Отчет по пятому этапу индивидуального проекта

Информационная безопасность

Кармацкий Никита Сергеевич

Содержание

Список иллюстраций

1 Цель работы

Научиться использовать Burp Suite.

2 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. [**parasram?**].

3 Выполнение лабораторной работыё

Запускаем локальный сервер Apache (рис. 1).

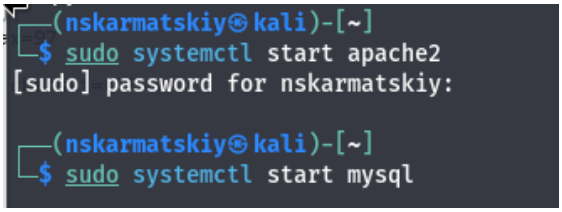


Рис. 3.1: Запуск локального сервера

Запускаем инструмент Burp Suite (рис. 3.2).

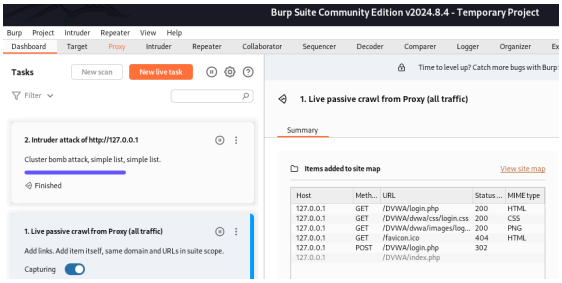


Рис. 3.2: Запуск приложения

Измененяем настроек сервера для работы с proxy и захватом данных

с помощью Burp Suite (рис. 3.3).

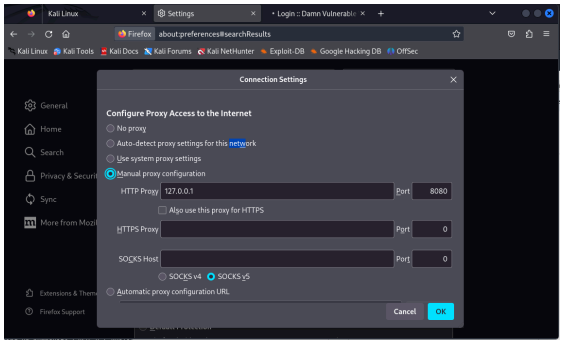


Рис. 3.3: Настройки сервера

Изменяем настройки Proxy инструмента Burp Suite для дальнейшей работы (рис. 3.4).

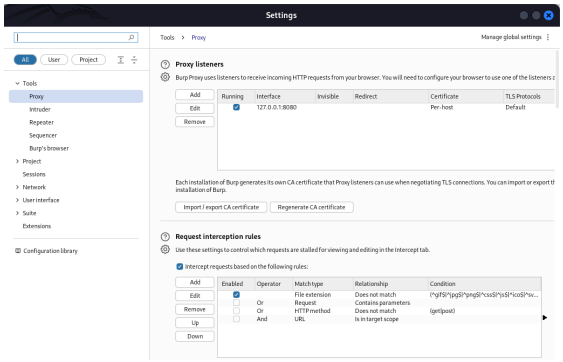


Рис. 3.4: Настройки Burp Suite

Во вкладке Proxy устанавливаем “Intercept is on” (рис. 3.5).

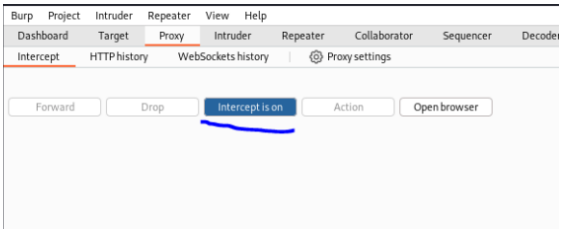


Рис. 3.5: Настройки Proxy

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

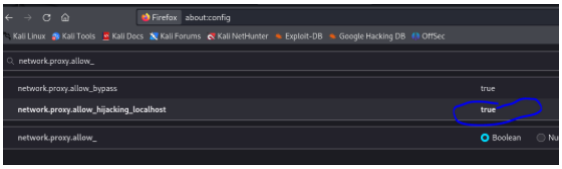


Рис. 3.6: Настройки параметров

Пытаемся зайти в браузере на DVWA, тут же во вкладки Proxy появляется захваченный запрос. Нажимаем “Forward”, чтобы загрузить страницу (рис. 3.7).

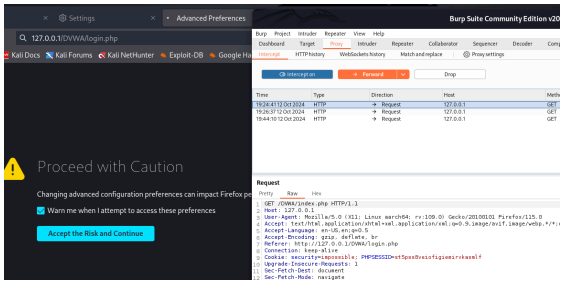


Рис. 3.7: Получаемые запросы сервера

Загрузилась страница авторизации, текст запроса поменялся (рис. 3.8).

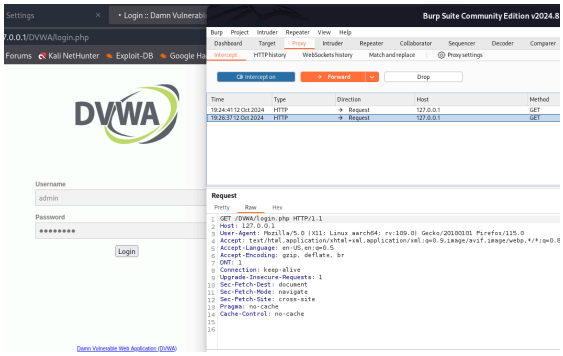


Рис. 3.8: Страница авторизации

История запросов хранится во вкладке Target (рис. 3.9).

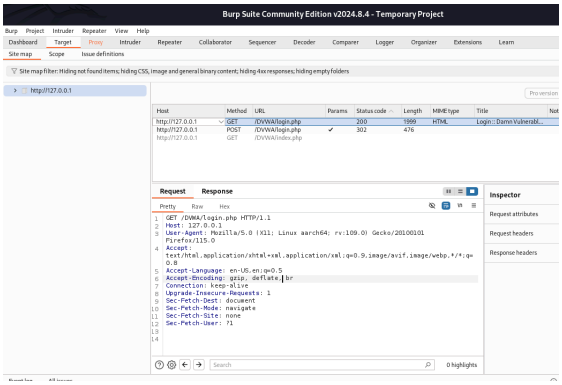


Рис. 3.9: История запросов

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. 3.10).

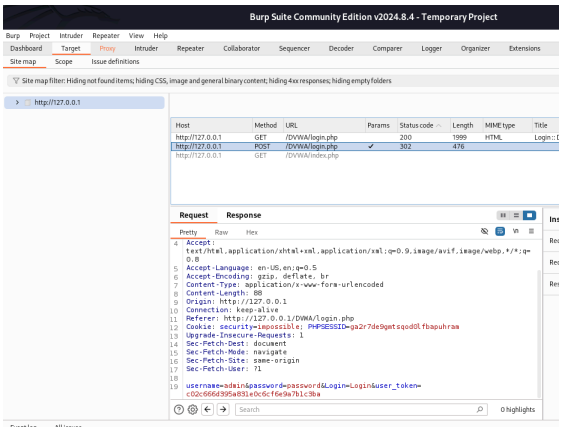


Рис. 3.10: Ввод случайных данных

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. 3.11).

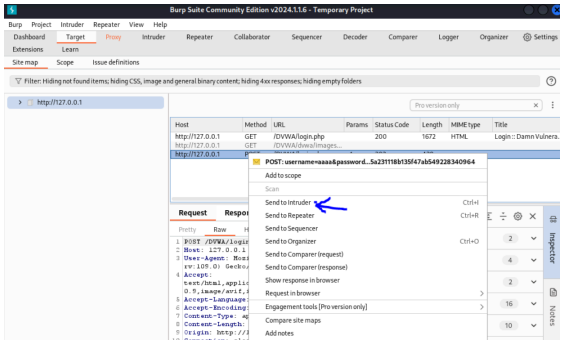


Рис. 3.11: POST-запрос с вводом пароля и логина

Попадаем на вкладку Intruder, видим значения по умолчанию у типа атаки и наш запрос (рис. 3.12).

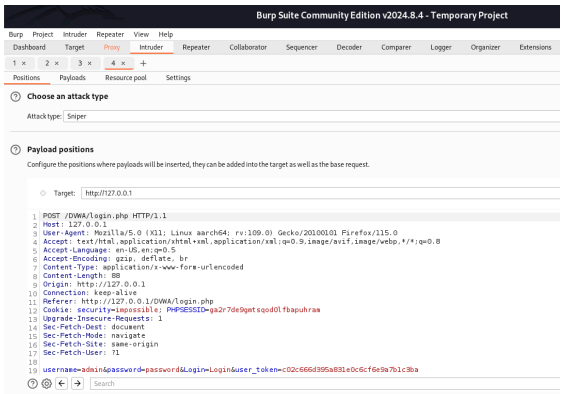


Рис. 3.12: Вкладка Intruder

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. 3.13).

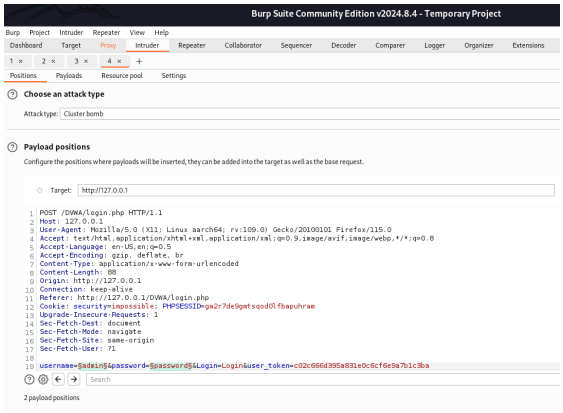


Рис. 3.13: Изменение типа атаки

Так как мы отметили два параметра для подбора, то нам нужно два списка со значениями для подбора. Заполняем первый список в `Payload setting` (рис. 3.14).

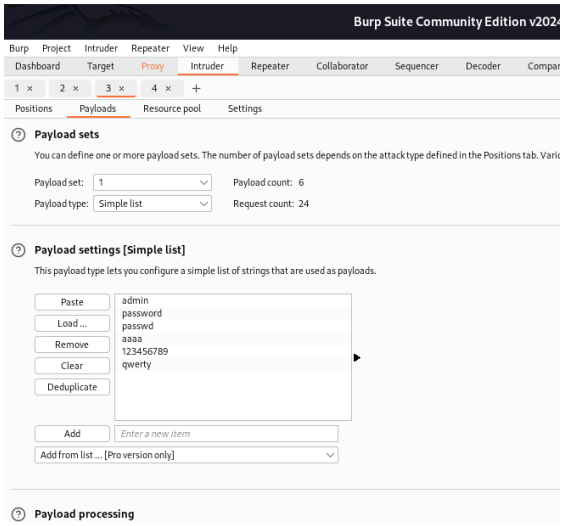


Рис. 3.14: Первый Simple list

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. 3.15).

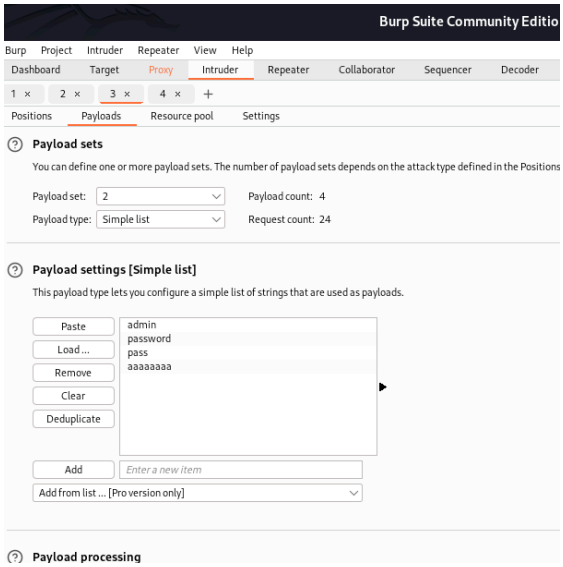


Рис. 3.15: Второй Simple list

Запускаем атаку и начинаем подбор (рис. 3.16).

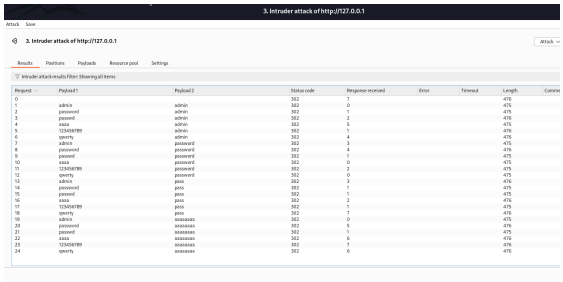


Рис. 3.16: Запуск атаки

При открытии результата каждого post-запроса можно увидеть по-

лученный 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. 3.17).

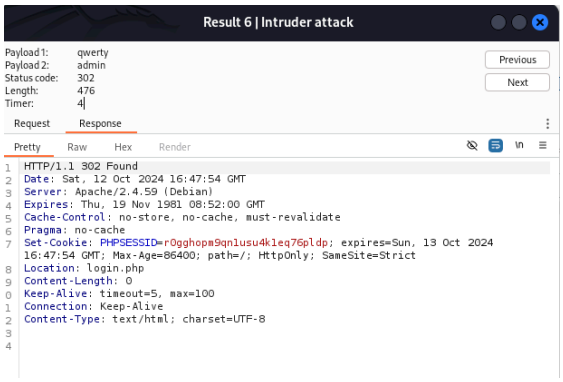


Рис. 3.17: Результат запроса

Проверим результат пары admin-password во вкладке Response, теперь нас перенаправляет на страницу index.php, значит пара должна быть верной (рис. 3.18).

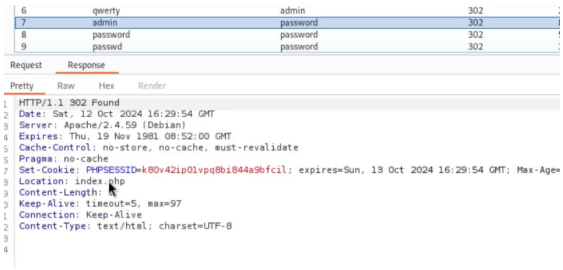


Рис. 3.18: Результат запроса

Дополнительная проверка с использованием Repeater, нажимаем на нужный нам запрос правой кнопкой мыши и жмем “Send to Repeater” (рис. 3.19).

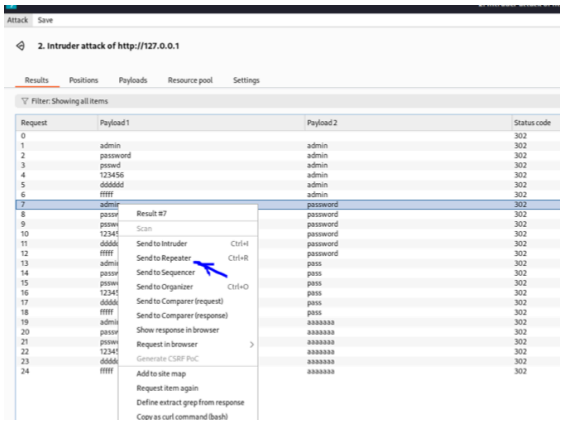


Рис. 3.19: Дополнительная проверка результата

Переходим во вкладку “Repeater” (рис. 3.20).

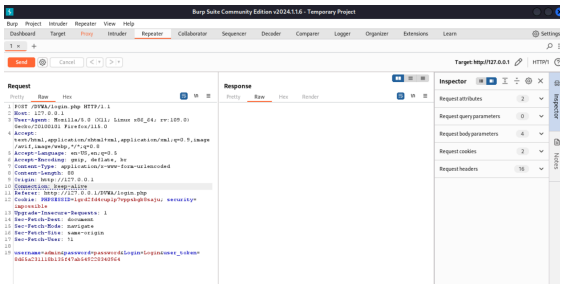


Рис. 3.20: Вкладка Repeater

Нажимаем “send”, получаем в Response в результат перенаправление

на index.php (рис. 3.21).

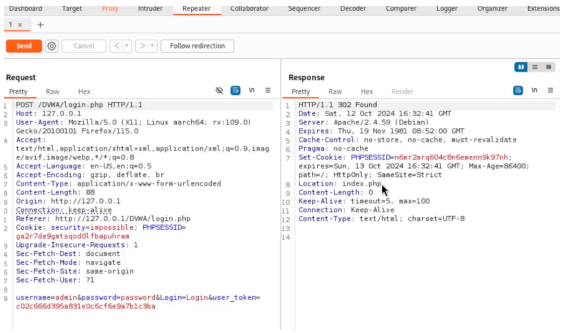


Рис. 3.21: Окно Response

После нажатия на `Follow redirection`, получим нескомпилированный html код в окне Response (рис. 3.22).

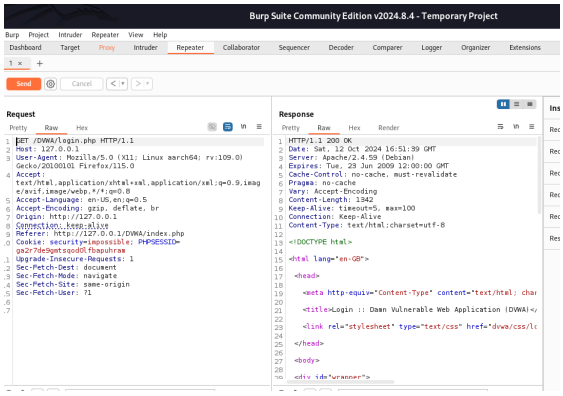
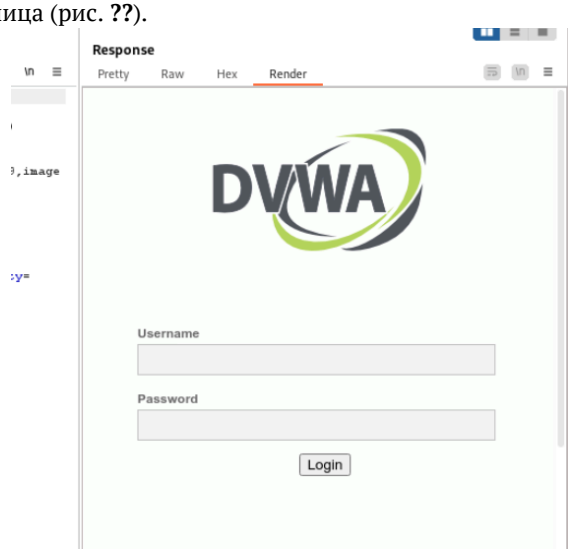


Рис. 3.22: Изменение в окне Response

Далее в подокне Render получим то, как выглядит полученная стра-

ница (рис. **??**).



Вывод

Научились использовть инструмент Burp Suite

4 Список литературы