

# Индивидуальный проект

## Этап 5

---

Кармацкий Н. С. Группа НФИбд-01-21

12 Октября 2024

Российский университет дружбы народов, Москва, Россия

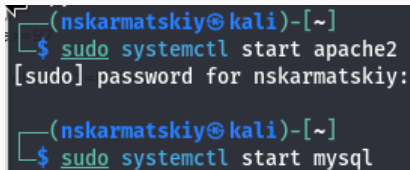
Научиться использовать Burp Suite.

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Эти инструменты позволяют сканировать, анализировать и использовать веб-приложения с помощью ручных и автоматических методов. Интеграция интерфейсов этих инструментов обеспечивает полную платформу атаки для обмена информацией между одним или несколькими инструментами, что делает Burp Suite очень эффективной и простой в использовании платформой для атаки веб-приложений

## Выполнение лабораторной работы

---

Запускаем локальный сервер Apache (рис. [-@fig:001]).



```
(nskarmatskiy@kali)-[~]  
$ sudo systemctl start apache2  
[sudo] password for nskarmatskiy:  
  
(nskarmatskiy@kali)-[~]  
$ sudo systemctl start mysql
```

Рис. 1: Запуск локального сервера

Запускаем инструмент Burp Suite (рис. [-@fig:002]).

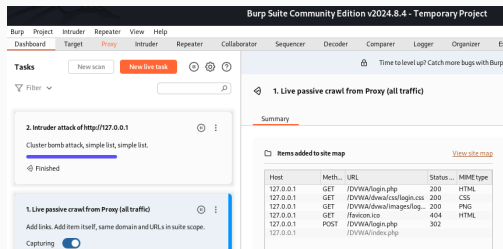


Рис. 2: Запуск приложения

Изменением настроек сервера для работы с прокси и захватом данных с помощью Burp Suite (рис. [-@fig:003]).

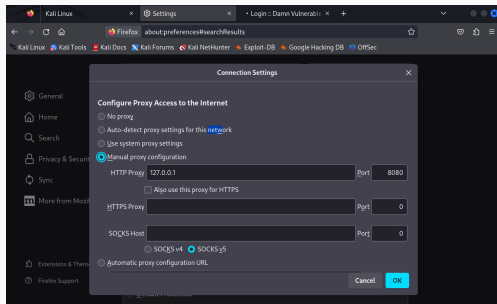


Рис. 3: Настройки сервера

Изменяем настройки Прoxy инструмента Burp Suite для дальнейшей работы (рис. [-@fig:004]).

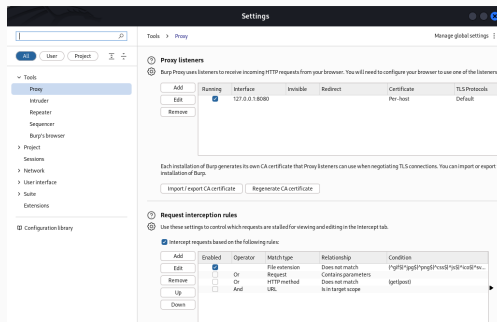


Рис. 4: Настройки Burp Suite



Во вкладке Проху устанавливаем “Intercept is on” (рис. [-@fig:005]).

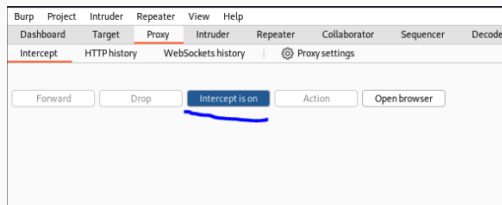


Рис. 5: Настройки Проху

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network.allow_hijacking_localhost` на `true` (рис. [-@fig:006]).

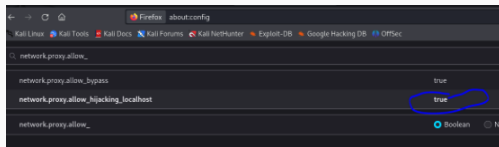


Рис. 6: Настройки параметров

Пытаемся зайти в браузере на DVWA, тут же во вкладки Проху появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. [-@fig:007]).

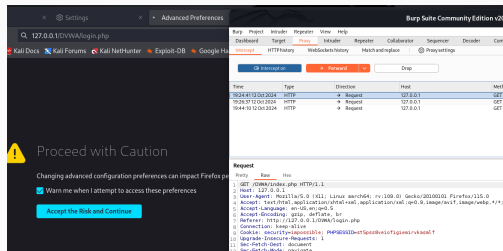


Рис. 7: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. [-@fig:008]).

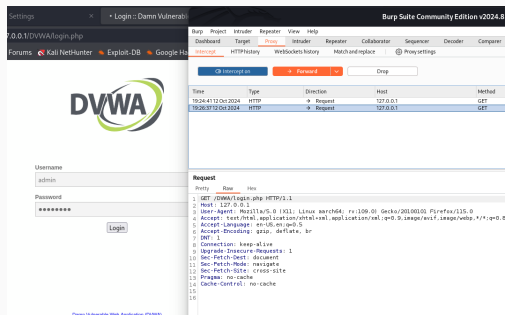


Рис. 8: Страница авторизации

История запросов хранится во вкладке Target (рис. [-@fig:009]).

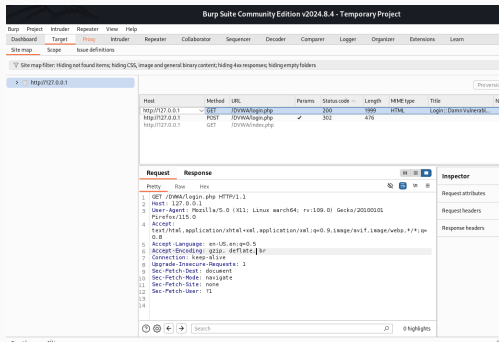


Рис. 9: История запросов

Попробуем ввести данные в веб-приложении и нажмем Login. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода (рис. [-@fig:010]).

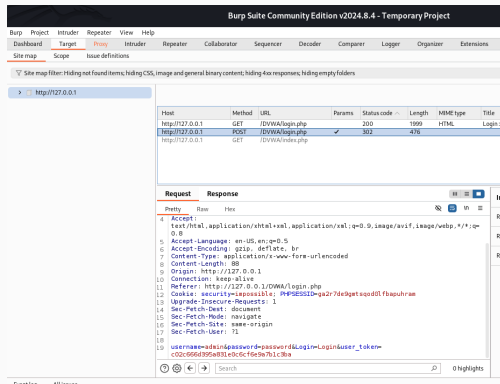


Рис. 10: Ввод случайных данных

Этот запрос так же можно найти во вкладке Target, там же жмем правой кнопкой мыши на хост нужного запроса, и далее нажимаем “Send to Intruder” (рис. [-@fig:011]).

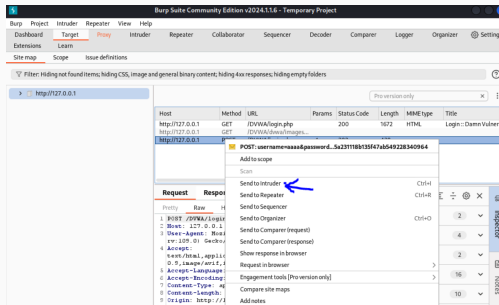


Рис. 11: POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. [-@fig:012]).

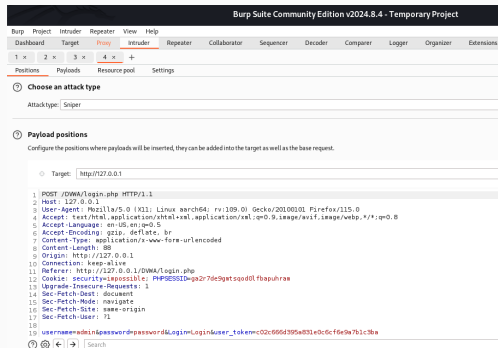


Рис. 12: Вкладка Intruder



Изменяем значение типа атаки на Cluster bomb и проставляем специальные символы у тех данных в форме для ввода, которые будем пробивать, то есть у имени пользователя и пароля (рис. [-@fig:013]).

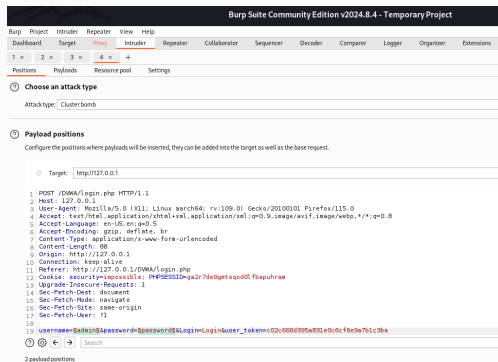


Рис. 13: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в Payload setting (рис. [-@fig:014]).

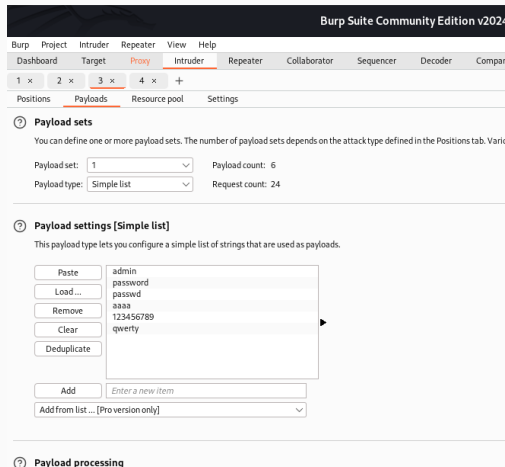


Рис. 14: Первый Simple list

Переключаемся на второй список и добавляем значения в него. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль (рис. [-@fig:015]).

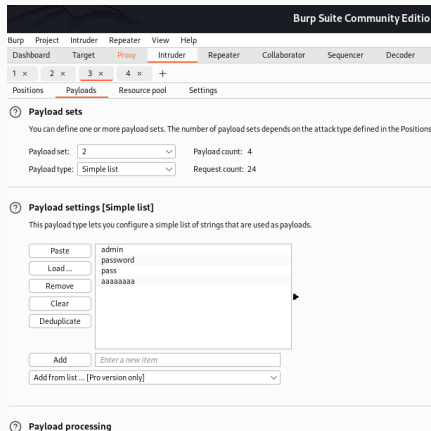


Рис. 15: Второй Simple list

Запускаем атаку и начинаем подбор (рис. [-@fig:016]).

Attack Stop

3. Intruder attack of http://127.0.0.1

Results Payloads Resource pool Settings

Intruder attack results filter (Showing all items)

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Content
0			302	3			476	
1	admin	admin	302	0			476	
2	password	admin	302	1			476	
3	password	admin	302	3			476	
4	user	admin	302	5			476	
5	123456789	admin	302	1			476	
6	qwerty	admin	302	4			476	
7	admin	password	302	3			476	
8	password	password	302	4			476	
9	password	password	302	1			476	
10	user	password	302	0			476	
11	123456789	password	302	2			476	
12	qwerty	password	302	0			476	
13	admin	user	302	3			476	
14	password	user	302	1			476	
15	password	user	302	1			476	
16	user	user	302	3			476	
17	123456789	user	302	1			476	
18	qwerty	user	302	3			476	
19	admin	00000000	302	0			476	
20	password	00000000	302	9			476	
21	password	00000000	302	1			476	
22	user	00000000	302	6			476	
23	123456789	00000000	302	7			476	
24	qwerty	00000000	302	6			476	

Рис. 16: Запуск атаки

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. В представленном случае с подбором пары admin-admin нас перенаправило на login.php, это значит, что пара не подходит (рис. [-@fig:017]).

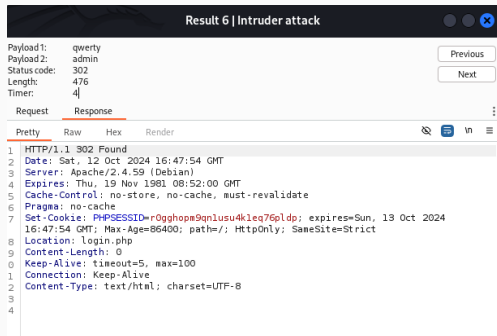


Рис. 17: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. [-@fig:018]).

6	qwerty	admin	302
7	admin	password	302
8	password	password	302
9	passwd	password	302

Request	Response
	<div>PrettyRawHexRender</div> <div>1 HTTP/1.1 302 Found 2 Date: Sat, 12 Oct 2024 16:29:54 GMT 3 Server: Apache/2.4.59 (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=k80v42ip01vpq8bi844a9bfcil; expires=Sun, 13 Oct 2024 16:29:54 GMT; Max-Age= 8 Location: index.php 9 Content-Length: 1 10 Keep-Alive: timeout=5, max=97 11 Connection: Keep-Alive 12 Content-Type: text/html; charset=UTF-8 13 14</div>

Рис. 18: Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и ждем “Send to Repeater” (рис. [-@fig:019]).

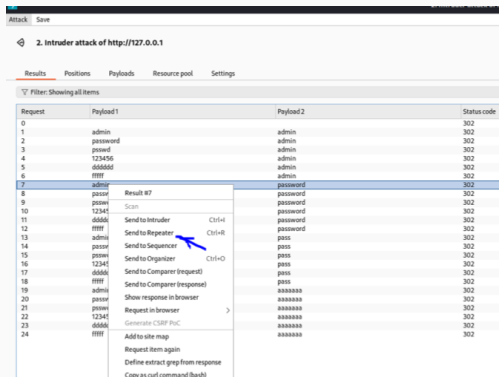


Рис. 19: Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. [-@fig:020]).

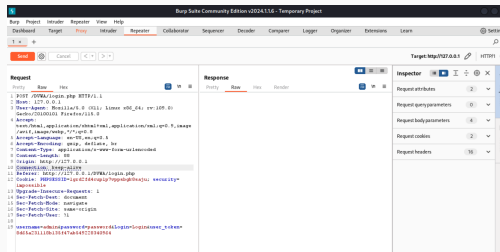


Рис. 20: Вкладка Repeater



Нажимаем “send”, получаем в Response в результат перенаправление на index.php (рис. [-@fig:021]).

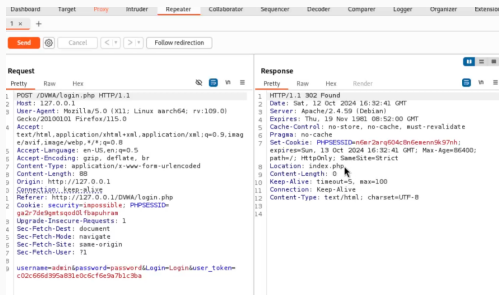


Рис. 21: Окно Response

После нажатия на Follow redirection, получим неcompiled html код в окне Response (рис. [-@fig:022]).

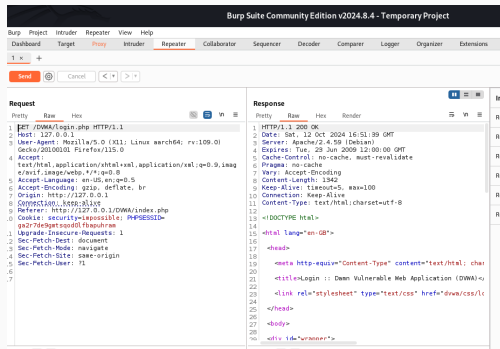


Рис. 22: Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная страница (рис. [-@fig:023]).

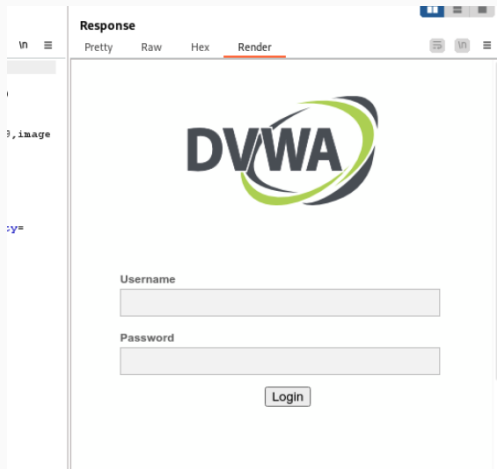


Рис. 23: Полученная страница

Научились использовать инструмент Burp Suite