

Пятый этап индивидуального проекта

Использование Burp Suite

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
4	Выводы	16
	Список литературы	17

Список иллюстраций

3.1	Скачивание Burp Suite	7
3.2	Установка ПО	7
3.3	Первоначальная настройка программы	8
3.4	Первоначальная настройка программы	8
3.5	Настройка прокси сервера	9
3.6	Настройки параметров	9
3.7	Страница авторизации	10
3.8	http история запросов	10
3.9	Попытка авторизации с неправильными данные, просмотр POST-запроса	11
3.10	Отправка запроса к Intruder	11
3.11	Задание параметров атаки	12
3.12	Первый Simple list	12
3.13	Второй Simple list	13
3.14	Результаты атаки	13
3.15	Результат неправильного запроса	14
3.16	Результат правильного запроса	14
3.17	Вкладка Repeater	15

1 Цель работы

Освоить навыки использования Burp Suite.

2 Теоретическое введение

Burp Suite – это платформа для выполнения тестирования по безопасности веб-приложений. В этой заметке я поделюсь несколькими приёмами, как использовать данный инструмент более эффективно[1].

Пакет состоит из набора утилит, среди которых есть инструменты для сбора и анализа информации, моделирования разных типов атак, перехвата запросов и ответов сервера и так далее.

- Target – создает карту сайта с подробной информацией о тестируемом приложении. Показывает, какие цели находятся в процессе тестирования, и позволяет управлять процессом обнаружения уязвимостей.
- Proxy – находится между браузером пользователя и тестируемым веб-приложением. Перехватывает все сообщения, передаваемые по протоколу HTTP(S).
- Spider – автоматически собирает данные о функциях и компонентах веб-приложения.
- Clickbandit – моделирует клиджекинг-атаки (clickjacking attacks), при которых поверх страницы приложения загружается невидимая страница, подготовленная злоумышленниками.
- DOM Invader – проверяет веб-приложение на уязвимость DOM-based межсайтовому скриптингу (основанному на объектной модели документа), внедрению вредоносного кода на страницу.
- Scanner (в профессиональной и корпоративной редакциях) — автоматически сканирует уязвимости в веб-приложениях. Также существует в

бесплатной версии, но, предоставляет только описание возможностей. Intruder – проводит автоматические атаки различного типа, от перебора открытых веб-директорий до внедрения SQL-кода.

- Repeater – утилита для ручного манипулирования и повторной выдачи отдельных HTTP-запросов и анализа ответов приложения. Отправить запрос в Repeater можно из любой другой утилиты Burp Suite.
- Sequencer – анализирует качество случайности в выборке элементов данных. Можно использовать для тестирования сеансовых маркеров приложения или других важных элементов данных, которые должны быть непредсказуемыми, например маркеров анти-CSRF, маркеров сброса пароля и так далее. Decoder— преобразовывает закодированные данные в исходную форму или необработанные в различные закодированные и хешированные формы. Способен распознавать несколько форматов кодирования, используя эвристические методы. Comparer – предоставляет функцию визуального сравнения различий данных.

3 Выполнение лабораторной работы

Скачаем Burp Suite с официального сайта (рис. 3.1).

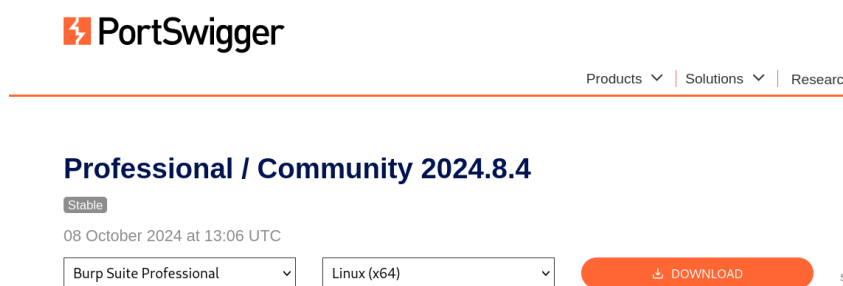


Рис. 3.1: Скачивание Burp Suite

Далее сделаем скачанный файл исполняемым и запустим его (рис. 3.2).

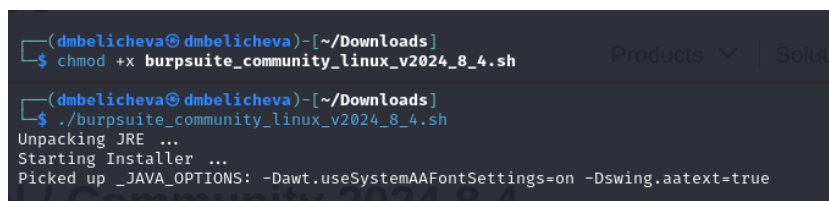


Рис. 3.2: Установка ПО

После того, как мы открыли Burp Suite идет первоначальная настройка программы. В первом окне выберем “Temporary project” (рис. 3.3).

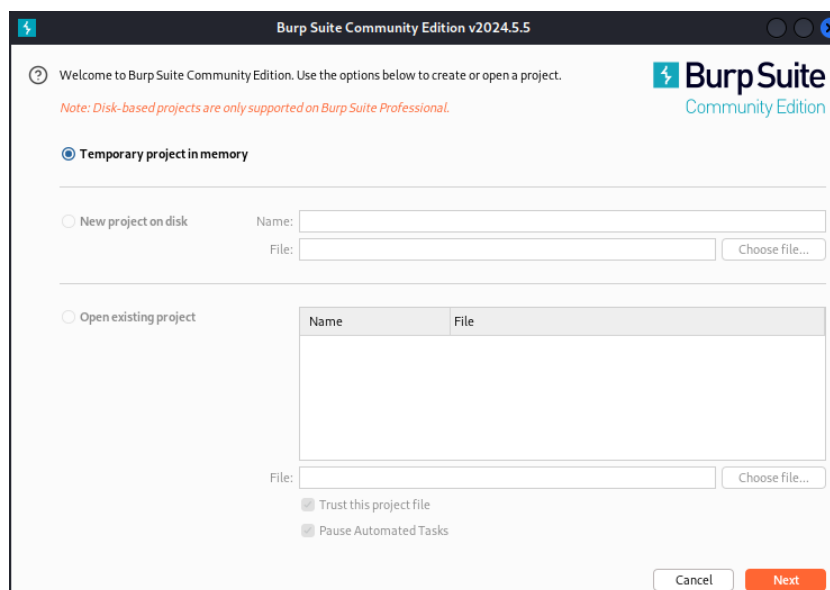


Рис. 3.3: Первоначальная настройка программы

Затем выберите “Use Burp defaults” (рис. 3.4).

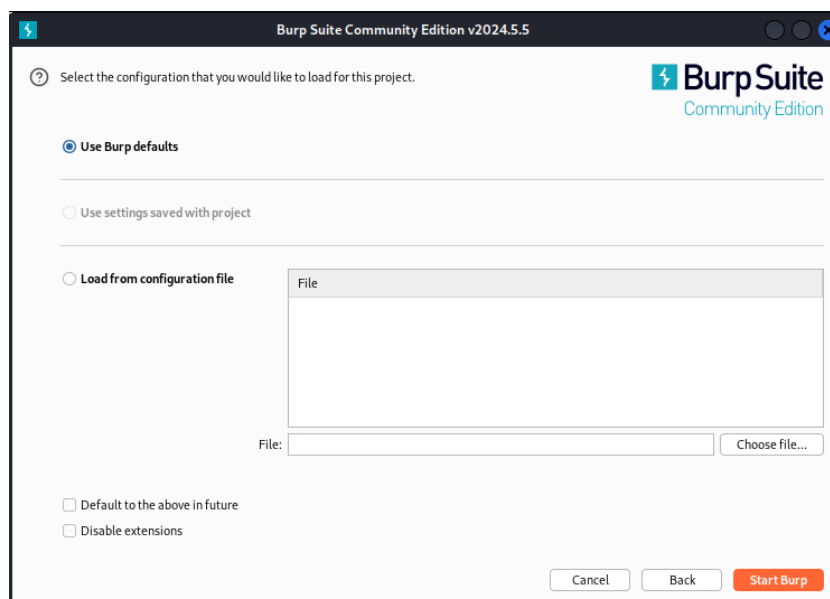


Рис. 3.4: Первоначальная настройка программы

Когда вы пропускаете запросы к сайтам через прокси Burp Suite, то программа позволяет вам редактировать на лету любой из запросов или ответов, вы можете отслеживать все передаваемые заголовки и многое другое. Когда вы запускаете

программу, прокси уже запущен, осталось только настроить браузер для работы с ним. Для этого перейдем в настройки прокси сервера в браузере и укажем там адрес прокси 127.0.0.1, а порт 8080 (рис. 3.5).

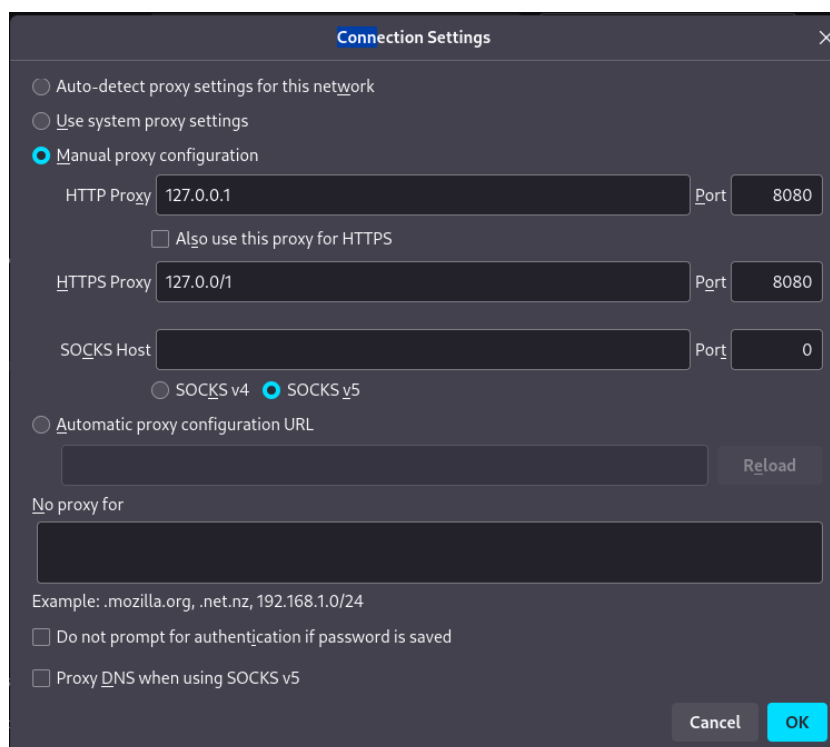


Рис. 3.5: Настройка прокси сервера

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_localhost` на `true` (рис. 3.6).

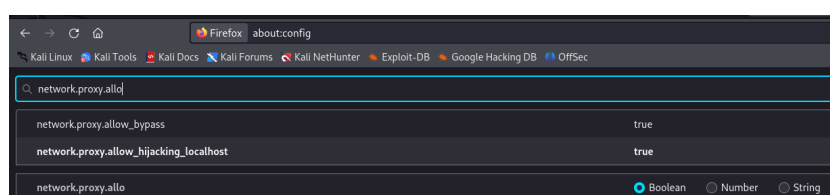


Рис. 3.6: Настройки параметров

Возвращаясь к Burp Suit, во вкладке Proxu устанавливаем “Intercept is on”. Будем проверять работу Burp Suit на DVWA (предварительно запустив для него все сервисы). Вводим в браузере адрес DVWA. Чтобы запрос обработался нам надо

выбрать запрос и нажать кнопку “Forward” в Burp Suite. Запрос успешно отправлен, и мы попали за страницу авторизации (рис. 3.7).

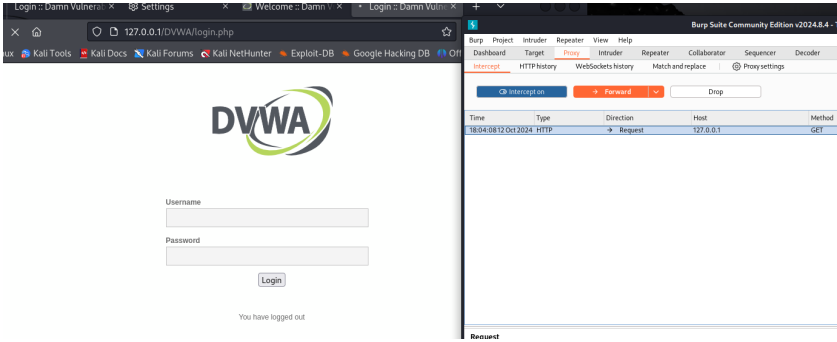


Рис. 3.7: Страница авторизации

Можем также посмотреть http историю запросов (рис. 3.8).

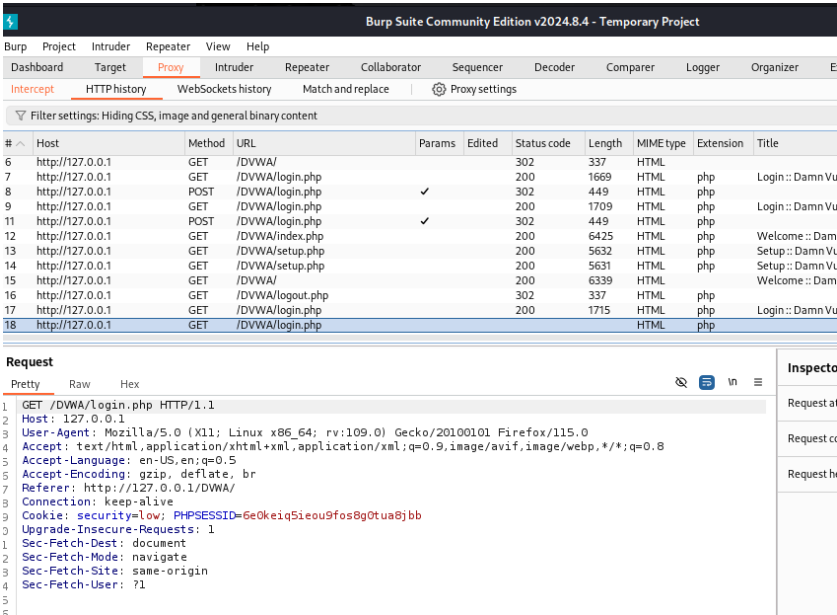


Рис. 3.8: http история запросов

Попробуем авторизоваться с неправильными данными и посмотреть на запрос. Можно увидеть в POST-запросе логин и пароль, с которыми была попытка авторизоваться (рис. 3.9).

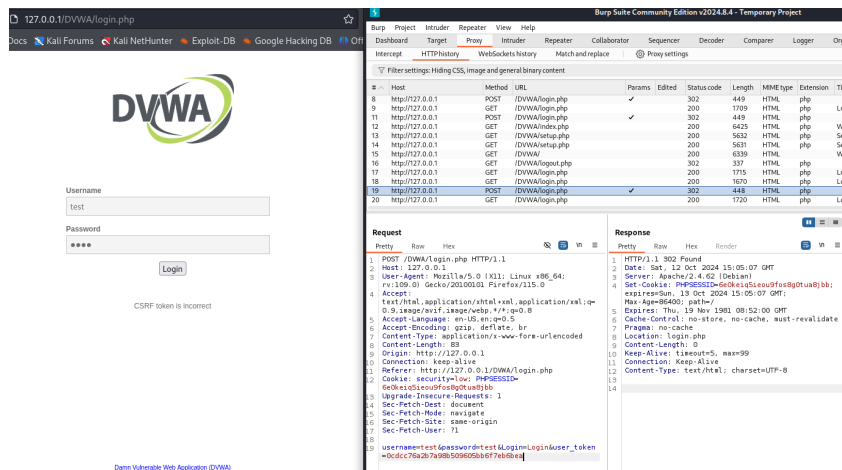


Рис. 3.9: Попытка авторизации с неправильными данные, просмотр POST-запроса

Отправим наш запрос к Intruder (рис. 3.10).

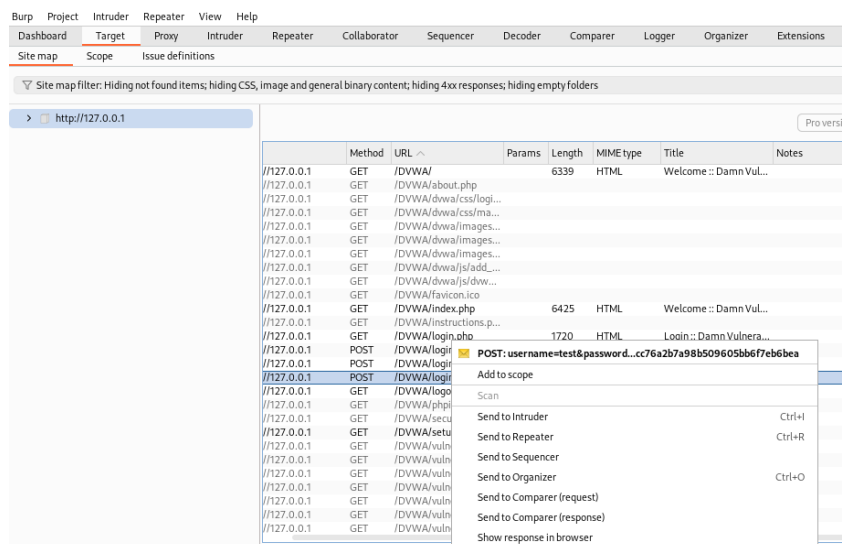


Рис. 3.10: Отправка запроса к Intruder

Здесь мы можем задать параметры атаки: ставим тип атаки Cluster bomb, обрабатываем логин и пароль в специальные символы (потому что подбирать будем их) (рис. 3.11).

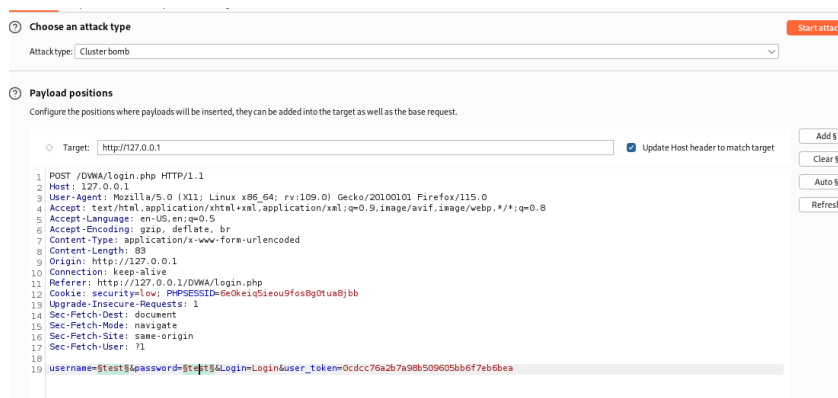


Рис. 3.11: Задание параметров атаки

Переходим к заданию Simple list. У нас их будет два: для логина и для пароля. Мы просто вручную введем сюда случайные данные, которые хотим проверить (не забудем ввести подходящий пароль) (рис. 3.12;3.13).

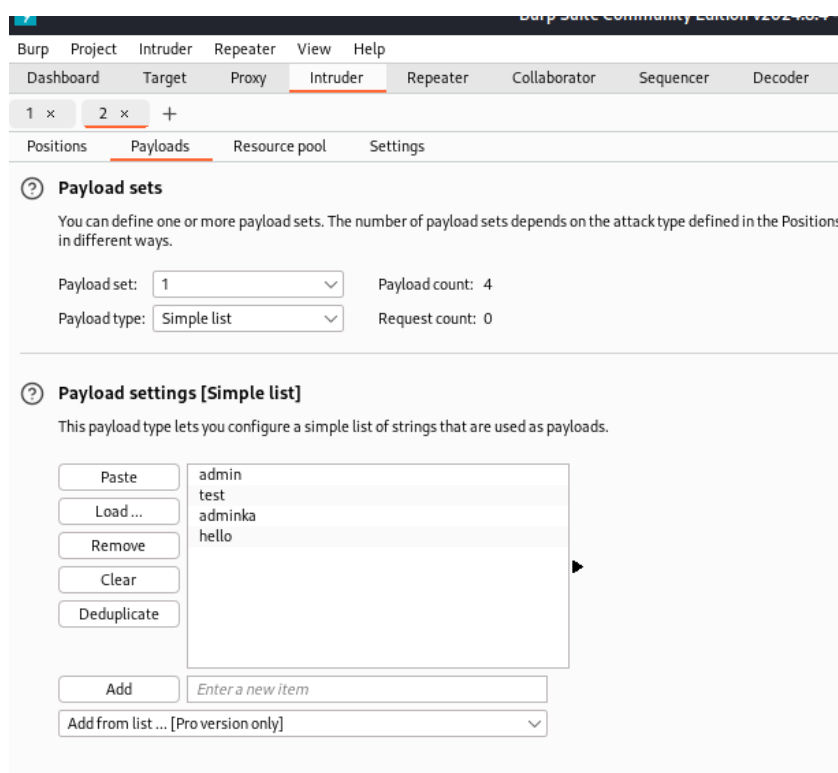


Рис. 3.12: Первый Simple list

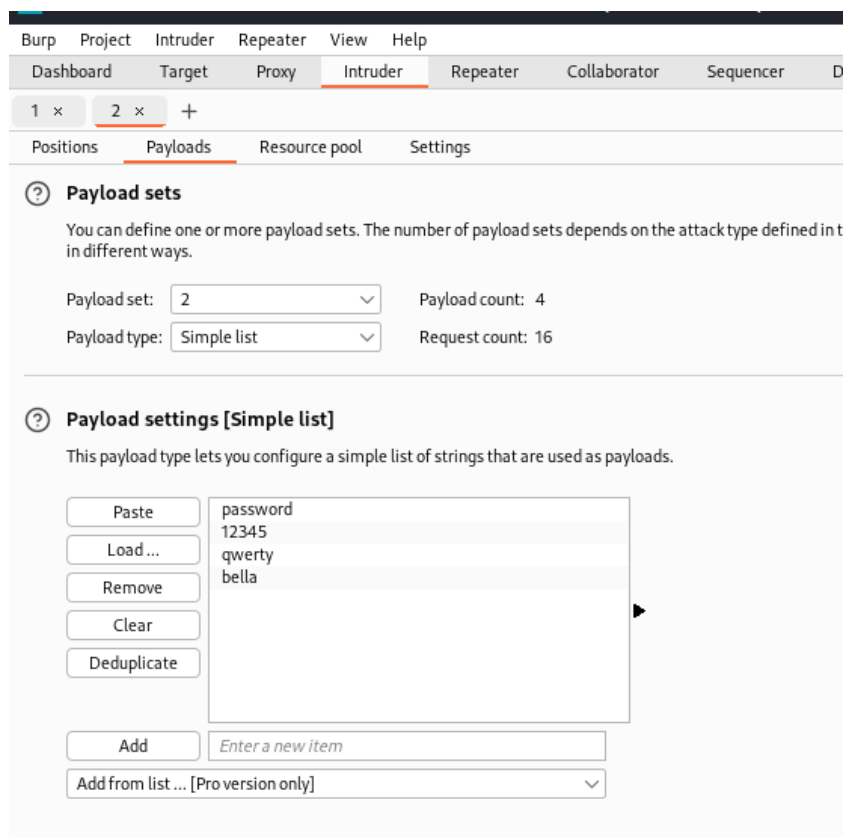


Рис. 3.13: Второй Simple list

Запускаем атаку, нам вывелось 16 возможных вариантов с введенными мною логинами и паролями (рис. 3.14).

The screenshot shows the Burp Suite Intruder interface with the 'Results' tab selected. The title bar says '2. Intruder attack of http://127.0.0.1'. The main area shows a table of results. The table has columns: Request, Payload1, Payload2, Status code, Response received, Error, Timeout, Length, and Comment. The table contains 16 rows of data, each representing a different combination of payload1 and payload2.

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0			302	3			449	
1	admin	password	302	0			448	
2	test	password	302	2			448	
3	adminika	password	302	4			448	
4	hello	password	302	3			449	
5	admin	12345	302	9			448	
6	test	12345	302	4			449	
7	adminika	12345	302	6			448	
8	hello	12345	302	4			449	
9	admin	qwerty	302	3			448	
10	test	qwerty	302	4			449	
11	adminika	qwerty	302	6			448	
12	hello	qwerty	302	4			449	
13	admin	bella	302	5			448	
14	test	bella	302	4			449	
15	adminika	bella	302	8			448	
16	hello	bella	302	16			449	

Рис. 3.14: Результаты атаки

Посмотрим на ответ полученный с использованием неправильных данных. Увидим, что мы остались на странице авторизации login.php (рис. 3.15).

Attack Save				
11. Intruder attack of http://127.0.0.1				
Results Positions Payloads Resource pool Settings				
Intruder attack results filter: Showing all items				
Request	Payload 1	Payload 2	Status code	Response received
0			302	6
1	admin	password	302	2
2	hello	password	302	4
3	adminika	password	302	6
4	testik	password	302	2
5	admin	12345	302	13
6	hello	12345	302	1
7	adminika	12345	302	4
8	testik	12345	302	3
9	admin	hello	302	2
10	hello	hello	302	3
11	adminika	hello	302	3
12	testik	hello	302	2
13	admin	muertv	302	14
Request Response				
Pretty Raw Hex Render				
1 HTTP/1.1 302 Found				
2 Date: Sat, 12 Oct 2024 15:41:54 GMT				
3 Server: Apache/2.4.62 (Debian)				
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT				
5 Cache-Control: no-store, no-cache, must-revalidate				
6 Pragma: no-cache				
7 Set-Cookie: PHPSESSID=e6sm4096m6jdpn0u5ngapgvb7; expires=Sun, 13 Oct 2024 15:41:54 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=				
8 Location: login.php				
9 Content-Length: 0				
10 Keep-Alive: timeout=5, max=98				
11 Connection: Keep-Alive				
12 Content-Type: text/html; charset=UTF-8				
13				

Рис. 3.15: Результат неправильного запроса

Посмотрим на ответ полученный с использованием правильных данных (admin, password). Увидим, что мы перешли на страницу DVWA index.php (рис. 3.16).

11. Intruder attack of http://127.0.0.1

Attack Save

11. Intruder attack of http://127.0.0.1

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload1	Payload2	Status code	Response received	Error
0			302	6	
1	admin	password	302	2	
2	hello	password	302	4	
3	adminika	password	302	6	
4	testik	password	302	2	
5	admin	12345	302	13	
6	hello	12345	302	1	
7	adminika	12345	302	4	
8	testik	12345	302	3	
9	admin	hello	302	2	
10	hello	hello	302	3	
11	adminika	hello	302	3	
12	testik	hello	302	2	
13	admin	muertv	302	14	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sat, 12 Oct 2024 15:41:54 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=npeqlgse5pj2d4lfee4s4b98jus; expires=Sun, 13 Oct 2024 15:41:54 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
```

Рис. 3.16: Результат правильного запроса

Также можем отправить результаты атаки к Repeater (рис. 3.17).

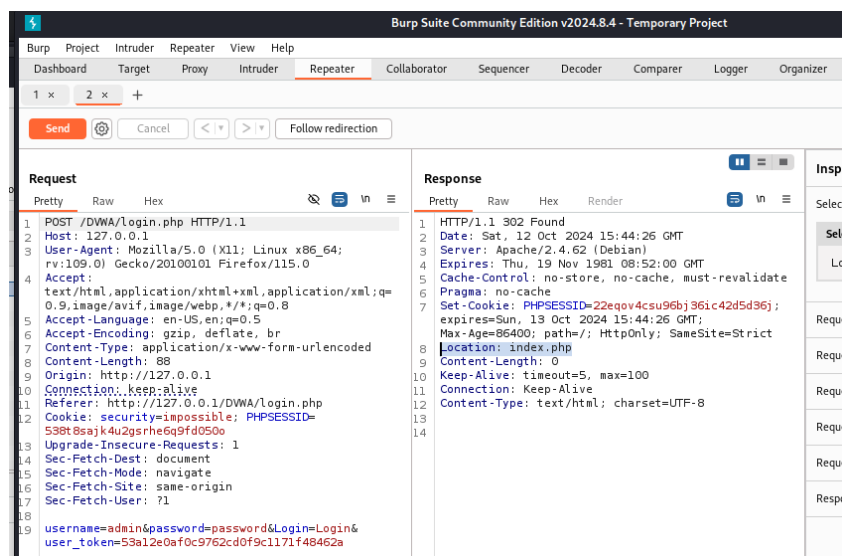


Рис. 3.17: Вкладка Repeater

4 Выводы

В результате выполнения данного этапа проекта я освоила навыки использования Burp Suite.

Список литературы

1. Burp Suite Tips [Электронный ресурс]. 2020. URL: <https://habr.com/ru/articles/510612/>.