Индивидуальный проект

Этап 5. Использование Burp suite

Артамонов Тимофей Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Использовать Burp suite для перехвата запросов и атак.

2 Теоретеческое введение

Burp Suite — это проприетарное программное обеспечение для оценки безопасности и тестирования на проникновение веб-приложений. Примечательные возможности этого пакета включают функции прокси-сканирования веб-страниц (Burp Proxy), регистрировать HTTP-запросы / ответы (Burp Logger и HTTP History), захватывать / перехватывать текущие HTTP-запросы (Burp Intercept), и агрегировать отчеты, указывающие на слабые места (Burp Scanner). Это программное обеспечение использует встроенную базу данных, содержащую заведомо небезопасные синтаксические шаблоны и ключевые слова для поиска в захваченных HTTP-запросах / ответах. [1]

3 Выполнение лабораторной работы

В настройках браузера зададим прокси. (рис. 3.1)

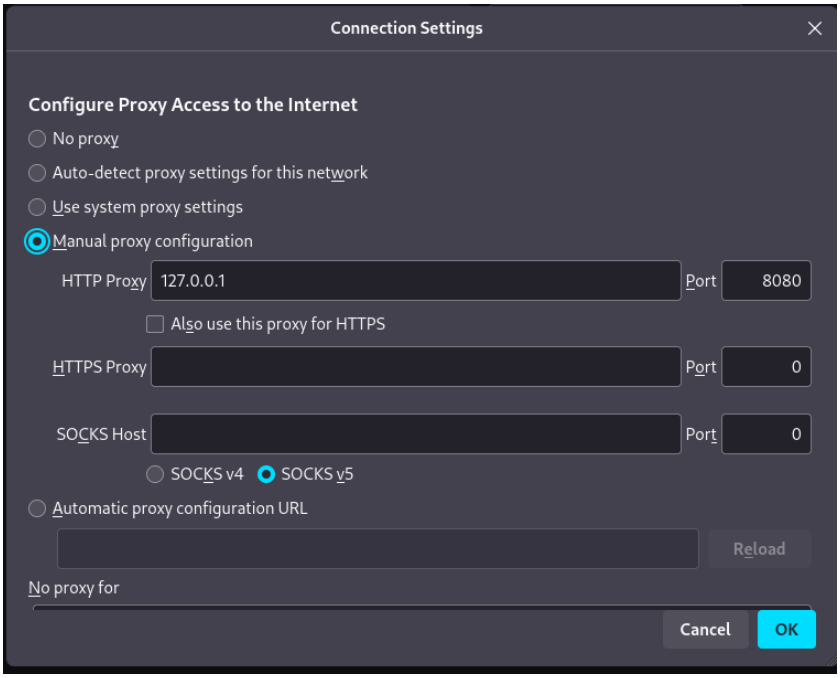

Рис. 3.1: HTTP Proxy

Запустим Burp suite и включим Intercept. (рис. 3.2)

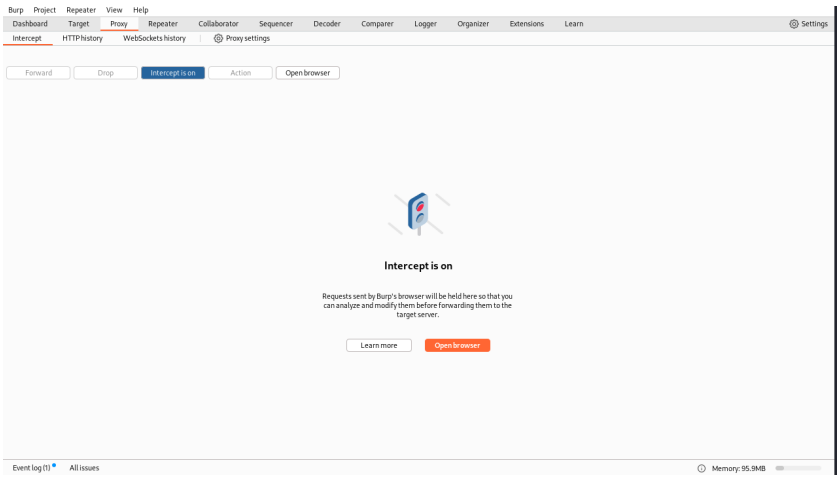

Рис. 3.2: Intercept is on - теперь запросы будут перехватываться

Пробуем открыть страницу в браузере. (рис. 3.3)

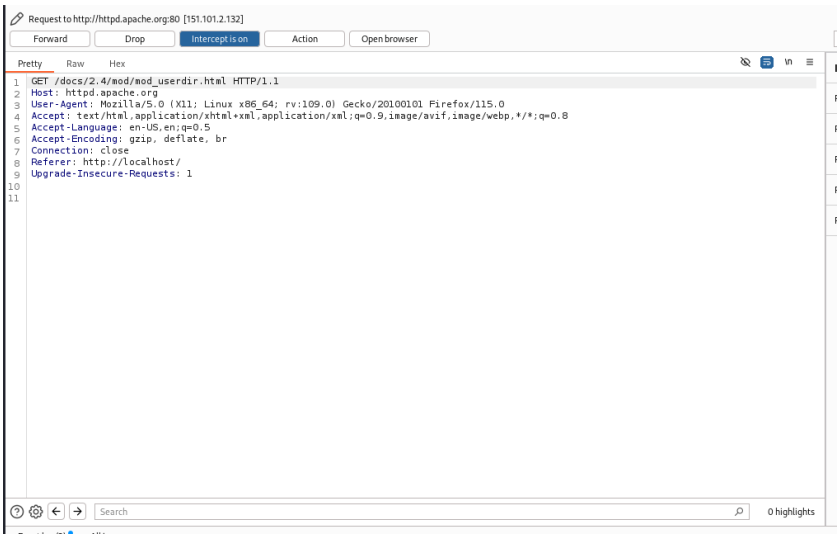

Рис. 3.3: Нас перекидывает в Burp suite и показывает данные, которые мы перехватили вместе с запросом

Нажимаем forward и заходим в раздел target. (рис. 3.4)

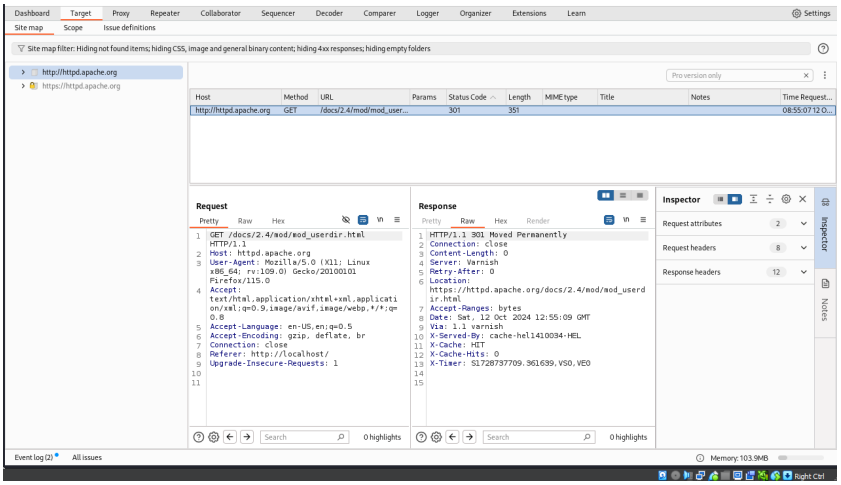

Рис. 3.4: Видим запрос который мы сюда перенаправили, справа внизу можно увидеть ответ на запрос

Зайдя обратно в раздел Proxy можем посмотреть историю http запросов. (рис. 3.5)

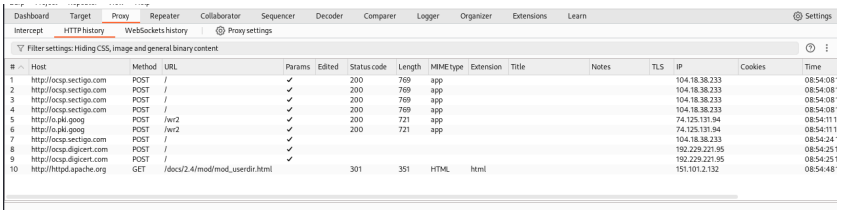

Рис. 3.5: Ссылки, методы запрсоов, код статуса и тд

4 Выводы

Использовали Burp suite для перехвата запросов, атаку провести не вышло тк отсутсвует необходимый раздел.

Список литературы

1. Burp Suite [Электронный ресурс]. Wikimedia Foundation, 2024. URL: https://en.wikipedia.org/wiki/Burp_Suite.