Индивидуальный проект - этап 5

Использование BurpSuite

Овезов Мерген

Содержание

# 1 Цель работы

Освоить работу с инструментом Burp Suite для перехвата, анализа и модификации HTTP‑запросов/ответов веб‑приложения DVWA, а также для поиска уязвимостей.

# 2 Выполнение работы

Запустить Burp Suite.Настроить прокси в Burp Suite на `127.0.0.1:8080`. В браузере включить ручной прокси `127.0.0.1:8080` и установить сертификат Burp в «Доверенные центры сертификации». Включить перехват.В браузере открыть DVWA, выполнить вход и зафиксировать перехваченные запросы. Вкладка “HTTP history” — выбрать запрос.Отправить запрос в Repeater.

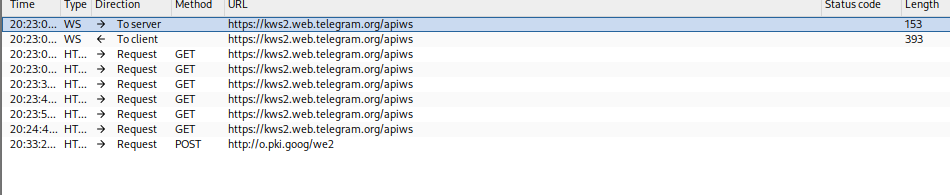


Figure 1: окно Intercept с перехваченным запросом

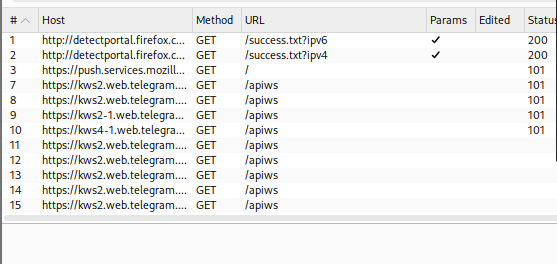


Figure 2: вкладка HTTP history с выбранным запросом

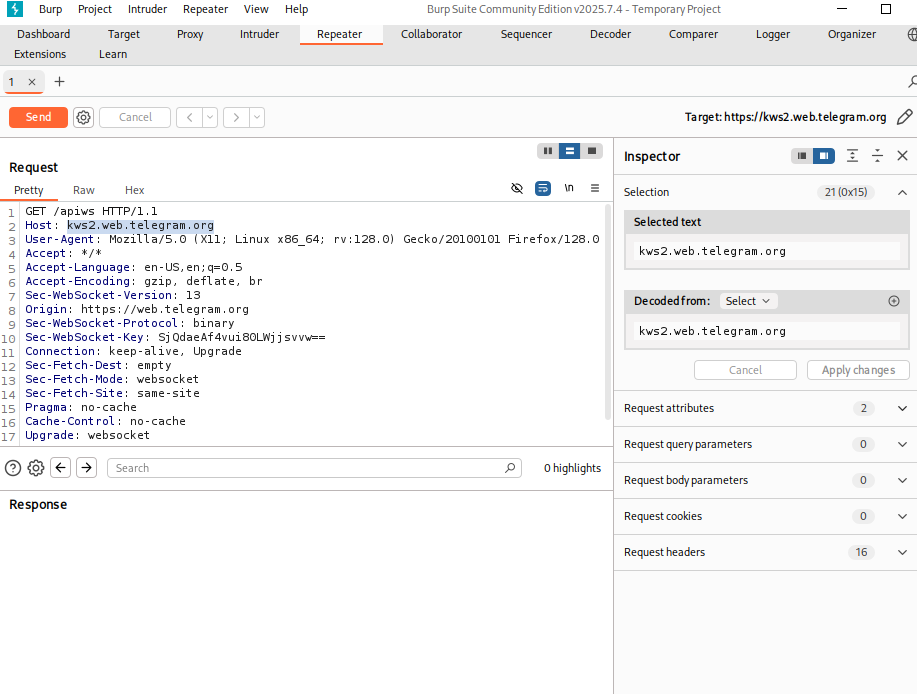


Figure 3: вкладка Repeater с изменённым запросом и ответом сервера

# 3 Вывод

Burp Suite позволяет детально анализировать взаимодействие клиента и сервера. - Инструмент полезен для поиска уязвимостей, тестирования валидации данных и проведения атак типа SQL Injection, XSS и др. - Для защиты необходимо фильтровать и проверять все входящие данные на стороне сервера.