

# **Индивидуальный проект - Этап 5**

**Основы информационной безопасности**

Худдыева Дженнет

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
1.1	Введение . . . . .	4
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.0.1	О user_token . . . . .	7
<b>3</b>	<b>Выводы</b>	<b>16</b>
<b>4</b>	<b>Список литературы</b>	<b>17</b>

# Список иллюстраций

2.1	Инициализация Burp Suite . . . . .	5
2.2	DVWA через встроенный браузер . . . . .	6
2.3	Высокий уровень защиты DVWA . . . . .	6
2.4	Код странички входа на сложности High . . . . .	7
2.5	Новое правило в Burp Suite . . . . .	8
2.6	Новое макро действие в Burp Suite . . . . .	8
2.7	Отслеживание параметра user_token в каждом реквесте . . . . .	9
2.8	Сохранение макро действия . . . . .	9
2.9	Сохранение нового правила . . . . .	10
2.10	Перехват реквеста с попыткой входа . . . . .	10
2.11	Отправляем реквест взломщику . . . . .	11
2.12	Выделяем переменные для подбора пароля и логина . . . . .	12
2.13	Выбираем файл для перебора логинов . . . . .	12
2.14	Выбираем файл для перебора паролей - http_default_pass.txt . . . .	13
2.15	Ставим маркер на слово incorrect . . . . .	14
2.16	ЗадOCUMENTИРОВАННАЯ брут форс атака . . . . .	15
2.17	Атака прошла успешно . . . . .	15

# 1 Цель работы

Получение навыков пользования 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. 2.1).

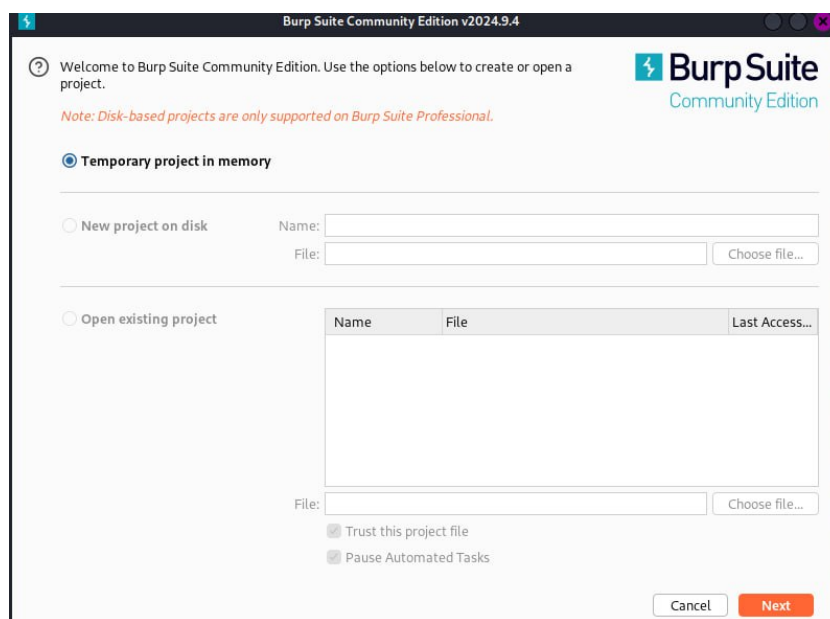


Рис. 2.1: Инициализация Burp Suite

Открываю встроенный в Burp Suite браузер и открываю в нём DVWA - всё как обычно (рис. 2.2).

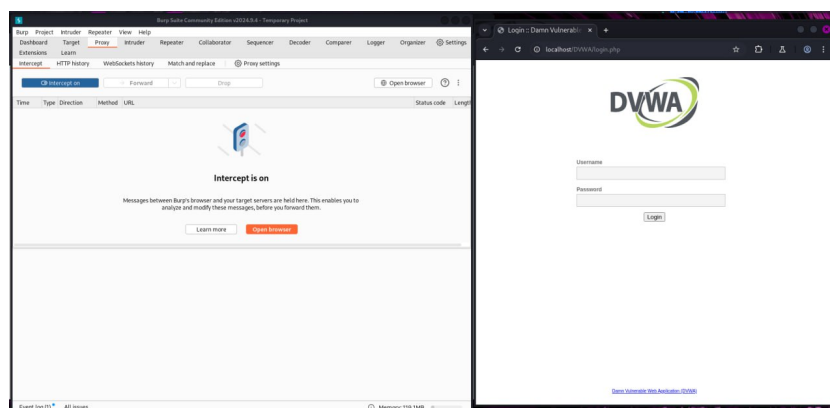


Рис. 2.2: DVWA через встроенный браузер

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. 2.3).

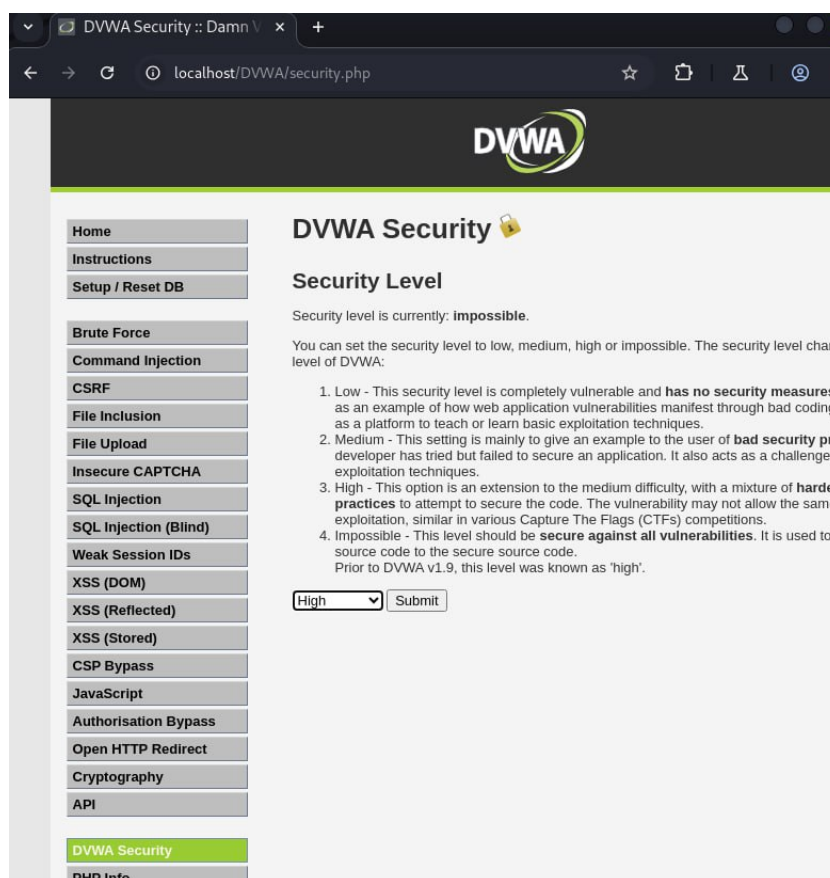


Рис. 2.3: Высокий уровень защиты DVWA

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. 2.4).

```
vulnerabilities/brute/source/high.php

<?php
if( isset( $GET[ 'Login' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $REQUEST[ 'user token' ], $SESSION[ 'session token' ], 'index.php' );

    // Sanitise username input
    $user = $GET[ 'username' ];
    $user = stripslashes( $user );
    $user = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $user) : addslashes($user));
    [MySQLConverterTool] Fix the mysql_escape_string() call! This code does not work.: E_USER_ERROR) ? "" : "");

    // Sanitise password input
    $pass = $GET[ 'password' ];
    $pass = stripslashes( $pass );
    $pass = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass) : addslashes($pass));
    [MySQLConverterTool] Fix the mysql_escape_string() call! This code does not work.: E_USER_ERROR) ? "" : "");
    $pass = md5( $pass );

    // Check database
    $query = "SELECT * FROM `users` WHERE user = '$user' AND password = '$pass'";
    $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '
```

Рис. 2.4: 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. 2.5).

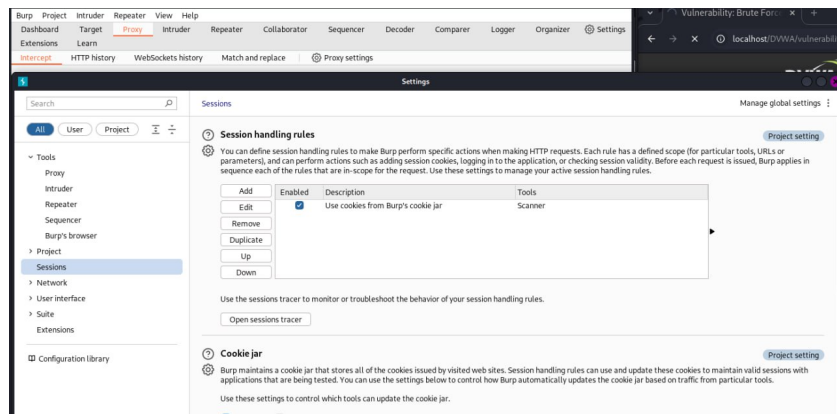


Рис. 2.5: Новое правило в Burp Suite

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 строки с user\_token (рис. 2.6).

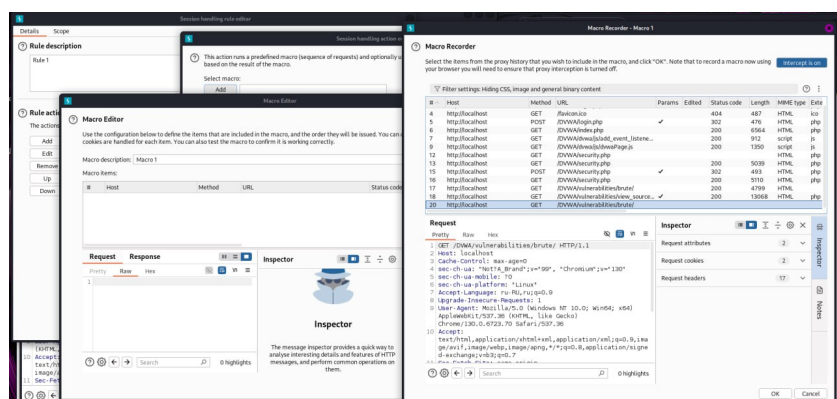


Рис. 2.6: Новое макро действие в Burp Suite

В открытом коде реквеста находим нужный параметр, за которым мы будем следить и запоминать - user\_token (рис. 2.7).



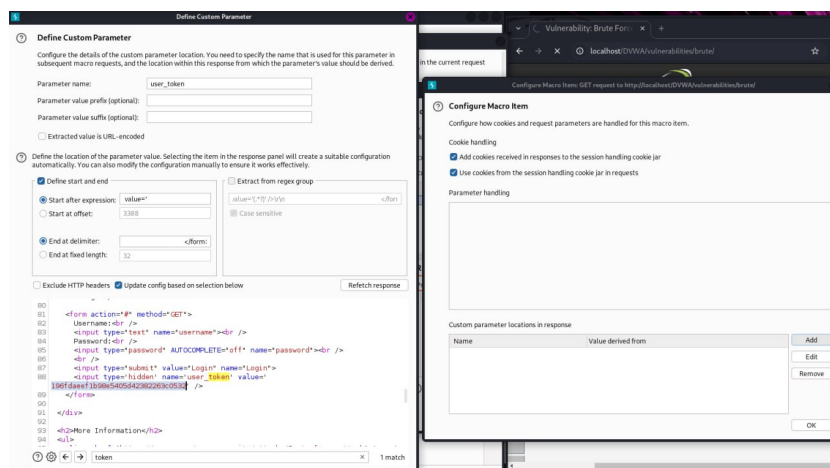


Рис. 2.7: Отслеживание параметра user\_token в каждом реквесте

Сохраняем наше макро действие, ставим галочку “Tolerate URL mismatch when matching parameters (Use for URL-agnostic CSRF tokens)” - тут написано ставить, если мы имеем дело с юзер токенами (рис. 2.8).

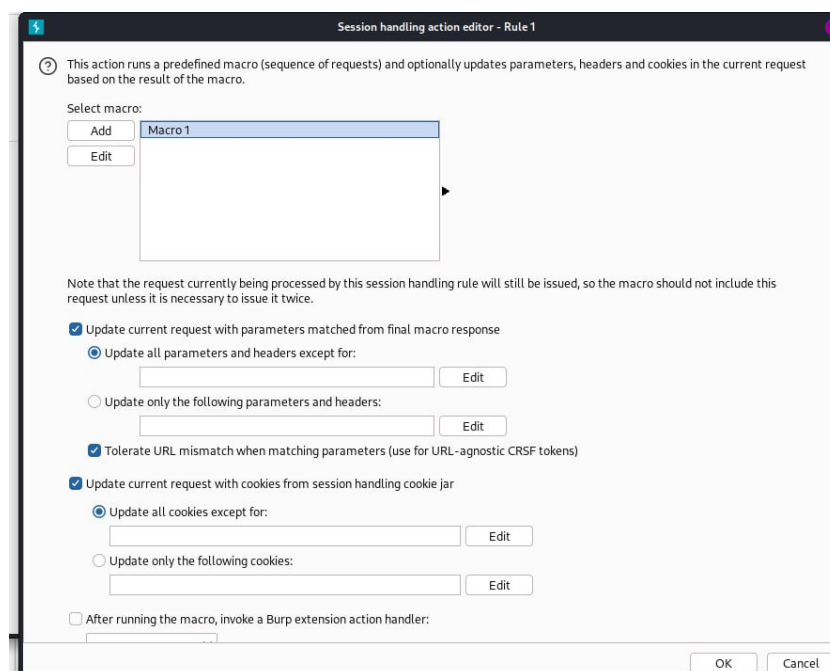


Рис. 2.8: Сохранение макро действия

Возвращаемся в настройку правила, выставляем галочки так, чтобы это правило применялось исключительно к инструменту Intruder - им мы будем пользо-

ваться для брут форса приложения (рис. 2.9).

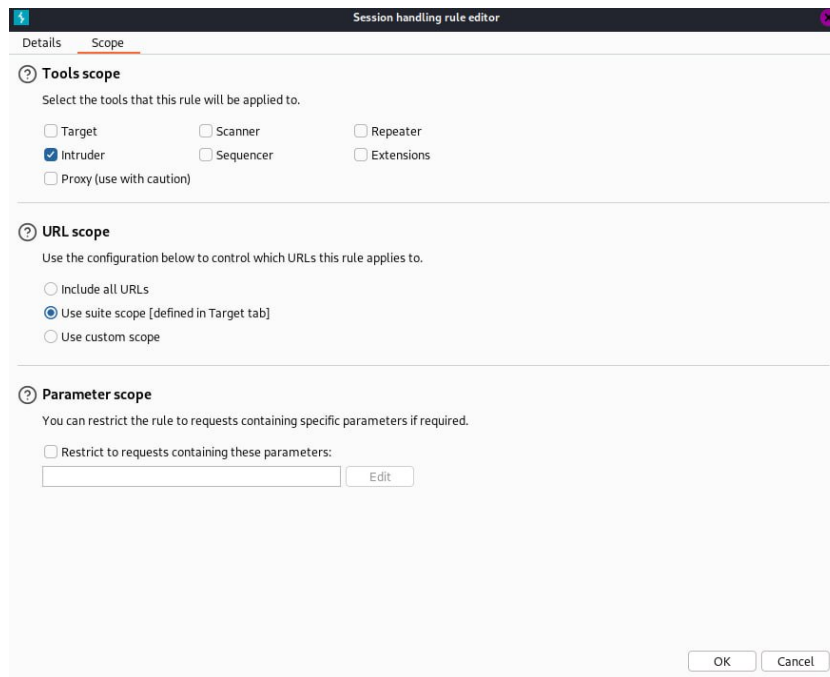


Рис. 2.9: Сохранение нового правила

Начнём. Включаем Interceptor - перехватываем реквест с попыткой входа (рис. 2.10).

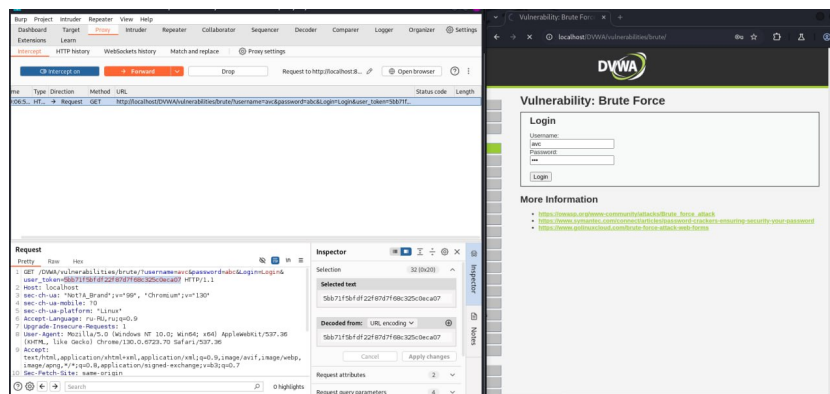


Рис. 2.10: Перехват реквеста с попыткой входа

Открываем вкладку HTTP-history и находим перехваченный реквест, нажимаем на него правой кнопкой и “Send to Intruder” (отправляем в инструмент взломщика), а затем “Add to scope” (рис. 2.11).

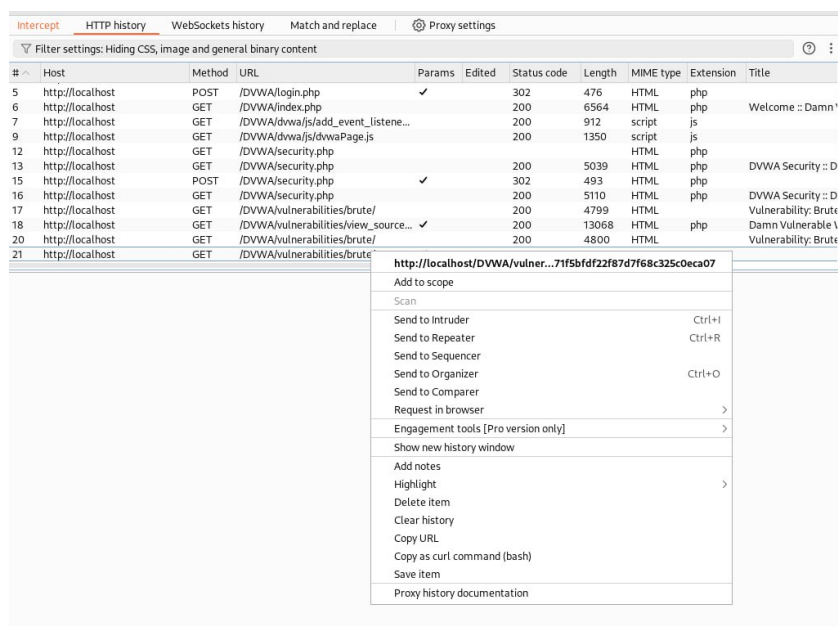


Рис. 2.11: Отправляем реквест взломщику

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. 2.12).

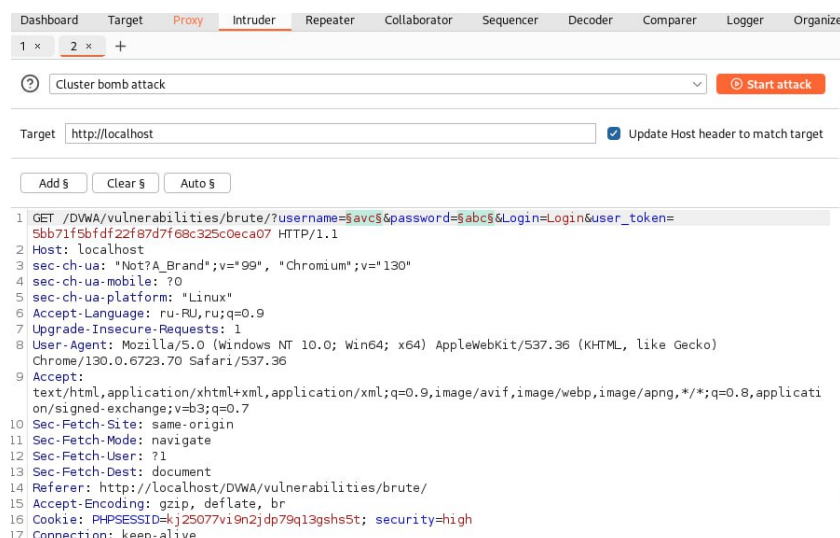


Рис. 2.12: Выделяем переменные для подбора пароля и логина

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. 2.13).

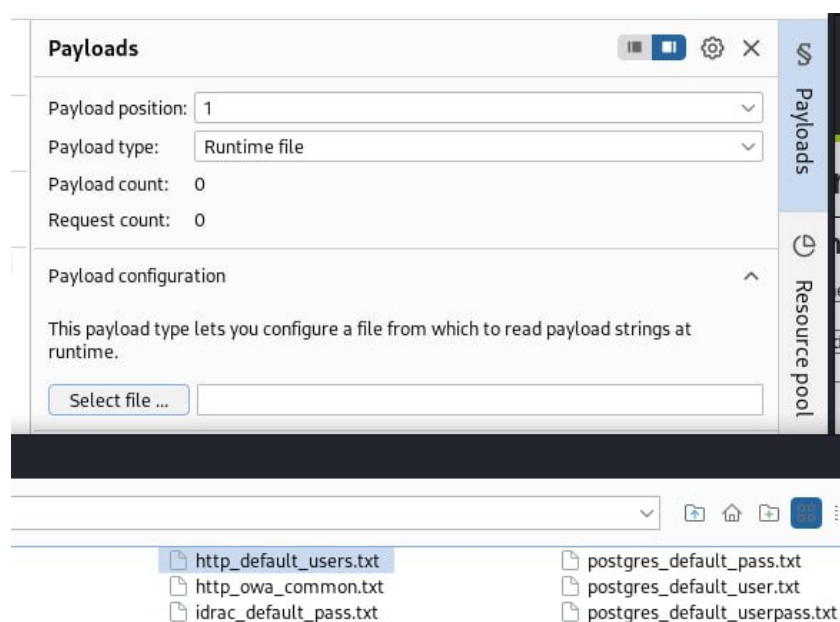


Рис. 2.13: Выбираем файл для перебора логинов

Аналогично делаем и для второго пейлоуда - перебор паролей - http\_default\_pass.txt (рис. 2.14).

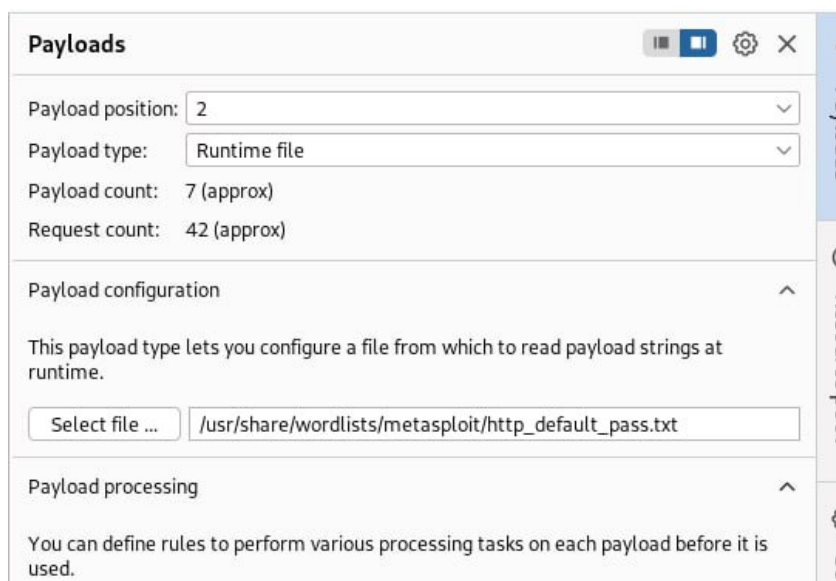


Рис. 2.14: Выбираем файл для перебора паролей - http\_default\_pass.txt

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. 2.15).

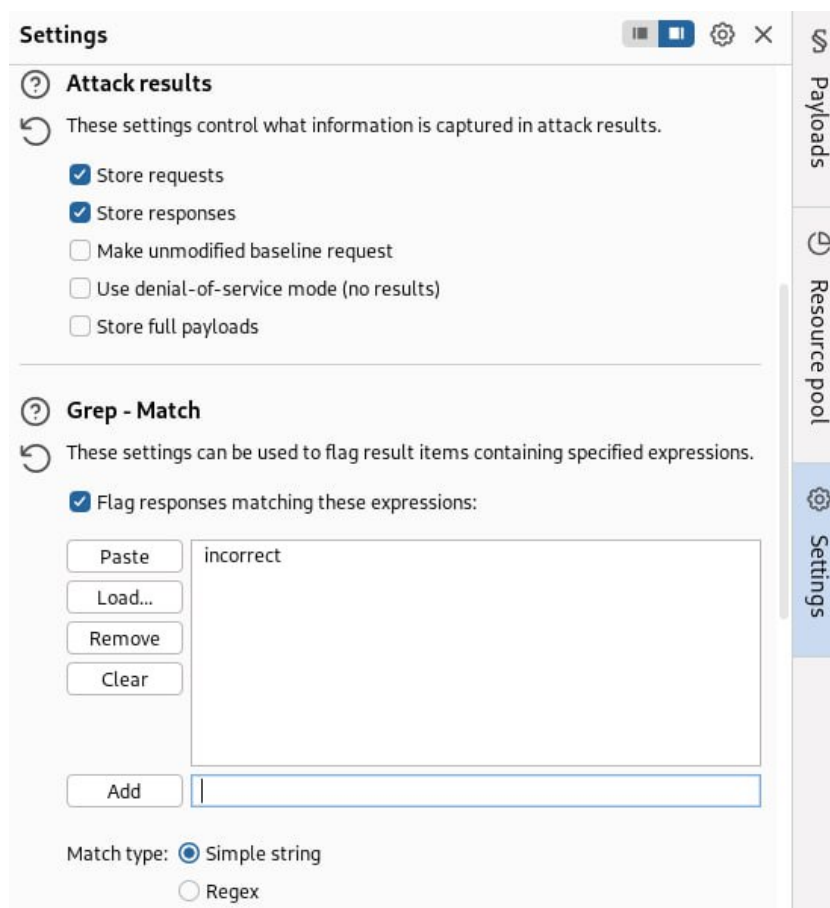


Рис. 2.15: Ставим маркер на слово incorrect

Запускаем нашего атакующего - начинаем брут форс. Наглядно видно, как посылается много реквестов. На фото я также их отсортировал по длине кода в страничке. 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. 2.16).

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Incorrect	Comment
15	admin	password	200	41			4894		
1	admin	admin	200	2054			4851	1	
2	manager	admin	200	1015			4851	1	
3	root	admin	200	3			4851	1	
4	cisco	admin	200	3020			4851	1	
5	sac	admin	200	6			4851	1	
6	pass	admin	200	1008			4851	1	
7	security	admin	200	3008			4851	1	
9	system	admin	200	12			4851	1	
11	wampp	admin	200	1005			4851	1	

Рис. 2.16: Задokumentированная брут форс атака

Вставляем такую комбинацию логина и пароля в страничку входа и видим, что мы успешно прорвались в чужок аккаунт (рис. 2.17).

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

Welcome to the password protected area admin

Рис. 2.17: Атака прошла успешно

## **3 Выводы**

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



## 4 Список литературы

Индивидуальный проект

Brute Force DVWA разной сложности с использованием Burp Suite (На английском)