Индивидуальный проект 5

Генералов Даниил, 1032212280

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

В этом этапе индивидуального проекта требуется использовать набор инструментов Burp Suite, чтобы найти и использовать какие-то уязвимости в DVWA.

2 Выполнение лабораторной работы

Burp Suite – набор инструментов для кибербезопасности, которые работают вместе. Изучение цели начинается с Burp Proxy: он используется, чтобы получить трафик для анализа. Используя встроенный браузер, можно собрать информацию о тех веб-запросах, которые выполняет приложение (рис. 2.1).

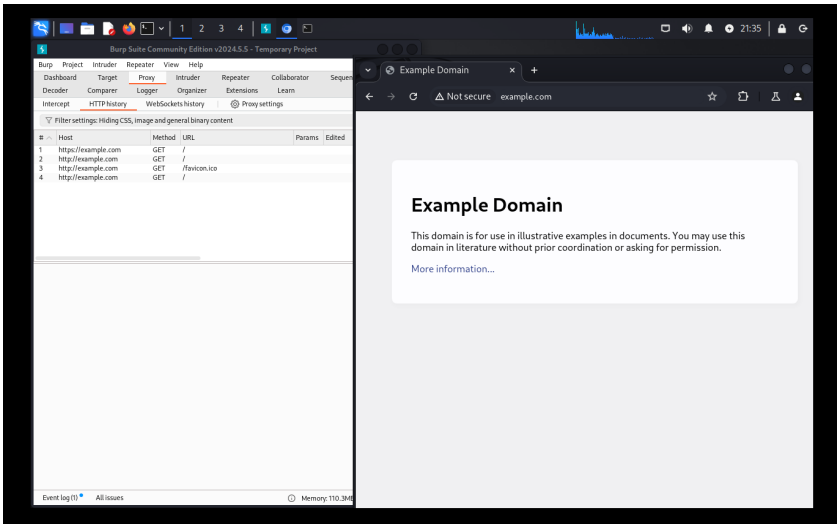

Рис. 2.1: Burp Proxy

Это можно использовать, чтобы отследить, какие запросы происходят. Например, можно увидеть содержимое этого POST-запроса, который используется для загрузки файлов на сервер (рис. 2.2).

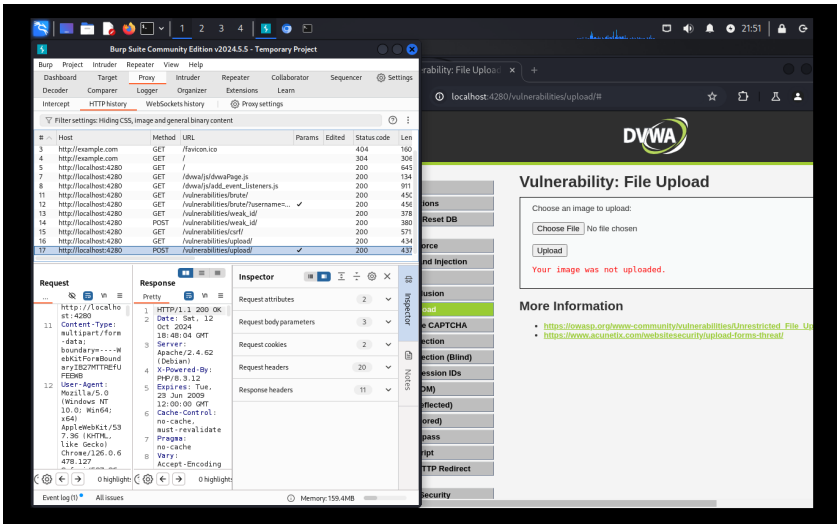

Рис. 2.2: POST-запрос

Теперь можно отправить этот запрос в вкладку Repeater, где можно отредактировать и выполнить этот запрос еще раз. Мы видим, что в этом запросе передается параметр MAX_FILE_SIZE: если его отредактировать, то наш файл будет успешно загружен (рис. 2.3).

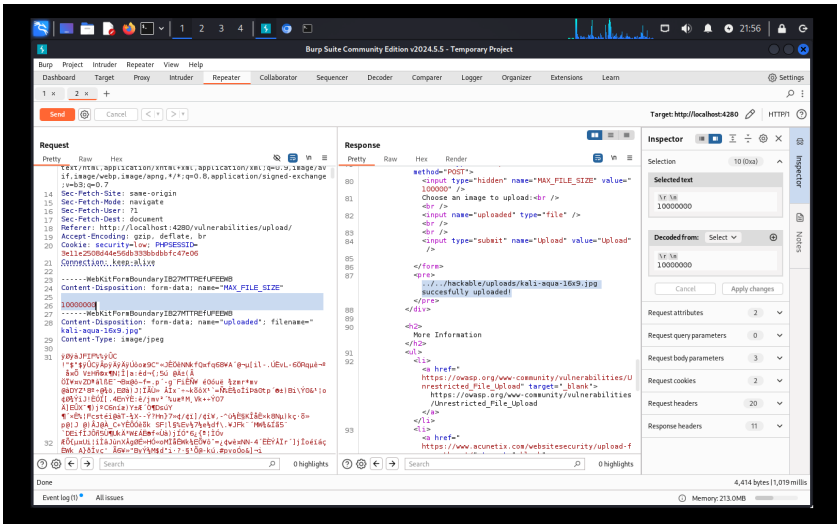

Рис. 2.3: MAX_FILE_SIZE

С помощью этого инструмента можно легко эксплуатировать любые уязвимости, связанные с редактированием данных запроса. Например, можно использовать его для эксплуатирования reflected XSS: сначала мы

записываем запрос, который используется на странице (рис. 2.4).

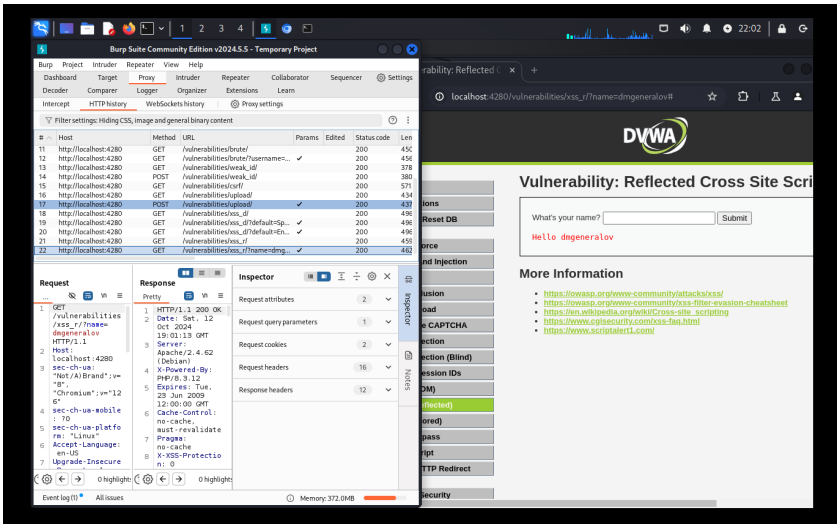

Рис. 2.4: XSS

После этого мы открываем его в вкладке Repeater, и меняем GET-параметр: мы видим, что он появляется в явном виде на странице (рис. 2.5), что значит, что если перейти на ссылку специального формата, то злоумышленник может добавить свой код на страницу.

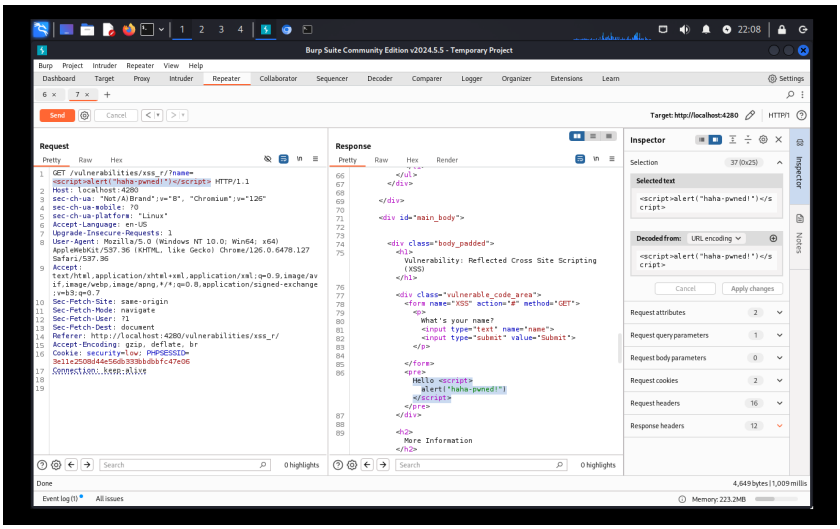

Рис. 2.5: XSS

Одна из очень полезных фич Burp Proxy – возможность интерактивного редактирования запросов. Если включить режим Intercept, то после того,

как клиент отправил запрос, но до того, как он был передан серверу, можно отредактировать этот запрос. Например, клиент сделал ping на адрес 1.2.3.4 (рис. 2.6), а получил ответ с ping на 1.1.1.1 (рис. 2.7).

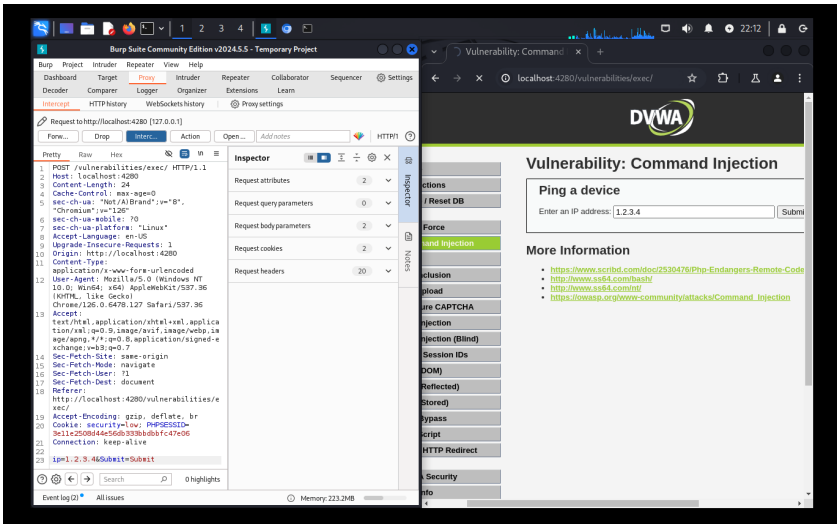

Рис. 2.6: Intercept

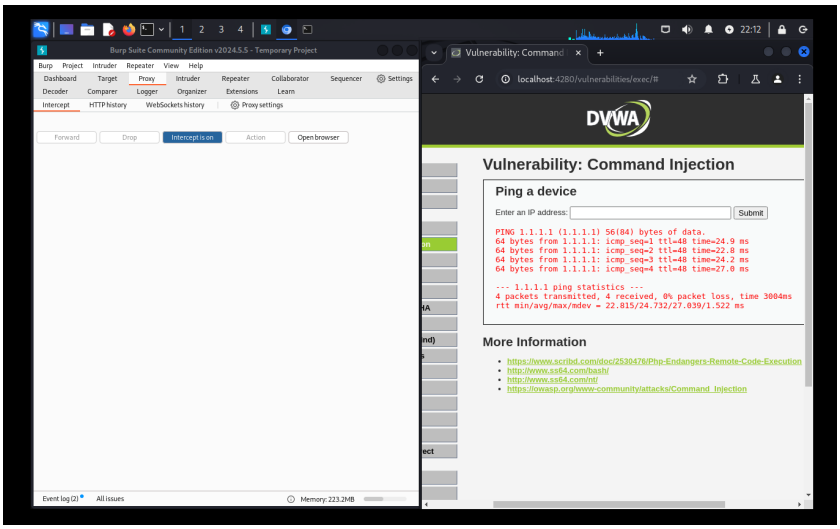

Рис. 2.7: Intercept

3 Выводы

Мы успешно использовали некоторые из утилит в Burp Suite для анализа и использования уязвимостей.