Индивидуальный проект - Этап 5

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

# 1 Цель работы

Получение навыков пользование Burp Suite.

## 1.1 Введение

Burp Suite - инструмент для тестирования безопасности веб-приложений, позволяющий множеством функций перехватывать, анализировать, модифицировать разные HTTP-запросы между клиентом и сервером.

# 2 Выполнение лабораторной работы

Запускаю Burp Suite, прохожу через пару диалоговых окон, где спрашивают, как будет устроен проект, над которым мы будем работать (рис. 1).

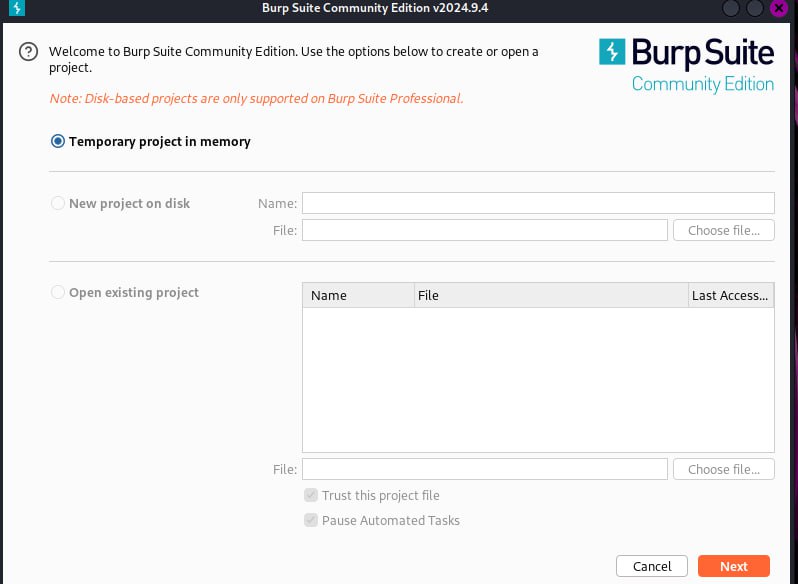


Рис. 1: Инициализация Burp Suite

Открываю встроенный в Burp Suite браузер и открываю в нём DVWA - всё как обычно (рис. 2).

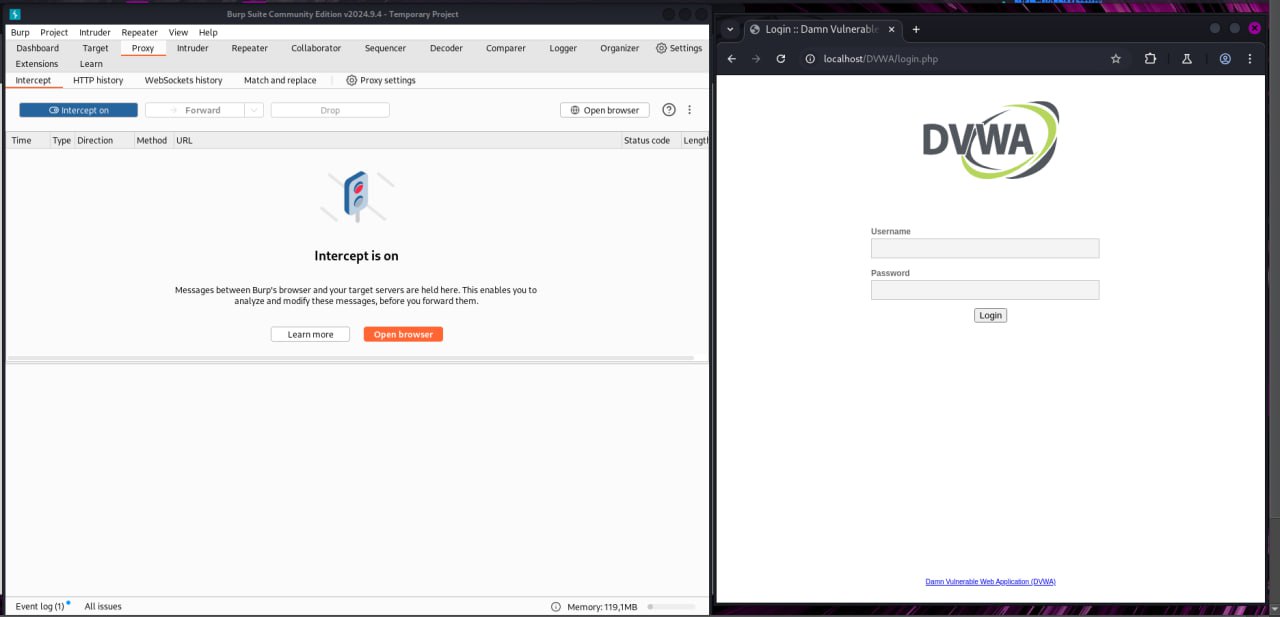


Рис. 2: DVWA через встроенный браузер

Перед работой надо запустить apache2 и mysql, буду тестировать Burp Suite на dvwa - брут форс пароля, как в этапе про Hydra, только в этот раз у DVWA будет уровень защиты “Высокий” (рис. 3).

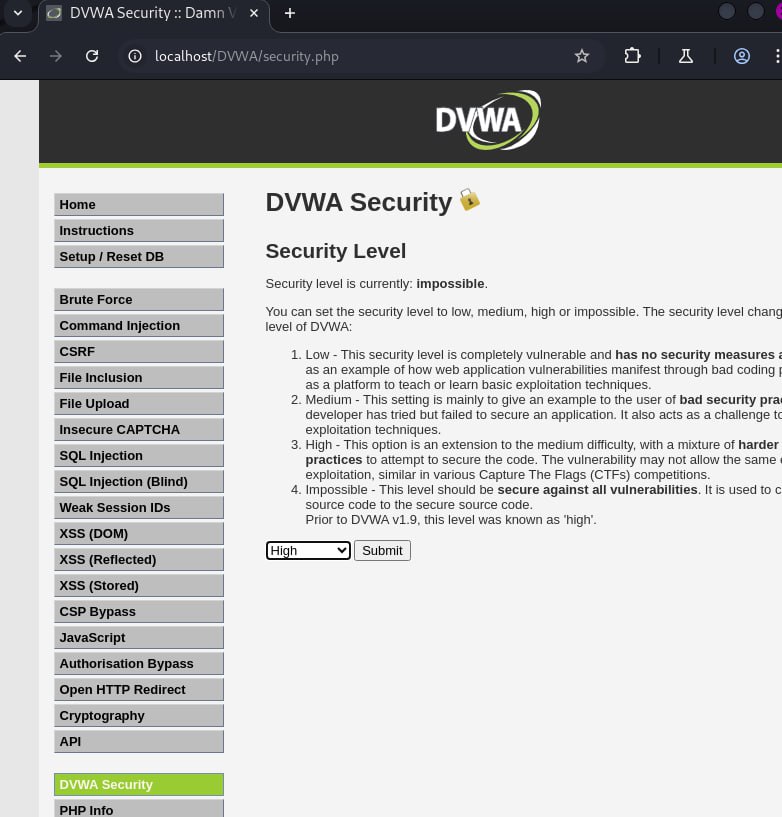


Рис. 3: Высокий уровень защиты DVWA

Перехожу на страничку Brute Force DVWA, там есть кнопку view source, которая позволяет посмотреть код данной странички. Такая страничка различается на разных уровнях сложности - на уровне сложности High появляется user\_token, который совсем чуток усложняет брут форс (рис. 4).



Рис. 4: Код странички входа на сложности High

### 2.0.1 О user\_token

При каждом обновлении страницы меняется и user\_token (а страница будет много обновляться при множестве неудачных попыток брут форса), сервер в свою очередь не пропускает реквесты, у которых уже устарел user\_token, т.е. взломщику нужно придумать способ, как этот user\_token получать автоматически при каждой попытке брут форса.

Идём далее, с помощью Burp Suite мы можем автоматизировать процесс нахождения user\_token (он вшит в страничку). Захожу в настройки и во вкладке Sessions создаю новое правило (рис. 5).

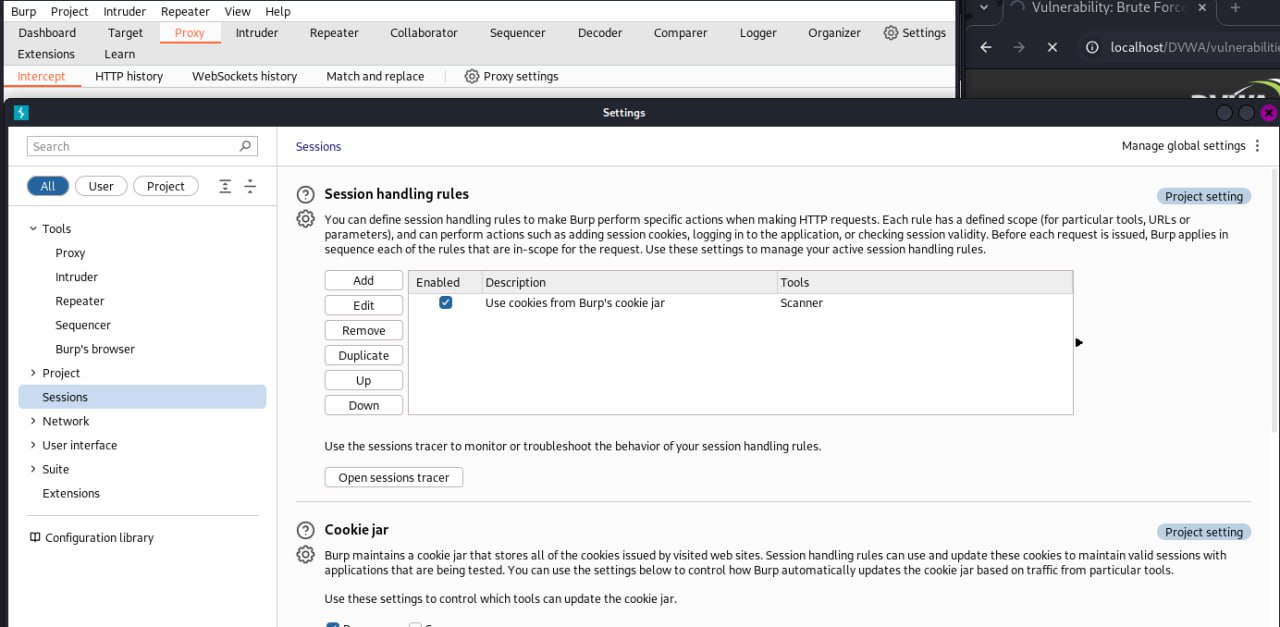


Рис. 5: Новое правило в Burp Suite

В новом правиле мы добавляем новое “макро действие”, и затем настраиваем его - открывается Macro Recorder, где мы выбираем наш последний реквест - попытку входа в DVWA, оттуда мы можем посмотреть на наш реквест в виде кода и найти строчки с user\_token (рис. 6).

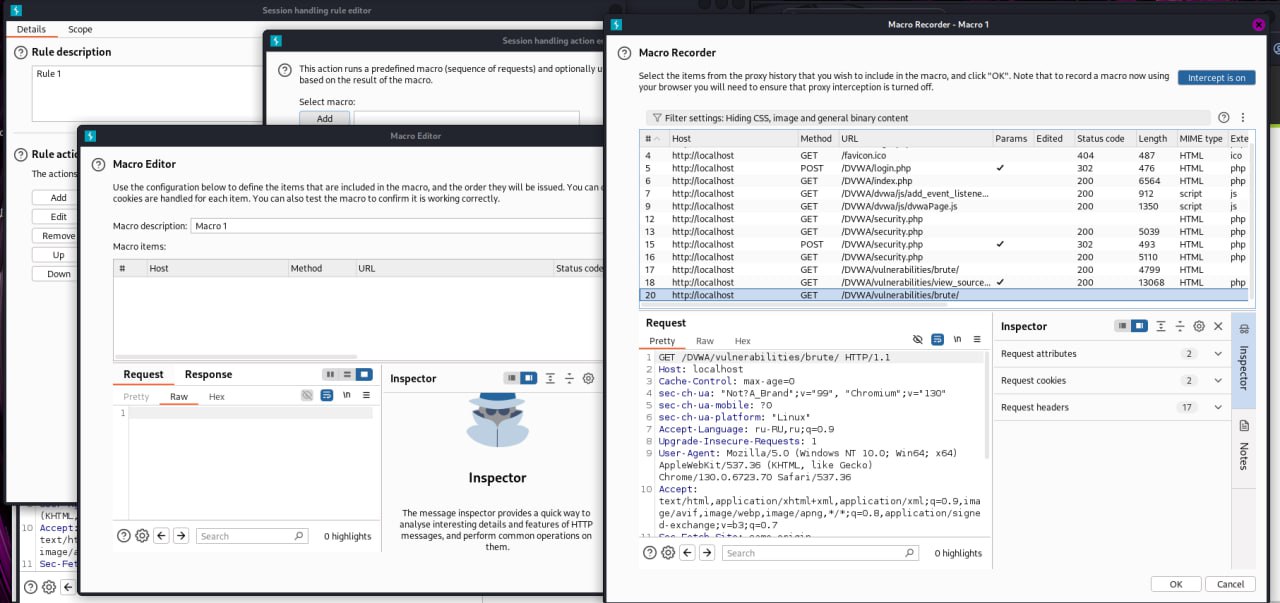


Рис. 6: Новое макро действие в Burp Suite

В открытом коде реквеста находим нужный параметр, за которым мы будем следить и запоминать - user\_token (рис. 7).

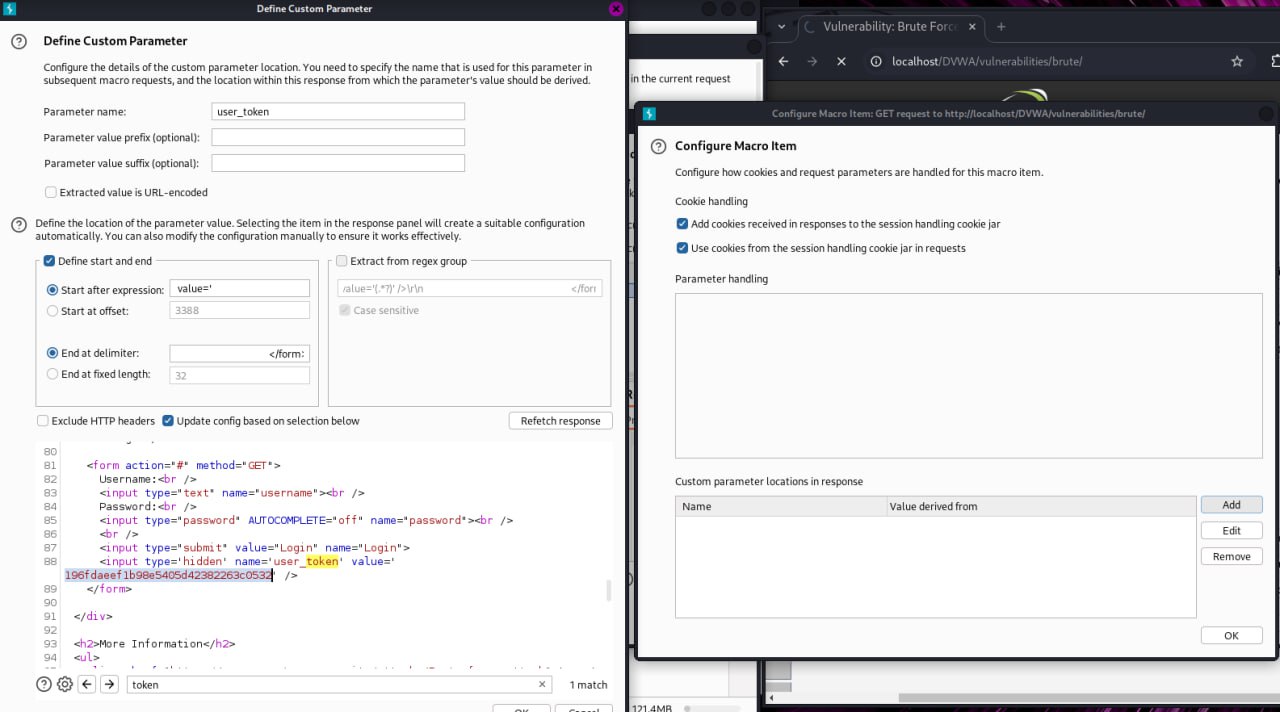


Рис. 7: Отслеживание параметра user\_token в каждом реквесте

Сохраняем наше макро действие, ставим галочку “Tolerate URL mismatch when matching parameters (Use for URL-agnostic CRSF tokens)” - тут написано ставить, если мы имеем дело с юзер токенами (рис. 8).

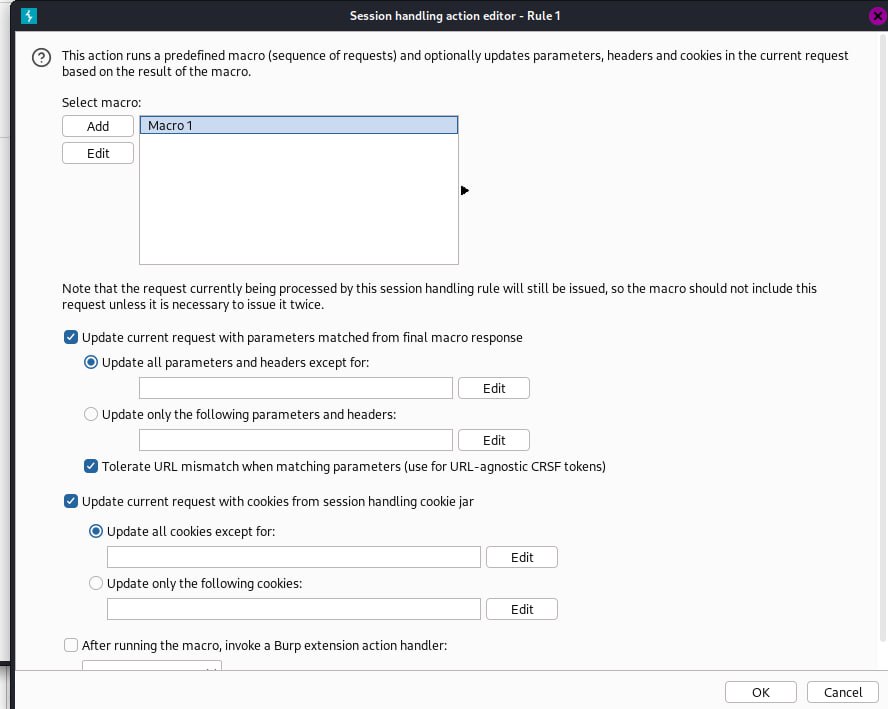


Рис. 8: Сохранение макро действия

Возвращаемся в настройку правила, выставляем галочки так, чтобы это правило применялось исключительно к инструменту Intruder - им мы будем пользоваться для брут форса приложения (рис. 9).

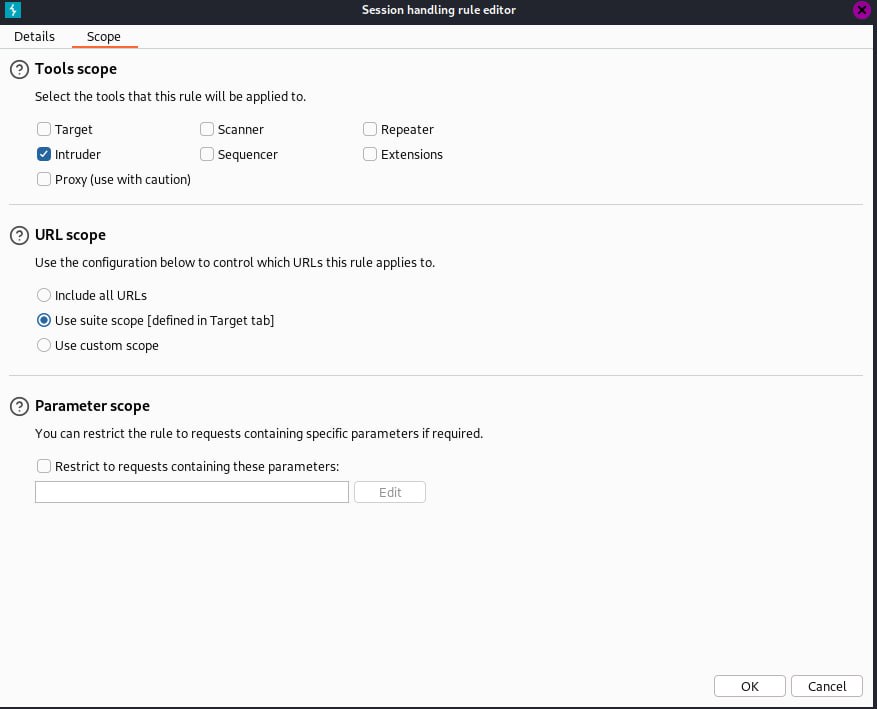


Рис. 9: Сохранение нового правила

Начнём. Включаем Intercepter - перехватываем реквест с попыткой входа (рис. 10).

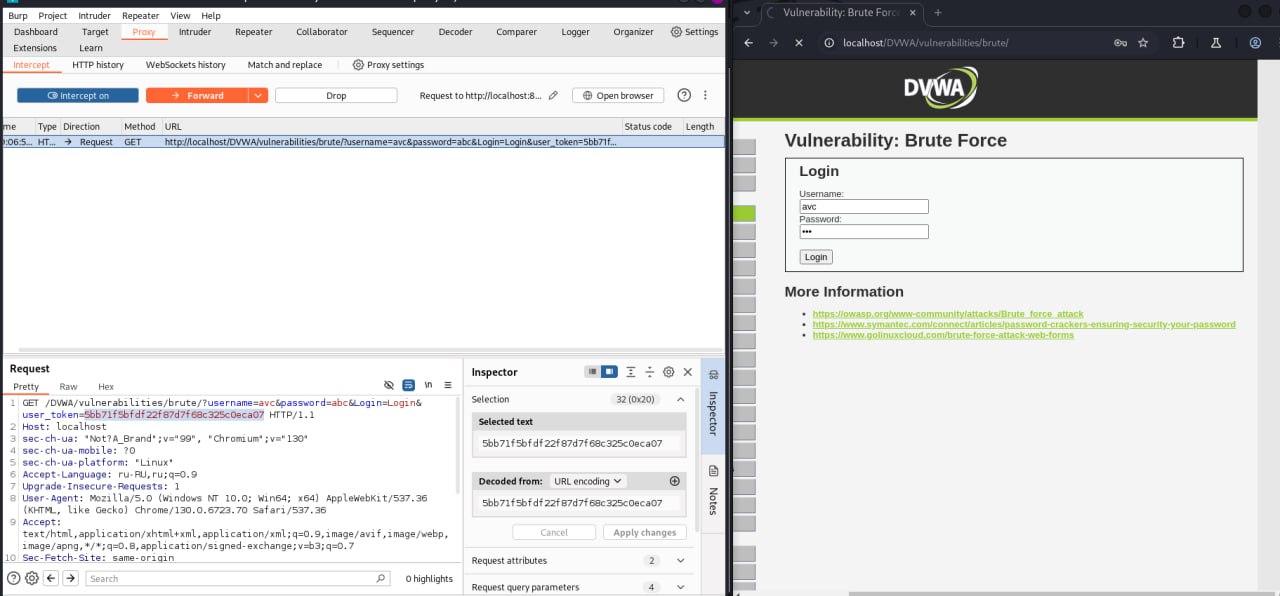


Рис. 10: Перехват реквеста с попыткой входа

Открываем вкладку HTTP-history и находим перехваченный реквест, нажимаем на него правой кнопкой и “Send to Intruder” (отправляем в инструмент взломащика), а затем “Add to scope” (рис. 11).

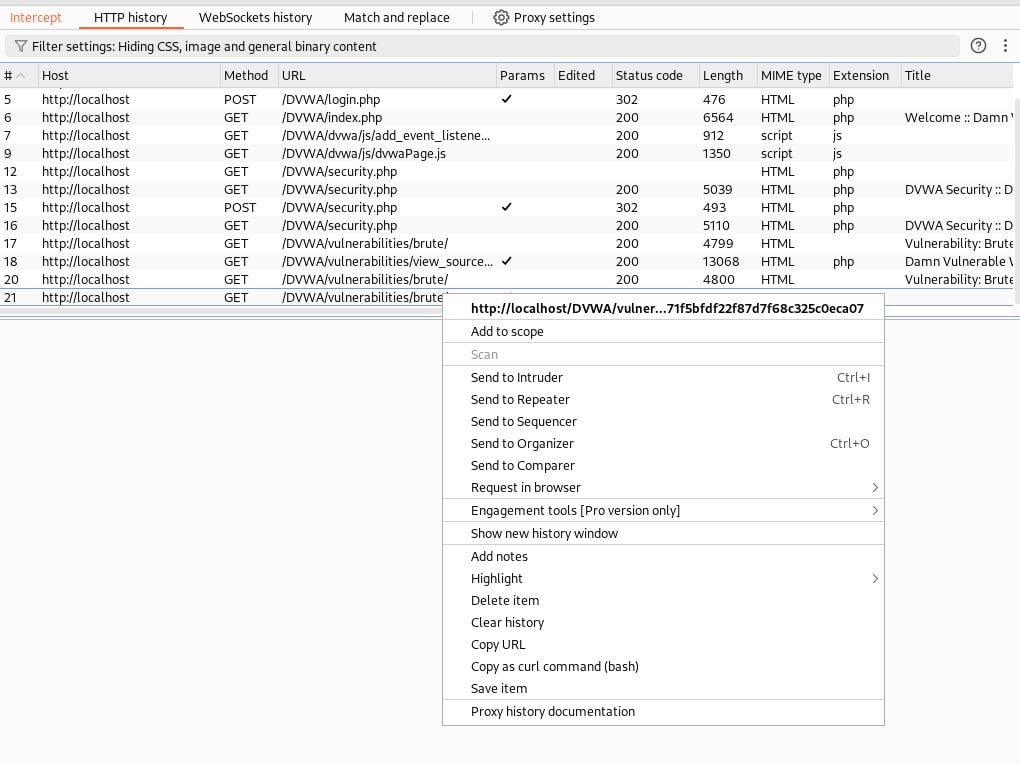


Рис. 11: Отправляем реквест взломщику

Теперь открываем вкладку “Intruder” - находим посланный нами реквест, выбираем тип атаки “Cluster Bomb” - стандартный брут форс - постоянный перебор и отправка реквестов, также выделяем значения параметра username и нажимаем “Add $”, так мы выделили первый параметр, который мы будем перебирать и посылать каждый реквест - аналогично делаем и со значением переменной password (рис. 12).

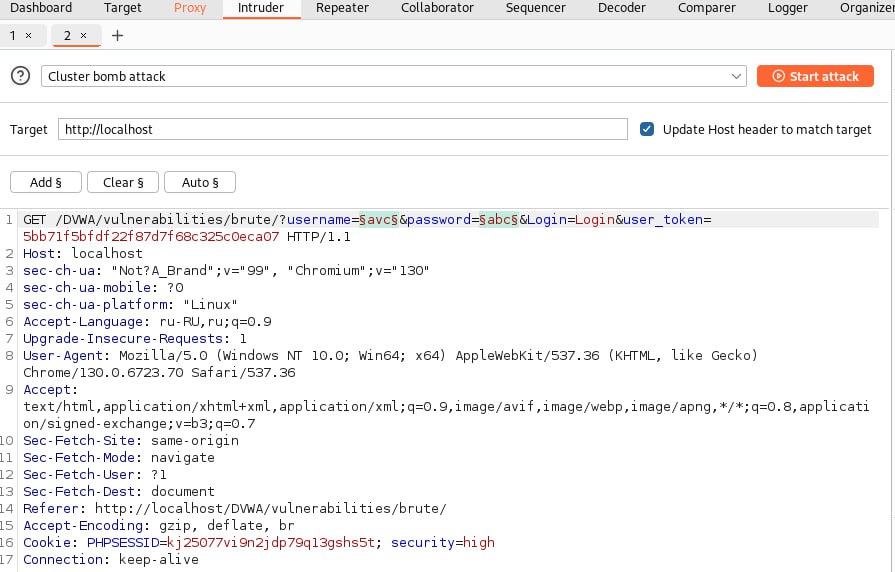


Рис. 12: Выделяем переменные для подбора пароля и логина

Открываем Payloads (тут мы настраиваем переменные, которые будем перебирать, т.к. мы перебираем логин и пароль, у нас их 2). Первый пейлоуд - выбираем, что будем перебирать: значения из файла, выбираем файл - в Kali есть стандартный список дефолтных логинов и паролей - они лежат в /usr/share/wordlists/metasploit. Для списка логинов выбираем http\_default\_users.txt (рис. 13).

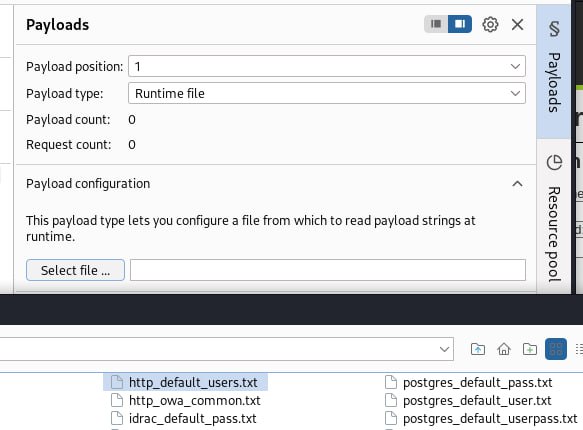


Рис. 13: Выбираем файл для перебора логинов

Аналогично делаем и для второго пейлоуда - перебор паролей - http\_default\_pass.txt (рис. 14).

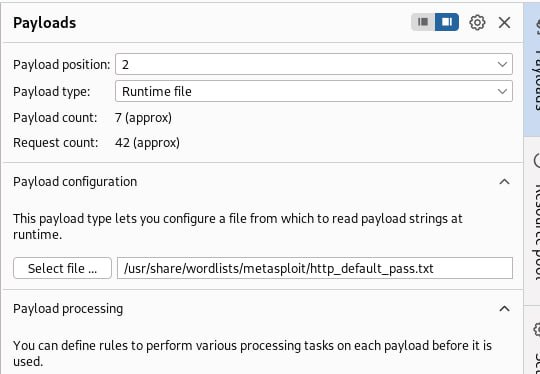


Рис. 14: Выбираем файл для перебора паролей - http\_default\_pass.txt

Открываем настройки Intruder, для наглядности добавим слово, за которым мы будем следить, и если оно появляется в коде странички - то мы ставим нашему реквесту флажок. Выбираем слово “incorrect”, тогда мы обратим внимание, что при правильном наборе логина и пароля флажка не будет (рис. 15).

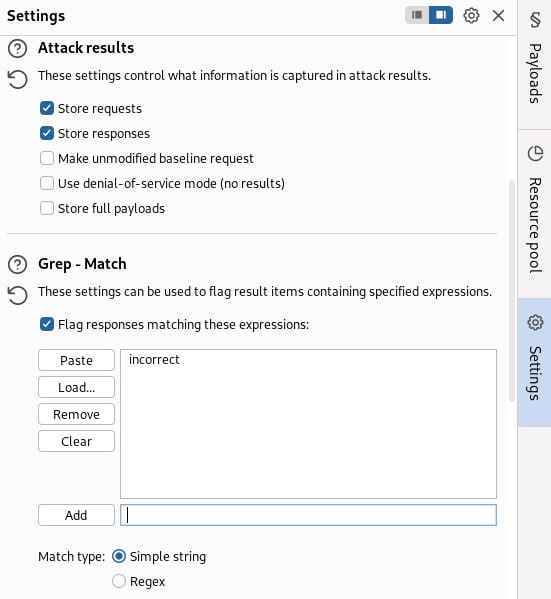


Рис. 15: Ставим маркер на слово incorrect

Запускаем нашего атакующего - начинаем брут форс. Наглядно видно, как посылается много реквестов. На фото я также их отсортировал по длине кода в страчничке. Обратим внимание, что тут в первой строке при логине admin и пароле password мало того, нету флажка Incorrect, так ещё и длина кода страничке значительно отличается от всех остальных - явно что-то особенное случилось при таком наборе логина и пароля. Обычно, взломщик в таком случае сам попробует такой набор логина и пароля (рис. 16).

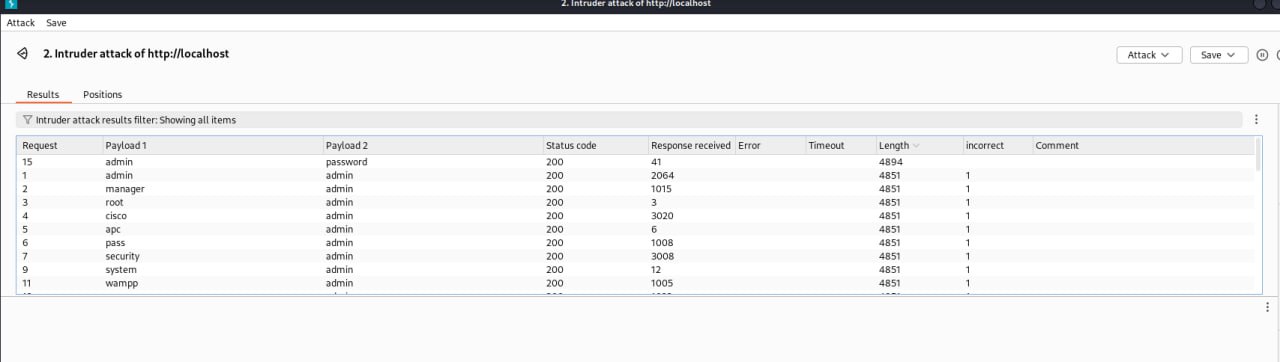


Рис. 16: Задокументированная брут форс атака

Вставляем такую комбинацию логина и пароля в страчнику входа и видим, что мы успешно прорвались в чужок аккаунт (рис. 17).

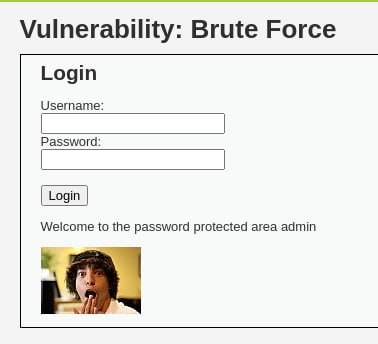


Рис. 17: Атака прошла успешно

# 3 Выводы

При выполнении данной работы я успешно получил навыки работы с Burp Suite.

# 4 Список литературы

[Индивидуальный проект](https://esystem.rudn.ru/mod/page/view.php?id=1220137#citeproc_bib_item_1)

[Brute Force DVWA разной сложности с использованием Burp Suite (На английском)](https://www.youtube.com/watch?v=pSBD9cgwgk0)