# Отчёт о выполнении. Индивидуальный проект. Этап 5

**Использование Burp Suite**

Щербак Маргарита Романовна, НПИбд-02-21

2024

# Содержание

**Цель работы** **4**

**Теоретическое введение** **5**

**Выполнение лабораторной работы** **6**

**Вывод** **9**

**Библиография** **10**

# Список иллюстраций

1 Настройка прокси-сервера в Burp Suite . . . . . 6
2 Перехват HTTP-запросов . . . . . 7
3 Просмотр и анализ результатов . . . . . 8

# Цель работы

Научиться использовать Burp Suite.

# Теоретическое введение

Информационная безопасность представляет собой защиту данных и поддерживающей инфраструктуры от случайных или преднамеренных воздействий природного или искусственного характера, которые могут нанести ущерб владельцам или пользователям этой информации и инфраструктуры [1].

Rocky Linux — это дистрибутив Linux, созданный Rocky Enterprise Software Foundation. Он задуман как полностью двоично-совместимый релиз, основанный на исходном коде операционной системы Red Hat Enterprise Linux (RHEL). Цель проекта — обеспечить сообщество корпоративной операционной системой производственного уровня, поддерживаемой сообществом. Rocky Linux наряду с Red Hat Enterprise Linux и SUSE Linux Enterprise стал популярен среди корпоративных пользователей [2].

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

Burp Suite уже установлен в Kali Linux по умолчанию. Чтобы запустить его, ввела команду в терминале: burpsuite. Burp Suite — это мощный инструмент для тестирования безопасности веб-приложений. Burp Suite перехватывает трафик между браузером и целевым веб-сайтом. Чтобы это работало, нужно настроить браузер на использование прокси-сервера. Я открыла Burp Suite, перешла во вкладку Proxy > Options. Убедилась, что Burp Suite слушает на порту 8080 (локальный адрес 127.0.0.1) (рис.1). Настроила также браузер Firefox для использования прокси. Теперь весь трафик между браузером и веб-сайтами будет перехватываться Burp Suite.

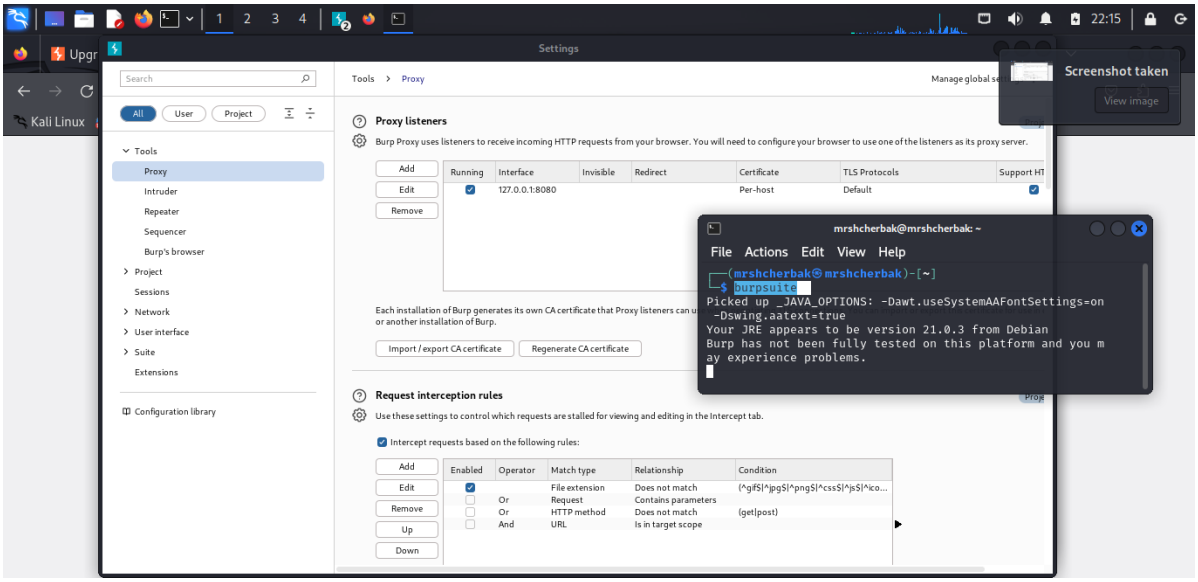


Рис. 1: Настройка прокси-сервера в Burp Suite

После настройки прокси-сервера, открыла браузер и перешла на сайт http://example.com. Burp Suite начал перехватывать запросы. Чтобы продемонстрировать это, выполнила

следующие шаги: в Burp Suite перешла во вкладку Proxy > Intercept и убедилась, что кнопка Intercept is on активна. Когда запрос перехвачен, в окне Burp Suite отобразится HTTP-запрос (рис.2).

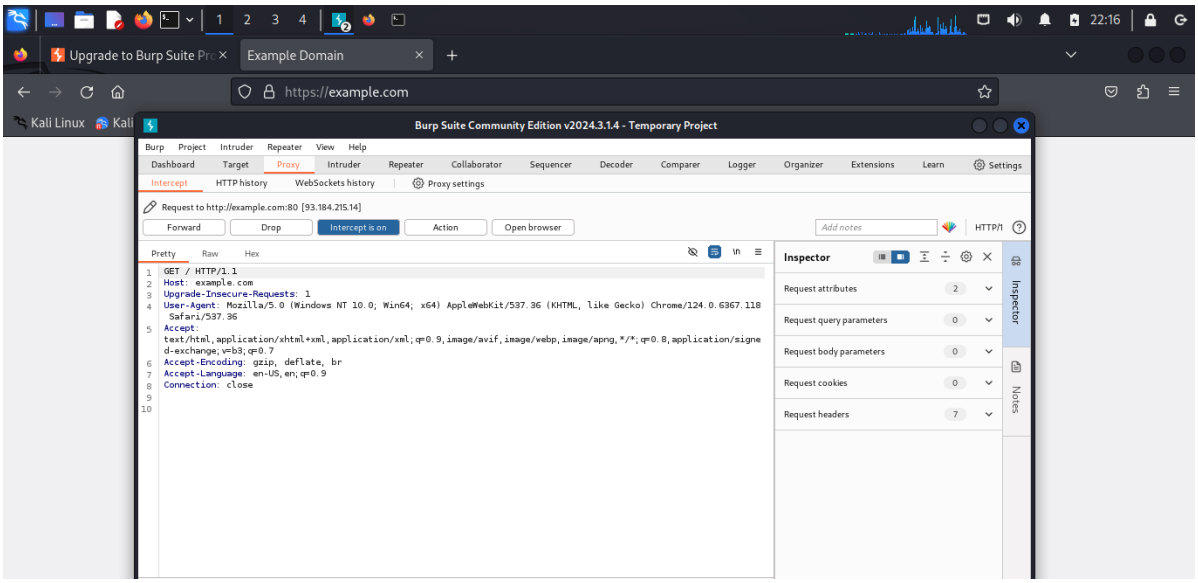


Рис. 2: Перехват HTTP-запросов

- GET / HTTP/1.1: запрос типа GET, который запрашивает корневую страницу веб-сайта (/) по протоколу HTTP/1.1.
- Host: example.com: целевой хост веб-сайта — example.com.
- User-Agent: Информация о клиенте.
- Accept-Language: Язык, предпочтительный для отображения контента.

Злоумышленники могут изменять перехваченные HTTP-запросы. Например, можно изменить параметры запроса или содержимое формы перед отправкой на сервер.

Использование других инструментов Burp Suite:

- Intruder: используется для проведения атак с перебором параметров (например, перебор паролей или идентификаторов сессий).
- Scanner (в профессиональной версии): автоматически сканирует веб-приложение на уязвимости, такие как SQL-инъекции или XSS.

После запуска атаки или тестирования запросов, можно перейти к анализу результатов:

- В HTTP History во вкладке Proxy можно просмотреть полный список запросов и ответов, которые прошли через Burp Suite (рис.3).
- Вкладка Repeater позволяет повторять запросы с изменёнными параметрами для тестирования реакции сервера.
- Intruder покажет результаты перебора, включая успешные или ошибочные попытки аутентификации.

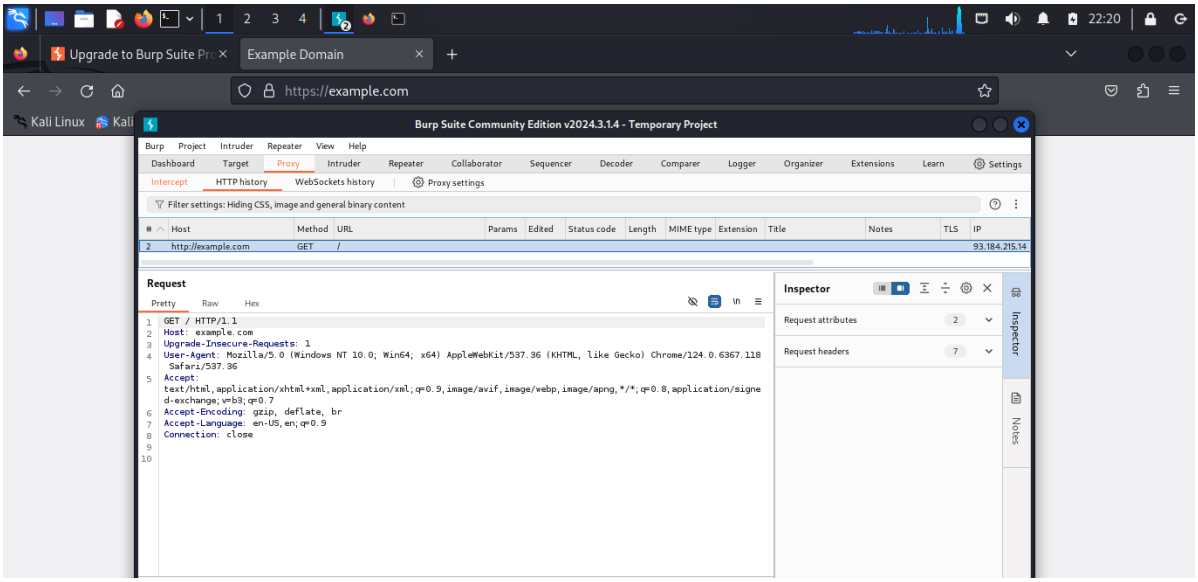


Рис. 3: Просмотр и анализ результатов

# Вывод

Таким образом, в ходе 5 этапа индивидуального проекта я научилась использовать Burp Suite. Инструменты Burp Suite позволяют исследовать и тестировать веб-приложения на уязвимости. Эти демонстрации помогают понять, как злоумышленники могут модифицировать запросы или перебирать параметры, чтобы скомпрометировать веб-приложение.

# Библиография

1. Методические материалы курса.
2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: Rocky Linux Documentation (Дата обращения: 01.10.2024).