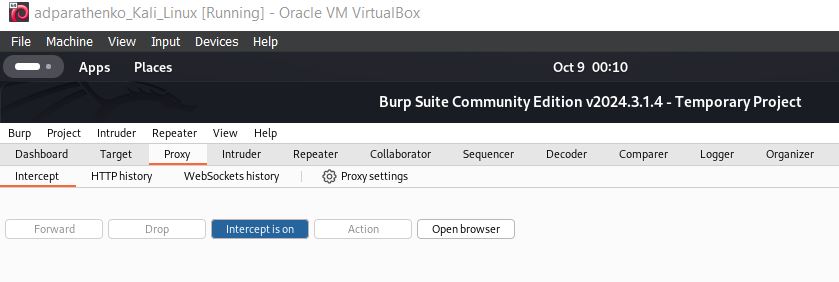


Рис. 3: Intercept is on

1. Изменяем настройки сервера в браузере для работы с Proxy и захватом данных с помощью Burp Suite. (рис. 4)

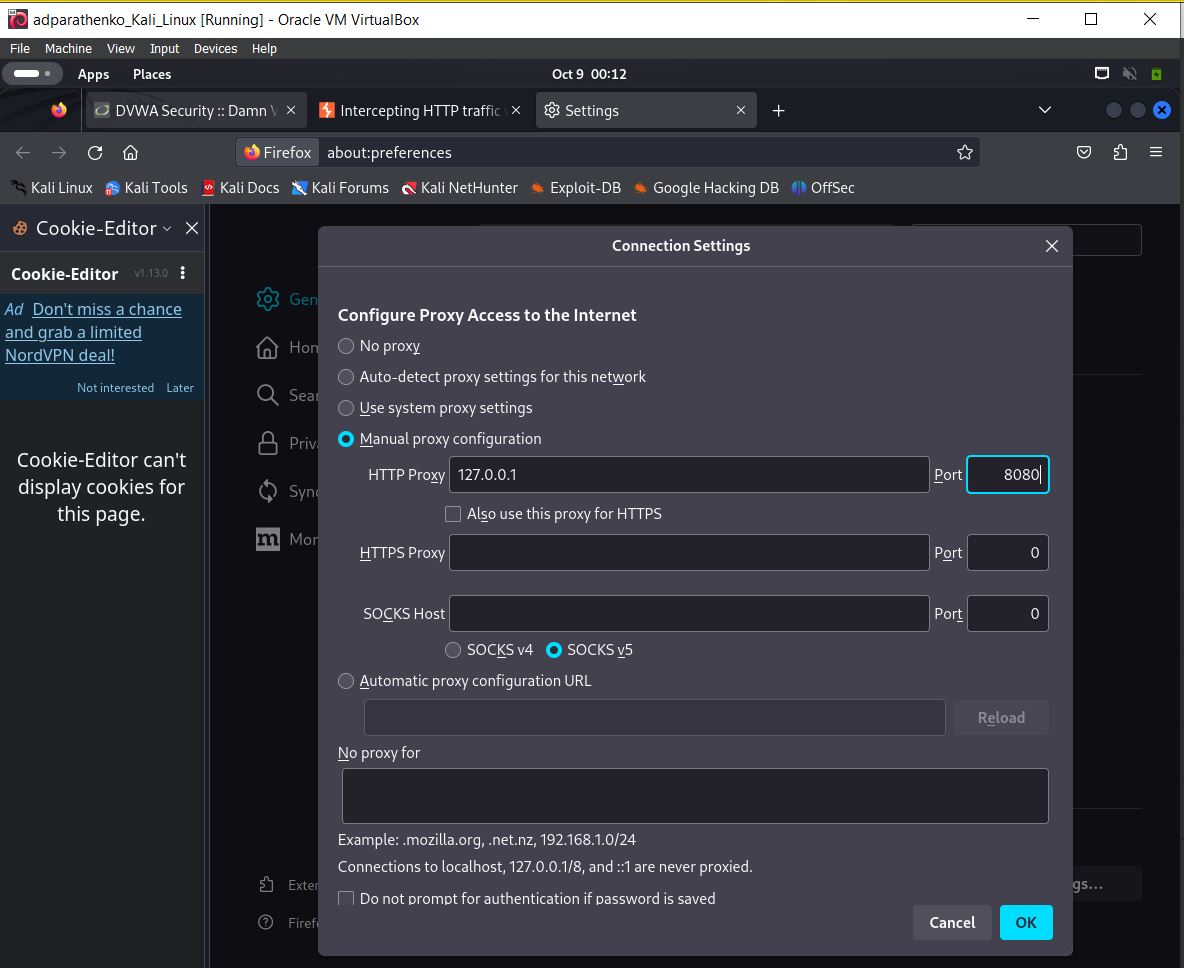


Рис. 4: Настройки сервера в браузере

1. Устанавливаем параметр network\_allow\_hijacking\_localhost на true. (рис. 5)

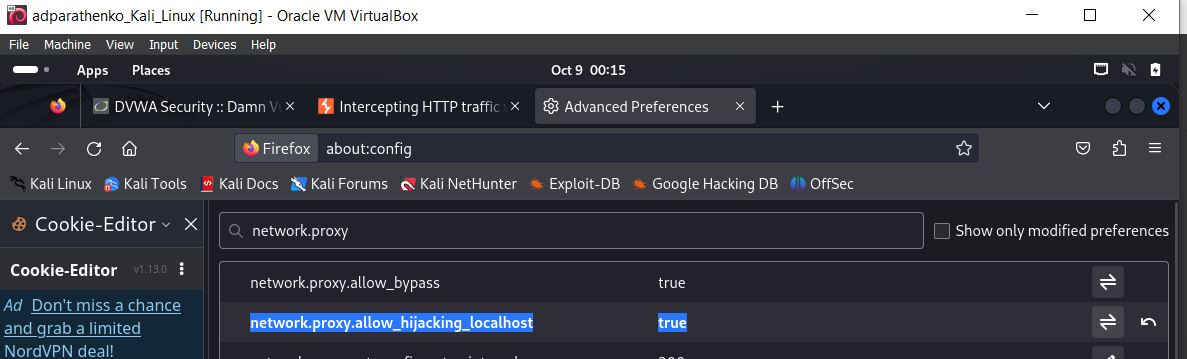


Рис. 5: network\_allow\_hijacking\_localhost

1. В браузере заходим на DVWA и во вкладке Proxy появляется захваченный запрос. нажимаем Forward, чтобы загрузить страницу. (рис. 6)

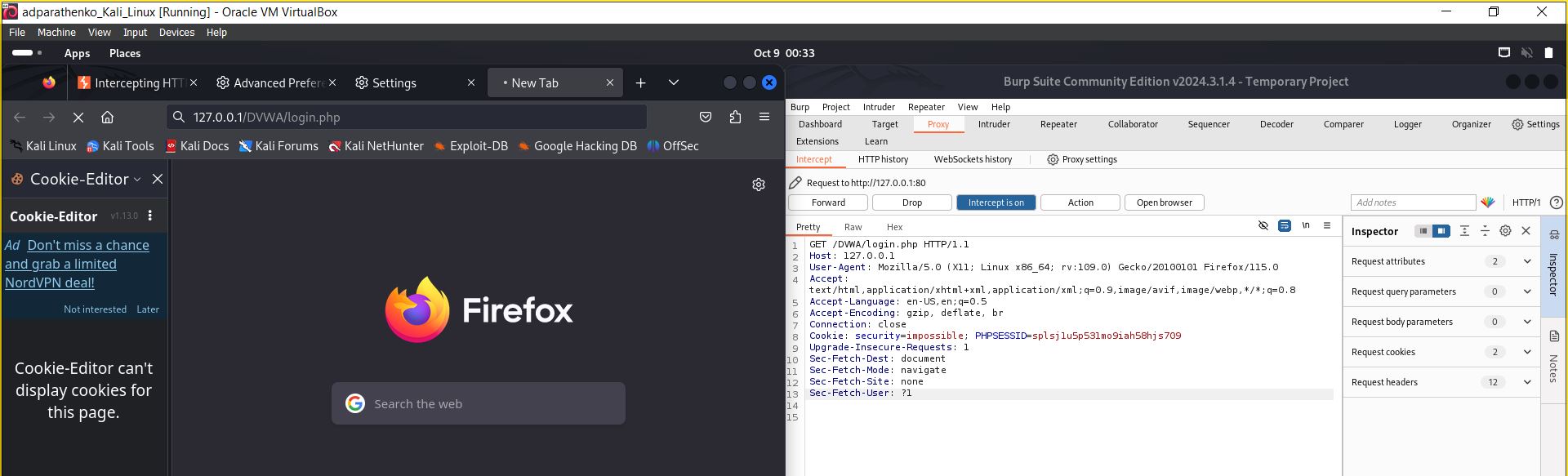


Рис. 6: Захваченный запрос

1. Загрузилась страница авторизации. (рис. 7)

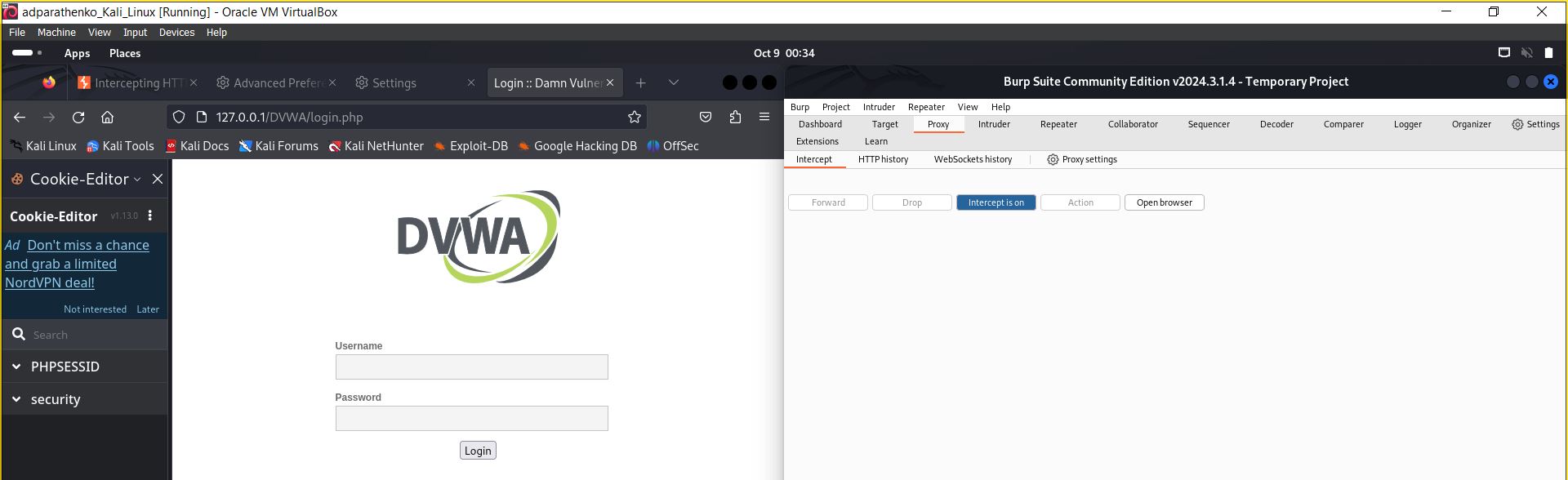


Рис. 7: Страница авторизации

1. Историю запросов можно посмотреть во вкладке Target. (рис. 8)

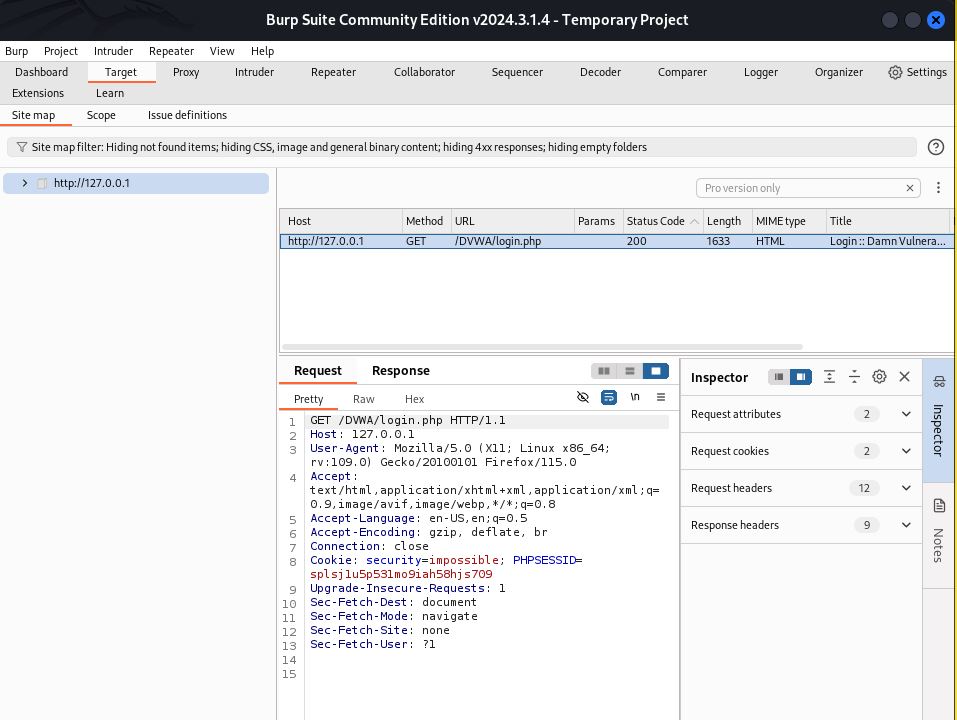


Рис. 8: Target

1. Вводя случайный логин и пароль, в запросе мы увидим введенные данные. (рис. 9)

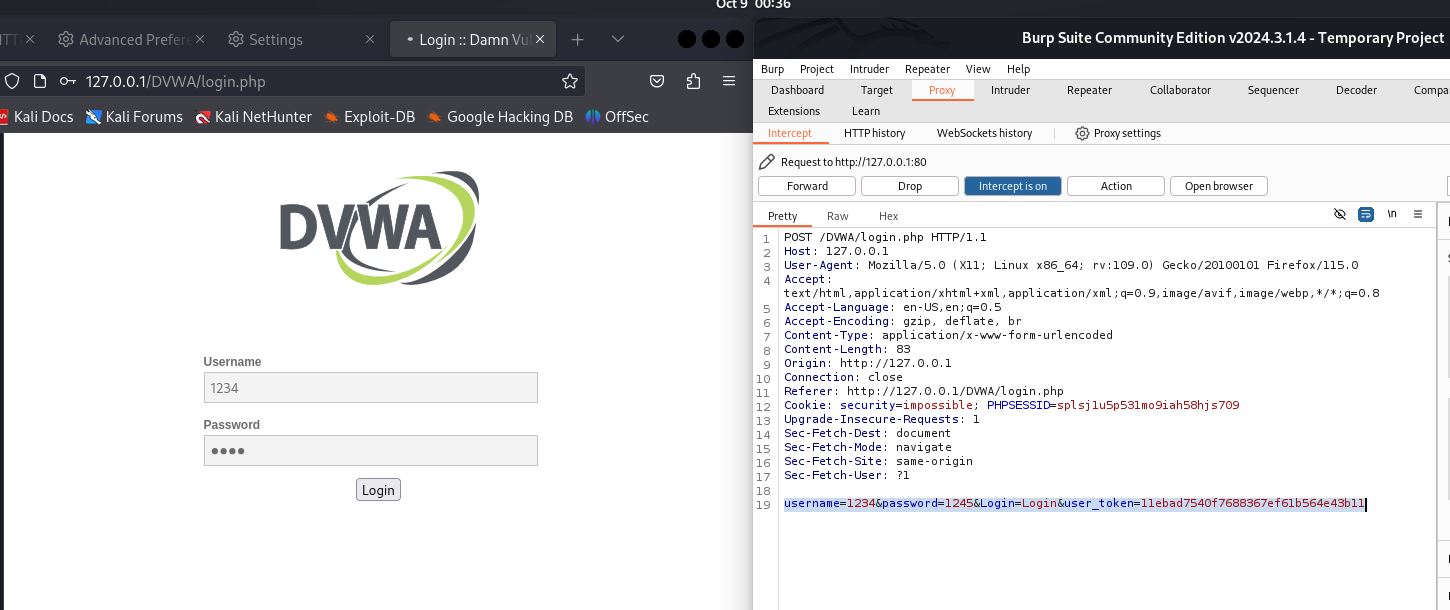


Рис. 9: случайный логин и пароль

1. Находим этот запрос во вкладке Target и, нажимая на правую кнопку мыши, нажимаем на Send to Intruder. Попадая во вкладку мы видим вид атаки. (рис. 10)

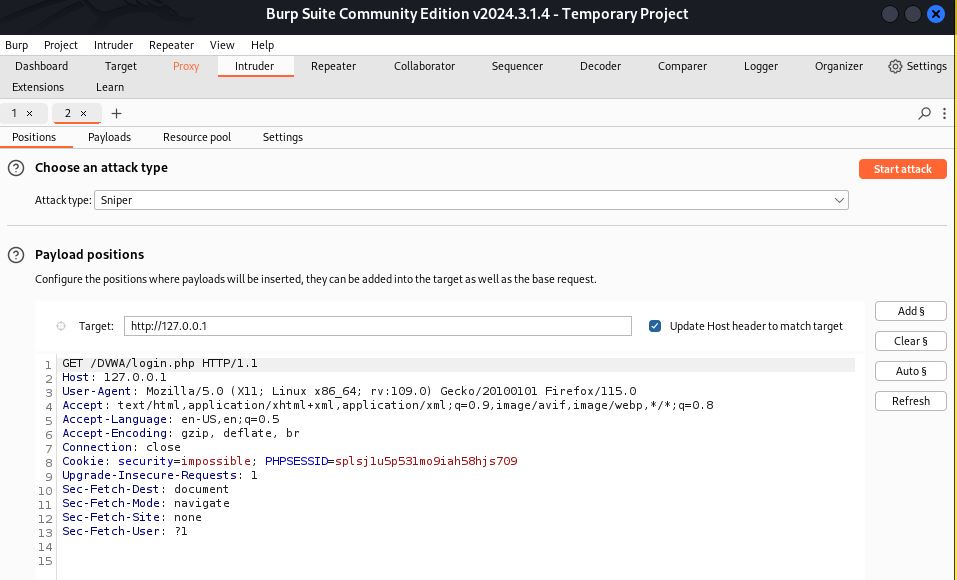


Рис. 10: Intruder

1. Меняем вид атаки на Cluster bomb и выделяем специальными знаками данные ввода, которые хотим подбирать, в нашем случае, это логин и пароль. (рис. 11)

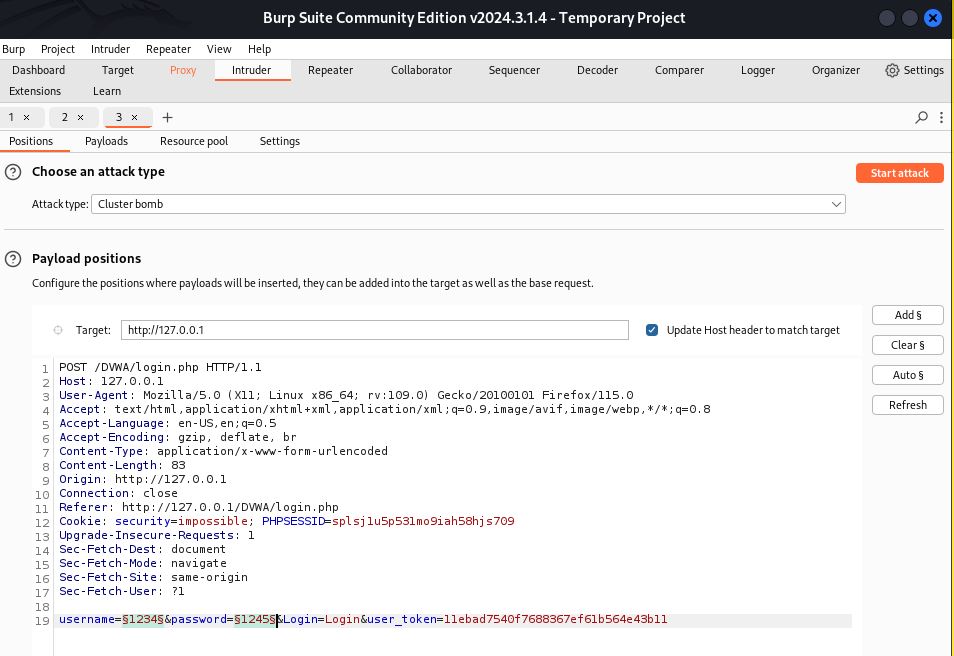


Рис. 11: Cluster bomb

1. Далее добавляем 2 списка параметров для подбора логина и пароля. (рис. 12) -(рис. 13)

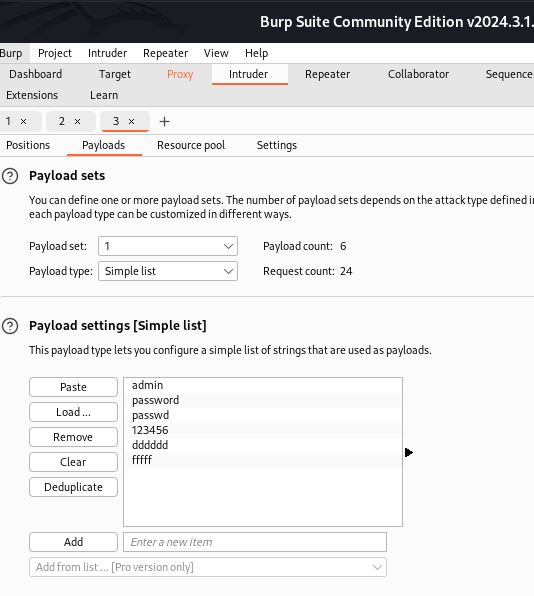


Рис. 12: Логин

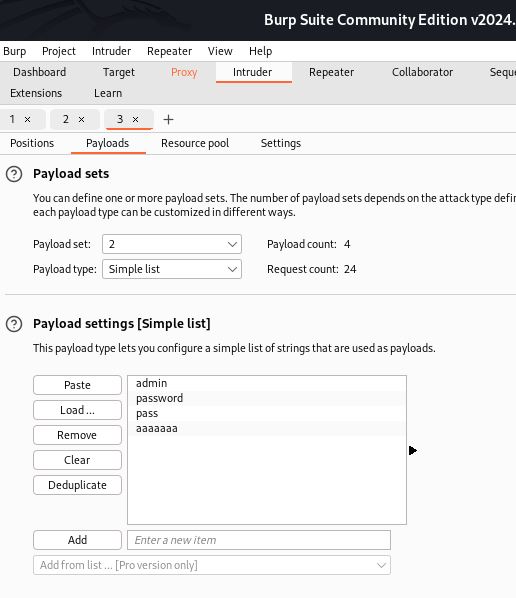


Рис. 13: Пароль

1. Запускаем атаку и получаем результаты перебора. (рис. 14)

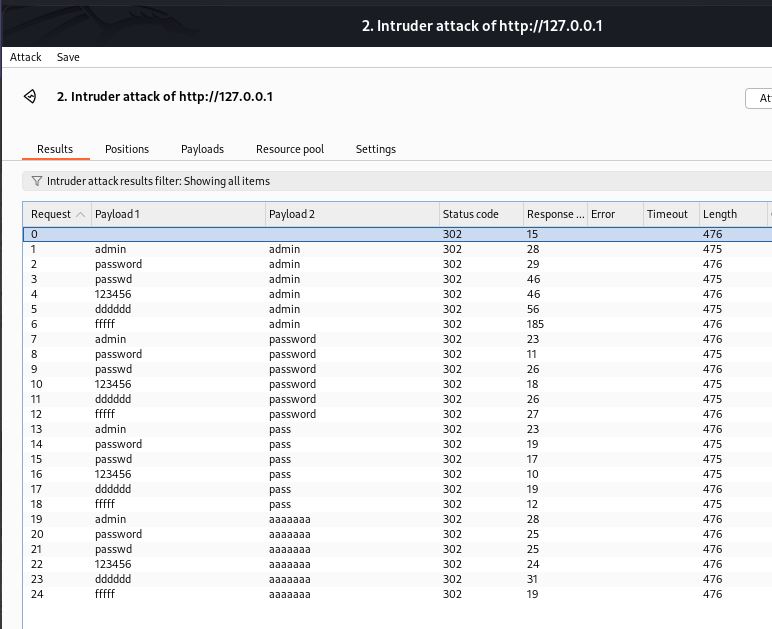


Рис. 14: Результаты атаки

1. У всех вариантов перебора, кроме одного, *location: login.php*. (рис. 15)

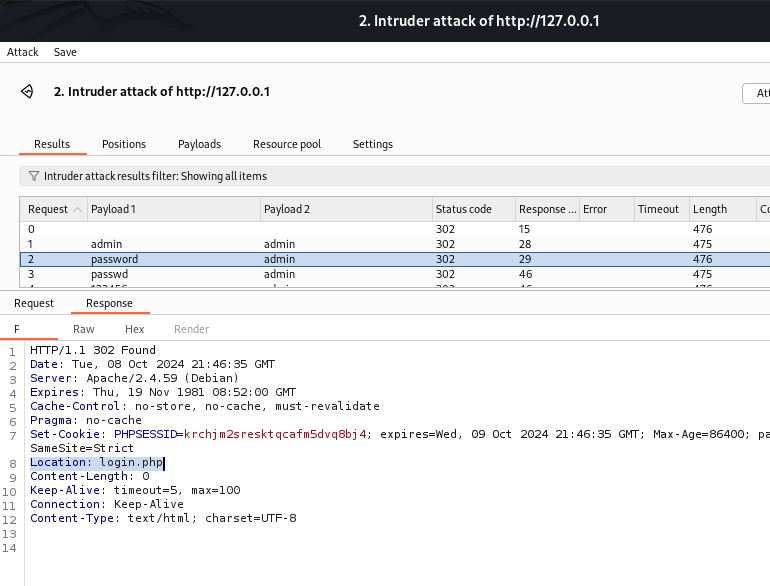


Рис. 15: location: login.php

1. А у пары ***admin password*** результат *location: index.php*. Это показывает нам, что это верная пара логин-пароль. (рис. 16)

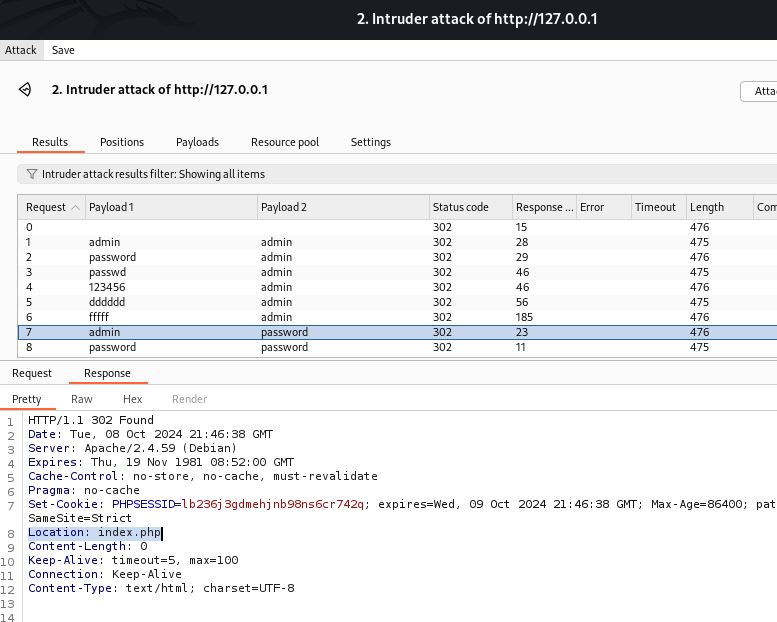


Рис. 16: admin password

1. Чтобы ещё раз проверить результат мы отправляем эту пару на повторную проверку *Send to Repeater*. (рис. 17)

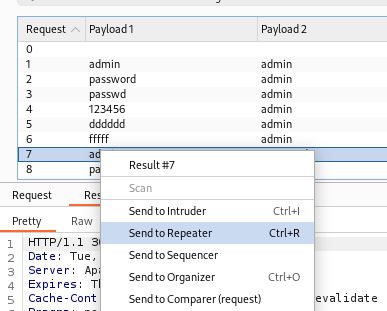


Рис. 17: Send to Repeater

1. Получаем тот же реузльтат *location: index.php*. (рис. 18)

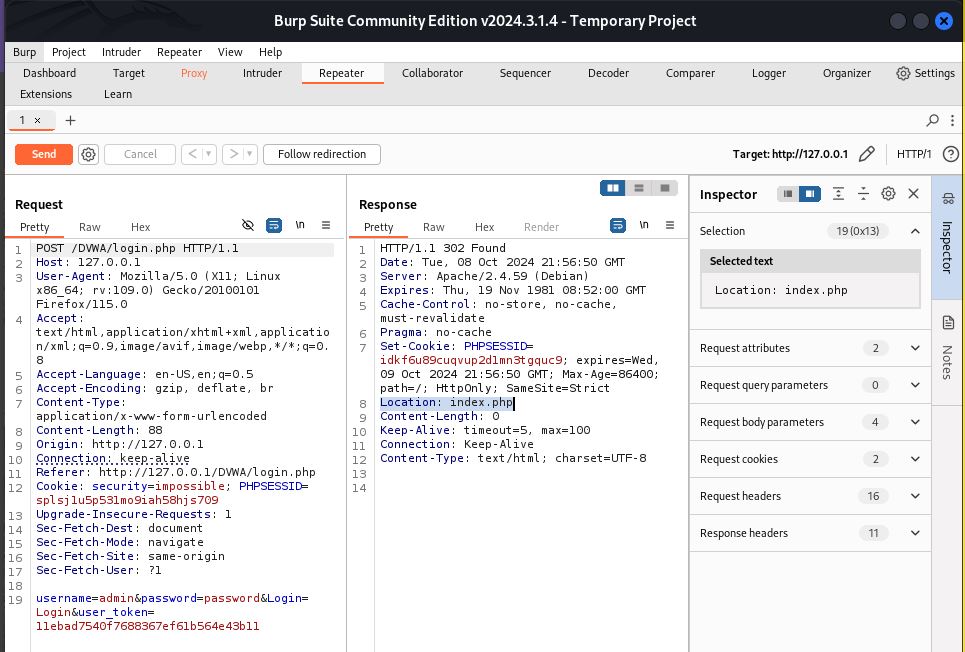


Рис. 18: location: index.php

1. Нажимаем на *Follow redirection* и получаем нескомпилированный html код в окне Response. (рис. 19)

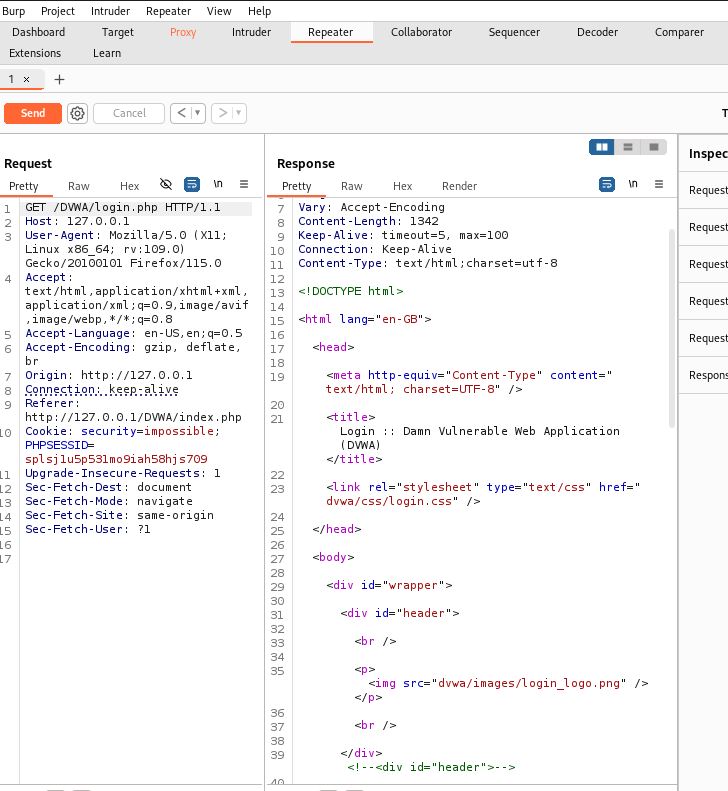


Рис. 19: Follow redirection

1. В подокне Render получаем вид страницы в браузере. (рис. 20)

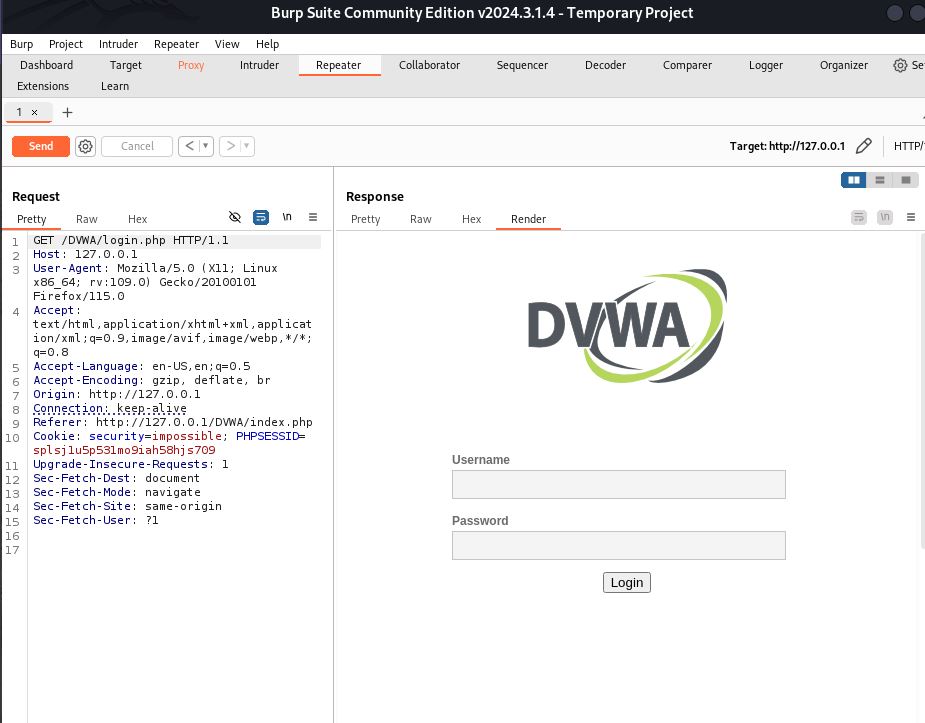


Рис. 20: Render

# 3 Вывод

В результате выполнения работы мы научились использовать инструмент Burp Suite и перебором возможных пар подобрали пару логин-пароль для входа на сайт.

# Список литературы

1. Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Хериянто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.