Индивидуальный проект

Этап 5. Использование Burp suite

Морозов Михаил Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

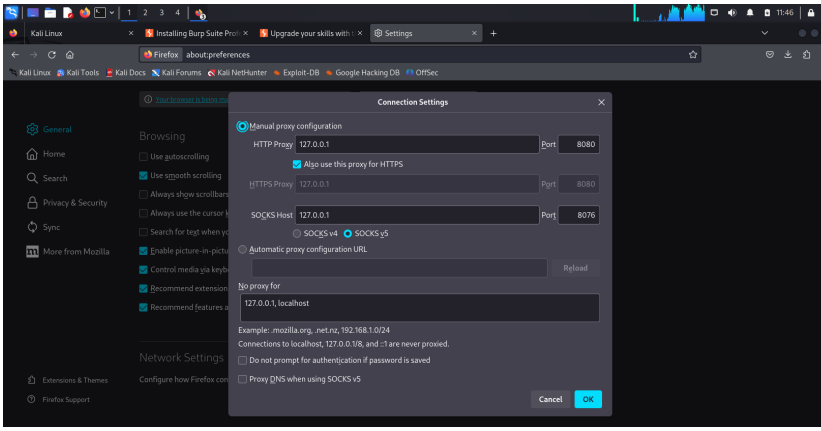
Использовать Burp suite для перехвата запросов и атак.

2 Теоретеческое введение

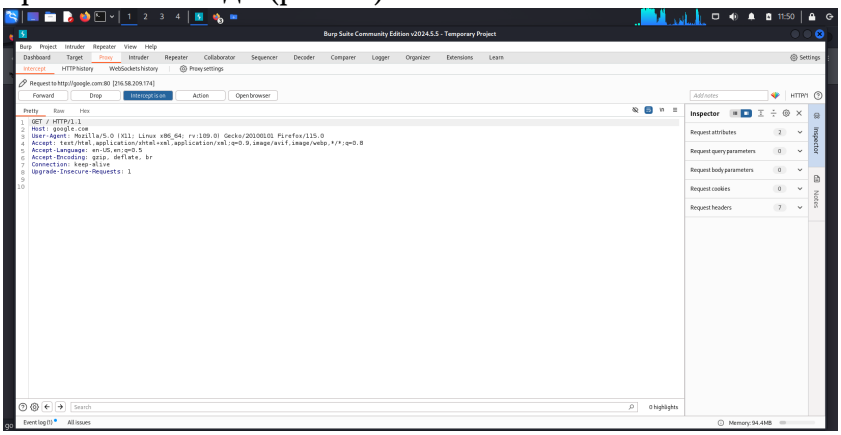
Burp Suite — это проприетарное программное обеспечение для оценки безопасности и тестирования на проникновение веб-приложений. Примечательные возможности этого пакета включают функции прокси-сканирования веб-страниц (Burp Proxy), регистрировать HTTP-запросы / ответы (Burp Logger и HTTP History), захватывать / 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

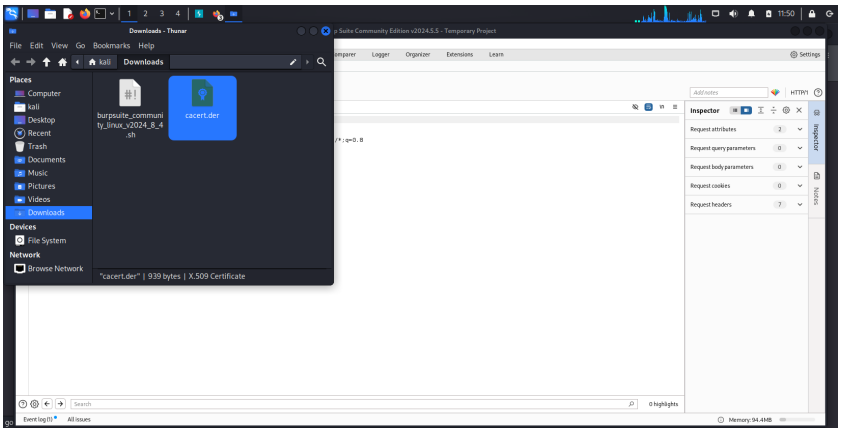
Результаты работы команд 1 (рис. **??**)



2 (рис. **??**)



3 (рис. **??**)



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.