Индивидуальный проект Этап №5

Использование Burp Suite

Чванова Ангелина Дмитриевна

2024 год

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Чванова Ангелина Дмитриевна
- студент
- Российский университет дружбы народов
- angelinachdm@gmail.com
- https://adchvanova-new.github.io/ru/

Цель работы

Научиться использовать Burp Suite.

Теоретическое введение

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, на котором необходимо открыть веб-приложение DVWA для тестирования инструмента Burp Suite

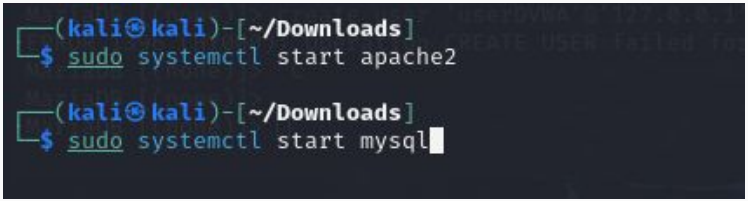


Рис. 1: Запуск локального сервера

Выполнение лабораторной работы

Запускаем инструмент Burp Suite

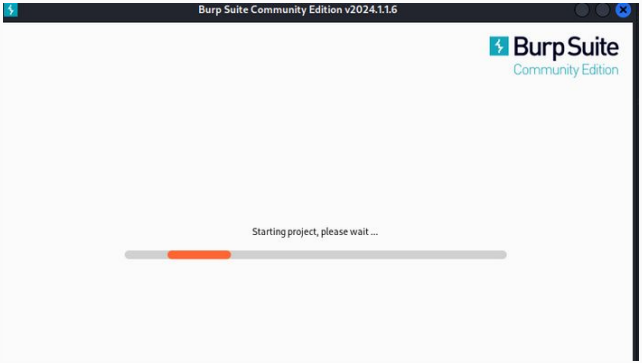


Рис. 2: Запуск приложения

Выполнение лабораторной работы

Открываем сетевые настройки браузера для подготовки к работе

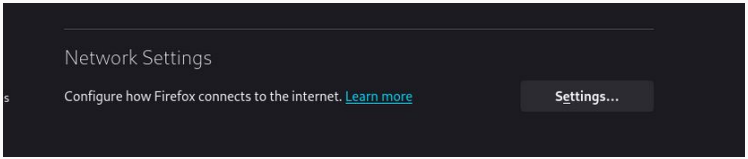
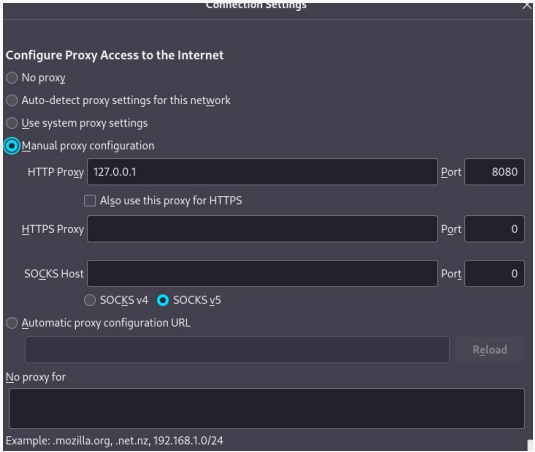


Рис. 3: Сетевые настройки браузера

Выполнение лабораторной работы

Изменение настроек сервера для работы с proxy и захватом данных с помощью Burp Suite



Выполнение лабораторной работы

Изменяем настройки Proxy инструмента Burp Suite

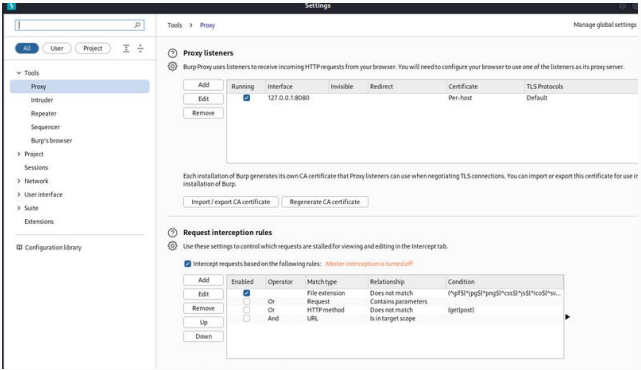


Рис. 5: Настройки Burp Suite

Выполнение лабораторной работы

Устанавливаем значение “Intercept is on” во вкладке Proxy

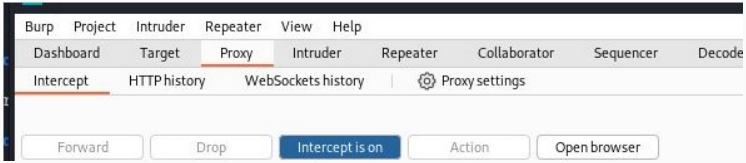


Рис. 6: Настройки Proxy

Выполнение лабораторной работы

Чтобы Burp Suite исправно работал с локальным сервером, необходимо установить параметр `network_allow_hijacking_loacalhost` на `true`

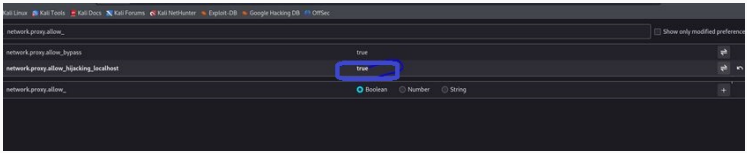


Рис. 7: Настройки параметров

Выполнение лабораторной работы

При входе в браузер на DVWA, во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу

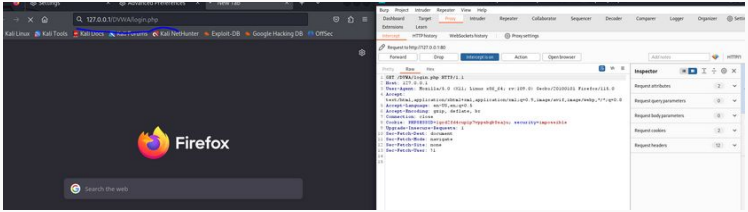


Рис. 8: Получаемые запросы сервера

Выполнение лабораторной работы

Загружаем страницу авторизации, текст запроса поменялся

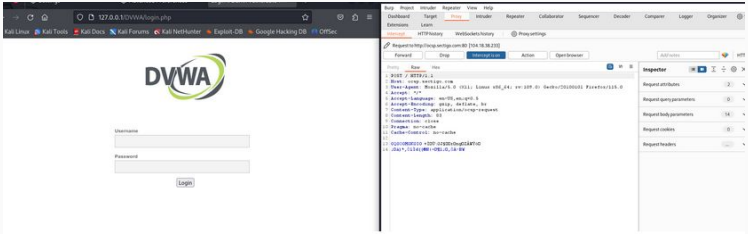


Рис. 9: Страница авторизации

Выполнение лабораторной работы

История запросов хранится во вкладке Target

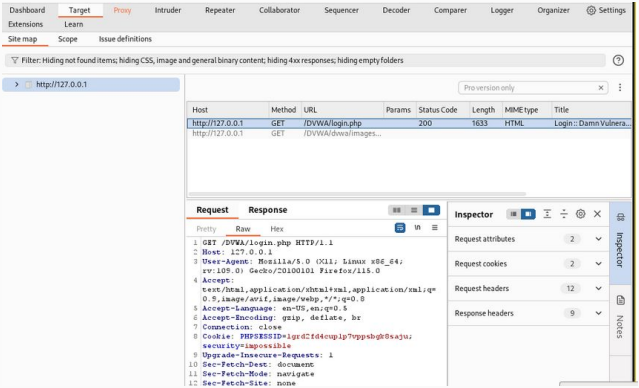


Рис. 10: История запросов

Выполнение лабораторной работы

Попробуем ввести неправильные, случайные данные в веб-приложении и нажмем `Login`. В запросе увидим строку, в которой отображаются введенные нами данные, то есть поле для ввода

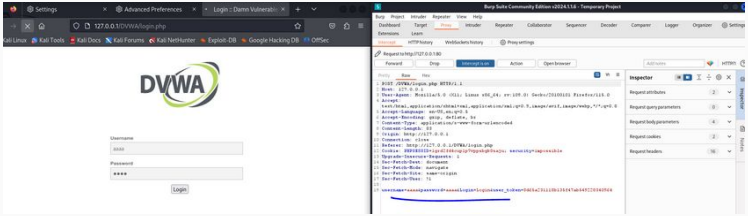
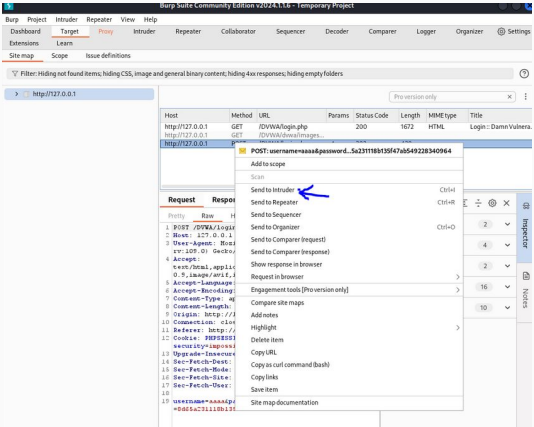


Рис. 11: Ввод случайных данных

Выполнение лабораторной работы

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”



Выполнение лабораторной работы

На вкладке Intruder видим значения по умолчанию у типа атаки и наш запрос

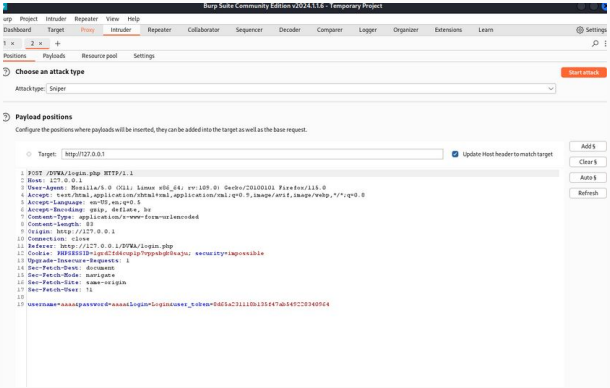


Рис. 13: Вкладка Intruder

Выполнение лабораторной работы

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

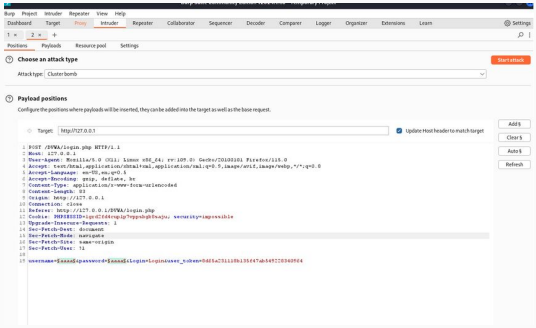


Рис. 14: Изменение типа атаки

Выполнение лабораторной работы

Так как мы отметили 2 параметра для подбора, то нам необходимо 2 списка со значениями для подбора. Заполняем первый список в `Payload setting`

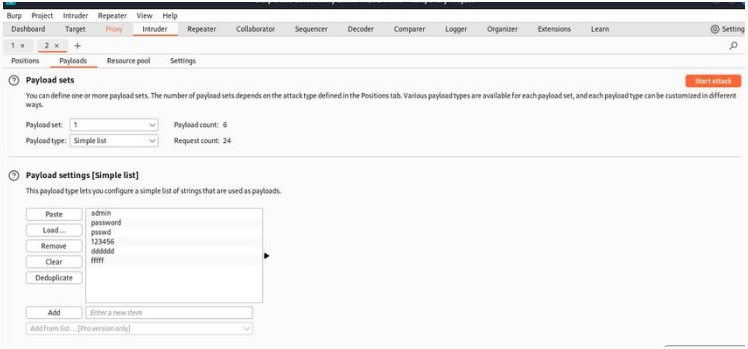


Рис. 15: Первый Simple list

Выполнение лабораторной работы

Заполняем значениями второй список. В строке request count видим нужное количество запросов, чтобы проверить все возможные пары пользователь-пароль

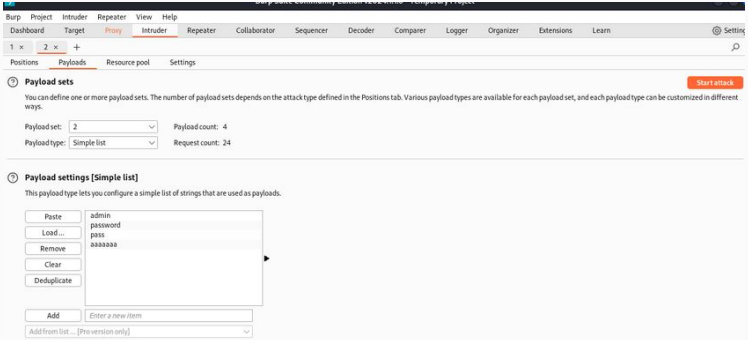
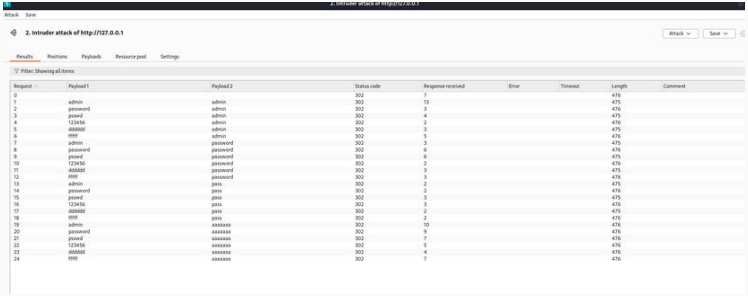


Рис. 16: Второй Simple list

Выполнение лабораторной работы

Запускаем атаку и начинаем подбор

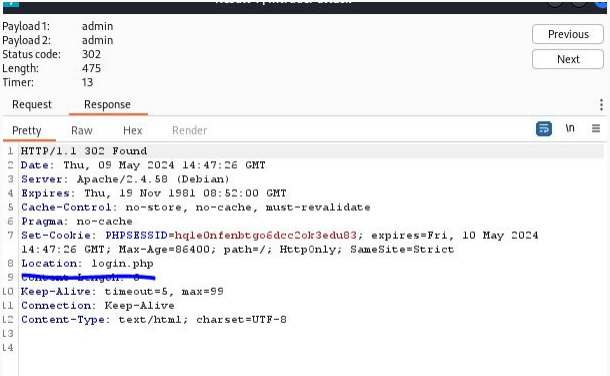


Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	7			476	
1	admin	admin	302	13			475	
2	password	admin	302	3			476	
3	psswd	admin	302	4			475	
4	123456	admin	302	2			476	
5	666888	admin	302	3			475	
6	ffffff	admin	302	5			476	
7	admin	password	302	3			475	
8	password	password	302	6			476	
9	psswd	password	302	6			475	
10	123456	password	302	2			476	
11	666888	password	302	3			475	
12	ffffff	password	302	3			476	
13	admin	pass	302	2			476	
14	password	pass	302	2			476	
15	psswd	pass	302	3			475	
16	123456	pass	302	3			476	
17	666888	pass	302	2			475	
18	ffffff	pass	302	2			476	
19	admin	aaaaaaa	302	10			476	
20	password	aaaaaaa	302	9			476	
21	psswd	aaaaaaa	302	7			476	
22	123456	aaaaaaa	302	5			476	
23	666888	aaaaaaa	302	4			476	
24	ffffff	aaaaaaa	302	7			476	

Рис. 17: Запуск атаки

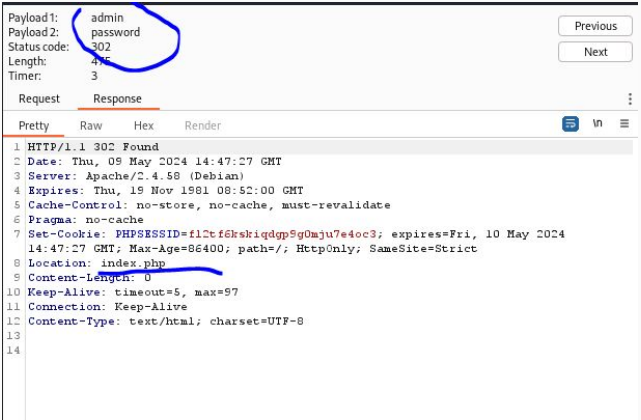
Выполнение лабораторной работы

При открытии результата каждого post-запроса можно увидеть полученный get-запрос, в нем видно, куда нас перенаправило после выполнения ввода пары пользователь-пароль. admin-admin нас перенаправило на login.php, это значит, что пара не подходит



Выполнение лабораторной работы

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной



Выполнение лабораторной работы

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater”

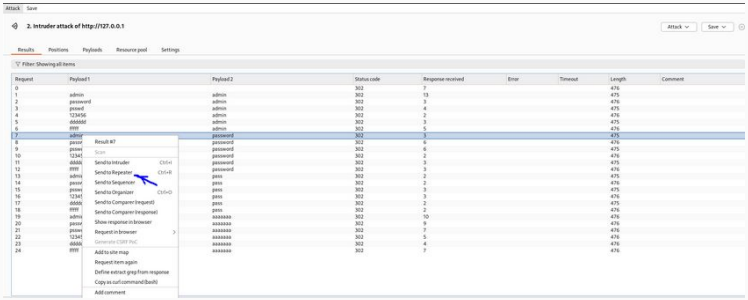


Рис. 20: Дополнительная проверка результата

Выполнение лабораторной работы

Переходим во вкладку “Repeater”

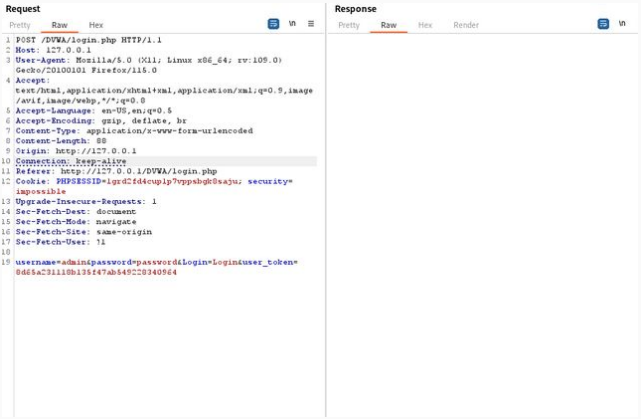


Рис. 21: Вкладка Repeater

Выполнение лабораторной работы

Нажимаем “send”, получаем в Response в результат перенаправление на index.php

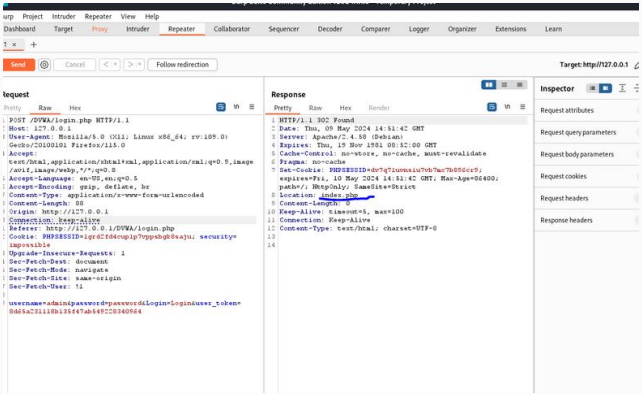


Рис. 22: Окно Response

Выполнение лабораторной работы

После нажатия на `Follow redirection`, получим нескомпилированный html код в окне Response

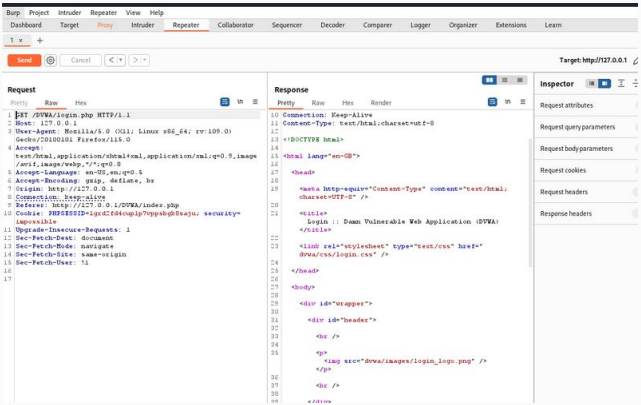


Рис. 23: Изменение в окне Response

Выполнение лабораторной работы

Далее в подокне Render получим то, как выглядит полученная страница

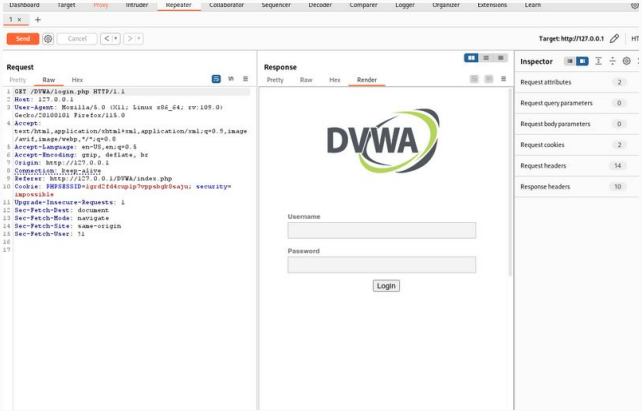


Рис. 24: Полученная страница

Выводы

При выполнении лабораторной работы научилась использовать инструмент Burp Suite.

Список литературы

[1] Документация по Virtual Box:
https://www.virtualbox.org/wiki/Documentation

[2] 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