Индивидуальный проект.

Этап 5. Использование Burp Suite

Стариков Данила НПИбд-02-22

Содержание

1 Цель работы

Познакомиться с экосистемой Burp Suite для поиска уязвимостей веб-приложений и демонстрации возможностей злоумышленника.

2 Выполнение работы

2.1 Знакомство с интерфейсом приложения

Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения. Открыли приложение и перешли во вкладку `Proxy` -> `Intercept` (Рис. 2.1).

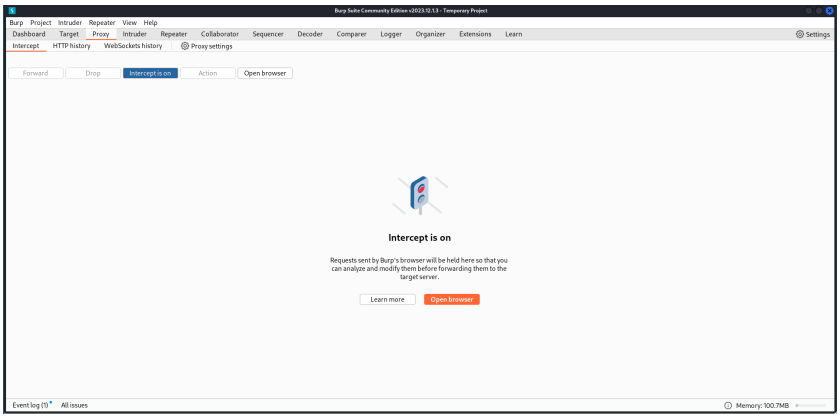

Рис. 2.1: Окно приложения Burp Suite.

Кнопка `Intercept` позволяет перехватывать все HTTP запросы, которые будут поступать. Для демонстрации перешли на сайт компании <portswigger.net>. Загрузка не началась, так как запрос был перехвачен приложением, посмотрели как он выглядит (Рис. 2.2):

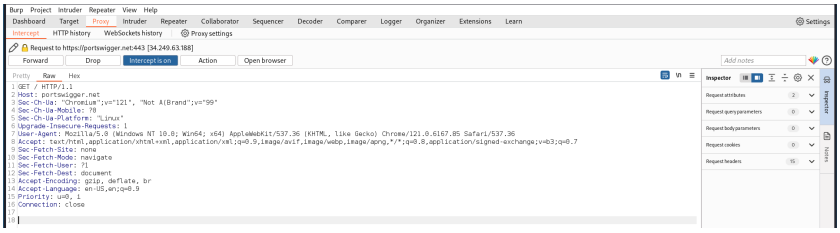

Рис. 2.2: Представление перехваченного HTTP запроса.

Нажатие кнопки `Forward` отправляет перехваченный запрос, и страница прогружается (Рис. 2.3). Далее отключили перехват `Intercept off`.‘

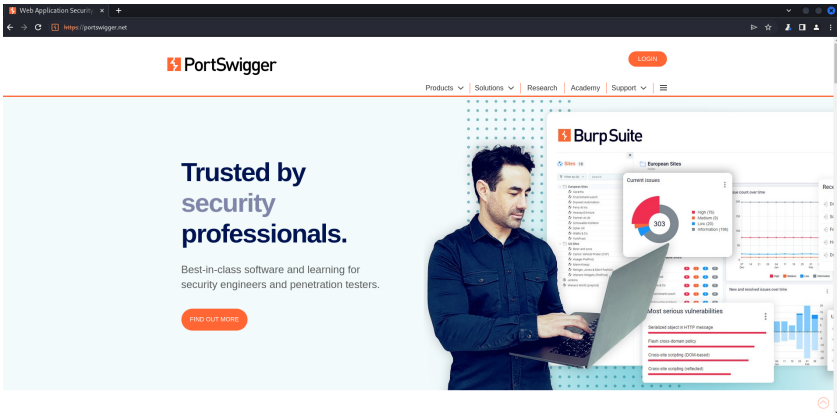

Рис. 2.3: Сайт открыт через приложение.

Во вкладке `HTTP history` можно посмотреть все проходящие запросы, даже если их перехват был выключен (Рис. 2.4):

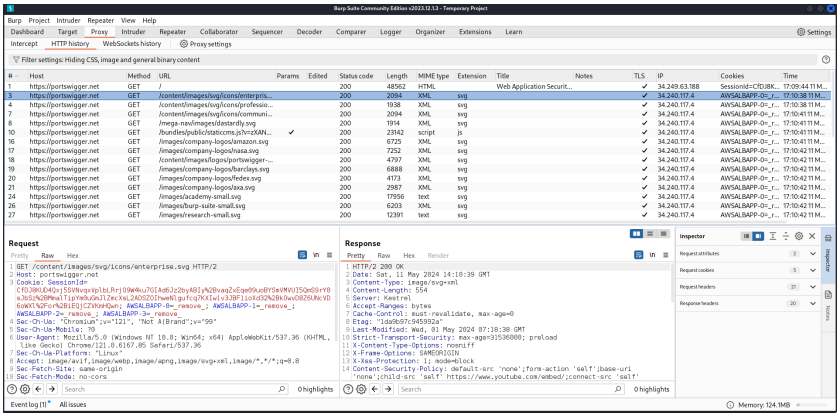

Рис. 2.4: История всех HTTP запросов.

2.2 Перехват и модификация HTTP запроса

Разработчики Burp Suite сделали серию гайдов для знакомства с приложением, прошли один из них: `Modifying requests` (Изменяем запросы) [1]. Перешли на тестовый сайт онлайн-магазин (перед этим необходимо зарегистрироваться) https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls (Рис. 2.5):

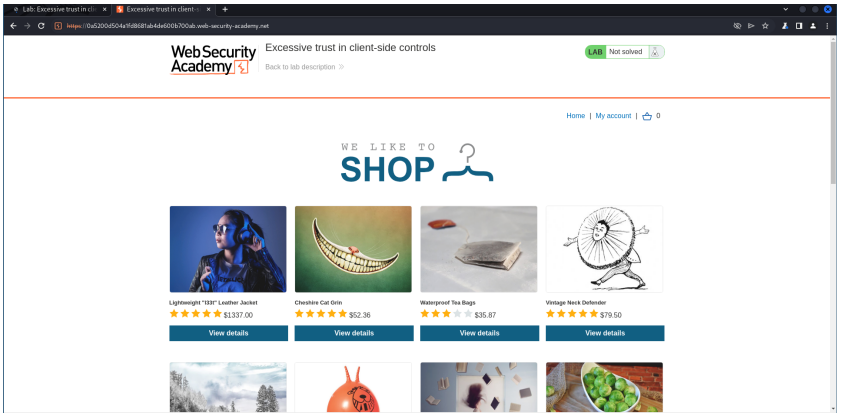

Рис. 2.5: Тестовое приложение.

Зашли в личный кабинет (My account) под пользователем `wiener` (пароль: `peter`) и увидели, что на счету 100 долларов (Рис. 2.6).

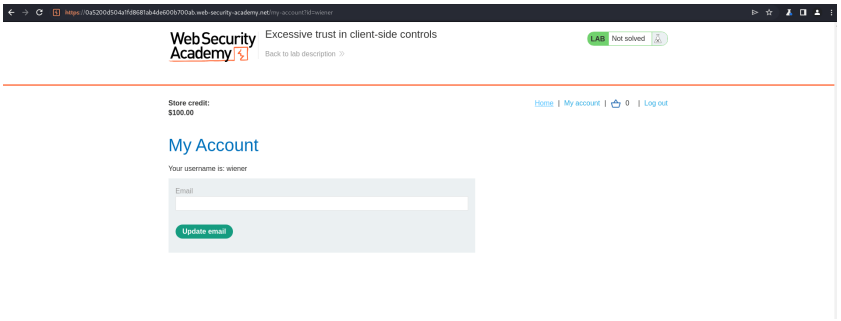

Рис. 2.6: Личный кабинет с 100 долларами на счету.

Вернулись на главную страницу (Home). Перед тем, как что-либо купить, открыли `brupsuite` и включили перехват пакетов `Intercept on`. Затем добавили в корзину товар и открыли перехваченный HTTP запрос (Рис. 2.7):

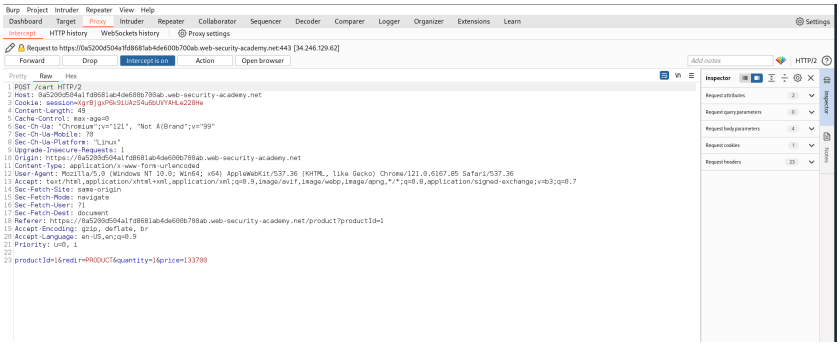

Рис. 2.7: Перехват HTTP запроса при добавлении товара в корзину.

Нашли поле `price`, изменили значение на `1`, отправили его (`Forward`) и отключили перехват (`Intercept off`) (Рис. 2.8):

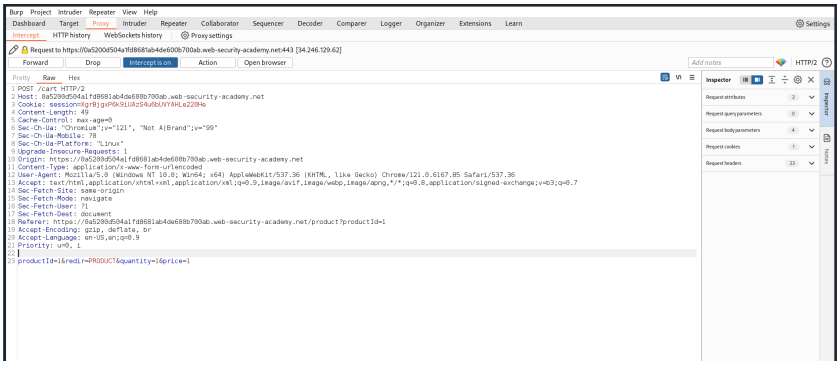

Рис. 2.8: Запрос после изменения цены.

Перешли в корзину и увидели, что стоимость товара поменялась на указанную в запросе (Рис. 2.9).

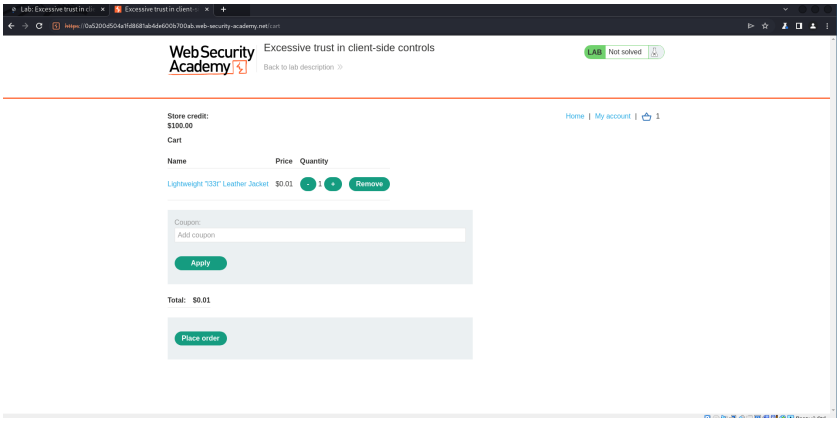

Рис. 2.9: Корзина с измененой ценой товара.

Нажали кнопку `Place Order` и завершили этот тестовый пример. Счет на аккаунте изменился всего на один цент (Рис. 2.10).

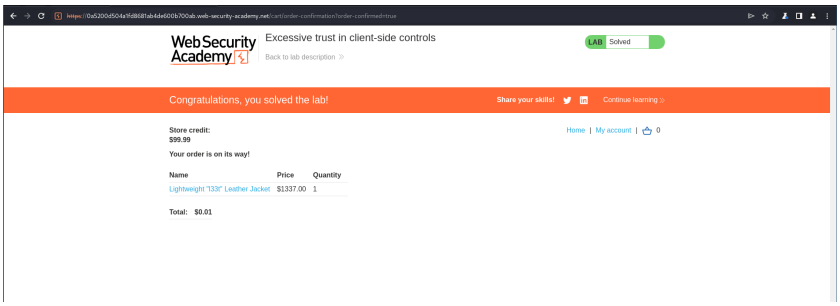

Рис. 2.10: Итоговый счет на аккаунте после оплаты заказа.

3 Выводы

В результате работы познакомились с экосистемой `Burp Suite` и продемонтсрировали ее работу при перехвате и модификации HTTP запроса.

Список литературы

1. PortSwigger Ltd. Modifying HTTP requests with Burp Proxy. https://portswigger.net/burp/documentation/desktop/getting-started/modifying-http-requests, 2024.

‘‘