Индивидуальный проект. Этап 5

Использования Burp Suite

Парфенова Е. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Парфенова Елизавета Евгеньвена
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- https://github.com/parfenovaee

Вводная часть

Актуальность

Важность понимания, как происходит перехват http-запросов, для поднятия уровня безопасности используемых систем, веб-сайтов и так далее

Цели и задачи

Цель: Обретение практических навыков использования Burp Suite

Задачи:

- Осуществить перехват запроса для веб-сервера DVWA
- Перехватить запрос аутентификации, попробовав изменить передаваемые данные

Теоретическое введение

Теоретичсекое введение(1)

Burp Suite – это мультитул для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многое другое. Сам инструмент представляет из себя проксирующий механизм, перехватывающий и обрабатывающий все поступающие от браузера запросы.

Теоретичсекое введение(2)

Основные модули:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender

Выполнение пятого этапа проекта

Запуск сервера и открытие Burp Suite

Рис. 1: Запуск сервера и открытие Burp Suite

Проект Burp Suite

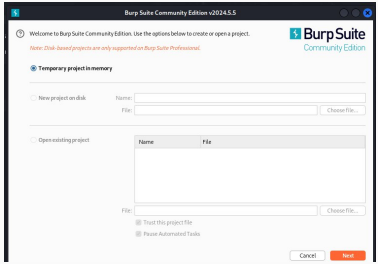

Рис. 2: Создание проекта в Burp Suite

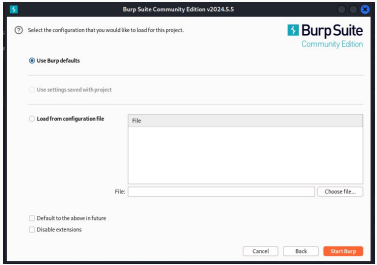

Рис. 3: Настройки проекта в Burp Suite

Запуск перехвата

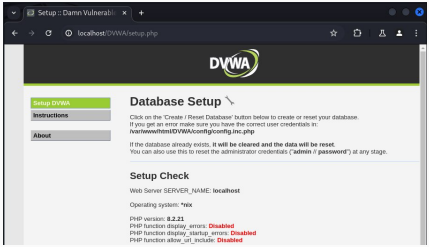

Рис. 4: Открытие DVWA через Burp-браузер

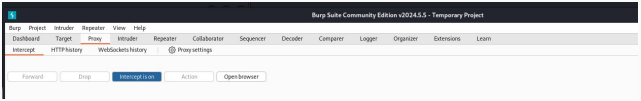

Рис. 5: Запуск перехвата

Перехват запроса

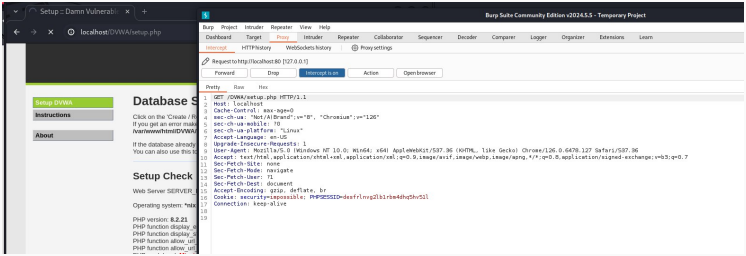

Рис. 6: Перехваченный запрос

Перехват запроса авторизации

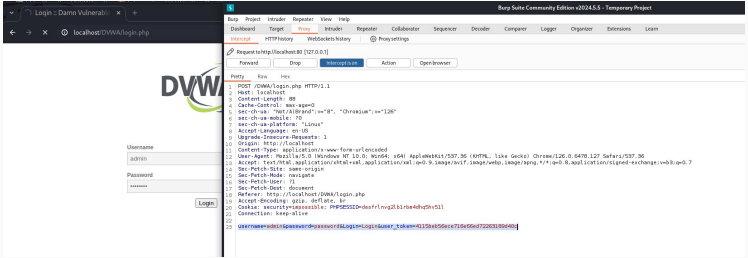

Рис. 7: Перехваченный запрос авторизации

История запросов

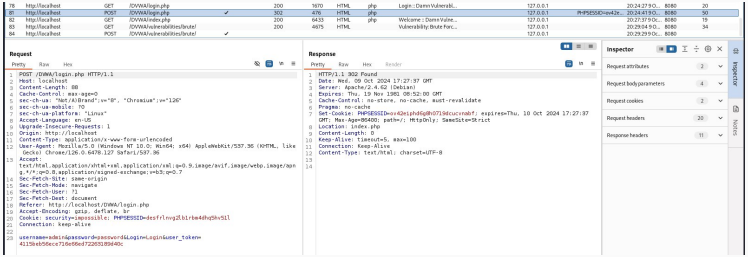

Рис. 8: Данные о запросе в истории запросов

Изменение данных перехваченного запроса

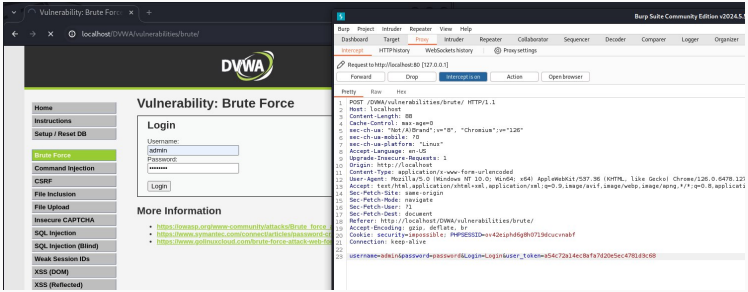

Рис. 9: Перехват логина и пароля с Brute Force

Изменение данных перехваченного запроса

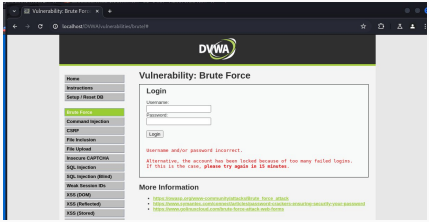

Рис. 10: Неудачная из-за измененных данных авторизация

Рис. 11: Запись об авторизации в истории запросов

Вывод

Выводы

Мы обрели практические навыки использования Burp Suite, осуществив перехват запроса для веб-сервера DVWA и перехватив запрос аутентификации с изменением его данных