Индивидуальный проект. Этап 5

Использования Burp Suite

Парфенова Елизавета Евгеньевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Обретение практических навыков использования Burp Suite

2 Задание

- Осуществить перехват запроса для веб-сервера DVWA
- Перехватить запрос аутентификации, попробовав изменить передаваемые данные

3 Теоретическое введение

Burp Suite – это мультитул для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многое другое. Также существует магазин дополнений BApp store, содержащий дополнительные расширения, увеличивающие функционал приложения. Burp Suite — это интегрированная платформа, предназначенная для проведения аудита веб-приложения, как в ручном, так и в автоматических режимах. Содержит интуитивно понятный интерфейс со специально спроектированными табами, позволяющими улучшить и ускорить процесс атаки. Сам инструмент представляет из себя проксирующий механизм, перехватывающий и обрабатывающий все поступающие от браузера запросы. Имеется возможность установки сертификата burp для анализа https соединений.

Основной функционал основан на следующих модулях:

- Proxy — перехватывающий прокси-сервер, работающий по протоколу HTTP(S) в режиме man-in-the-middle. Находясь между браузером и веб-приложением он позволит вам перехватывать, изучать и изменять трафик идущий в обоих направлениях.
- Spider — паук или краулер, позволяющий вам в автоматическом режиме собирать информацию о об архитектуре веб-приложения.
- Scanner — автоматический сканер уязвимостей (OWASP TOP 10 и т.д.) Доступен в Professional версии, в бесплатной версии только описание возможностей.

- Intruder — утилита, позволяющая в автоматическом режиме производить атаки различного вида, такие как подбор пароля, перебор идентификаторов, фаззинг и так далее.
- Repeater — утилита для модифицирования и повторной отправки отдельных HTTP-запросов и анализа ответов приложения.
- Sequencer — утилита для анализа генерации случайных данных приложения, выявления алгоритма генерации, предиктивности данных.
- Decoder — утилита для ручного или автоматического преобразования данных веб-приложения.
- Comparer — утилита для выявления различий в данных.
- Extender — расширения в BurpSuite. Можно добавлять как готовые из BApp store, так и собственной разработки [1].

4 Выполнение лабораторной работы

Для дальнейшей работы с DVWA запустим сервер и базу данных, а также запустим сам Burp Suite, который изначально был установлен в моей ОС. (рис. 4.1).

Рис. 4.1: Запуск сервера и открытие Burp Suite

Далее создадим временный проект в Burp Suite (рис. 4.2) с дефолтными Burp настройками (рис. 4.3).

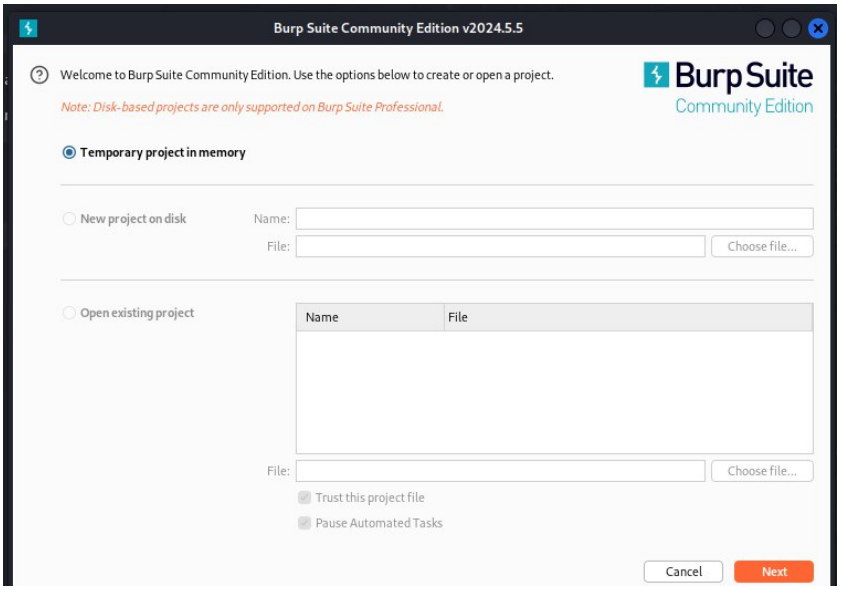

Рис. 4.2: Создание проекта в Burp Suite

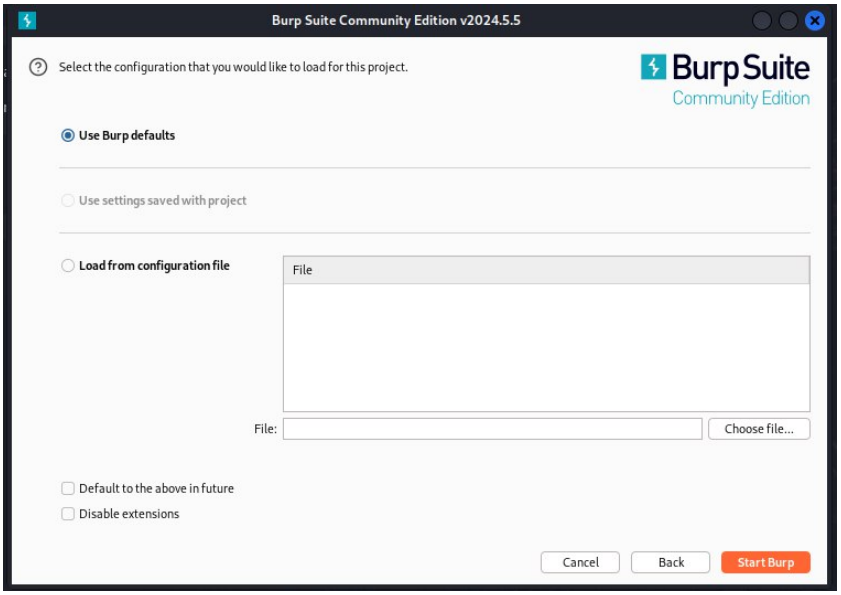

Рис. 4.3: Настройки проекта в Burp Suite

Зайдем в DVWA через привычный запрос “http://localhost/DVWA/setup.php”, но сделаем это именно через Burp-браузер, нажав на кнопку “Open browser” во вкладке Proxy самого приложения (рис. 4.4)

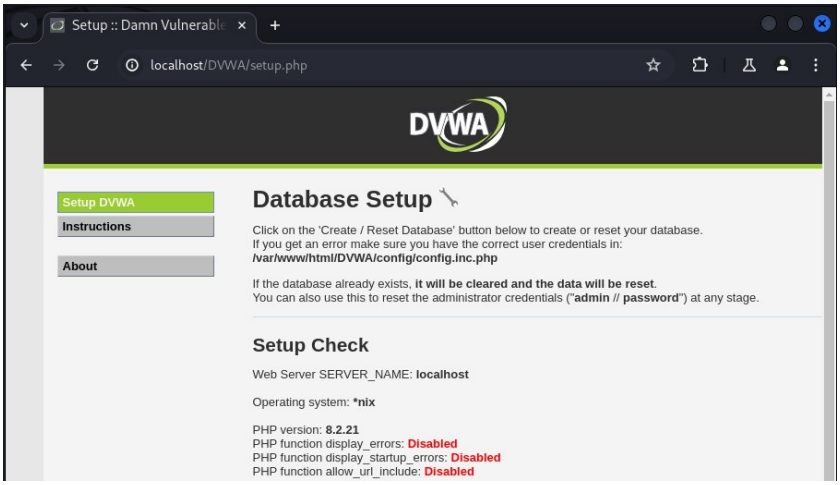

Рис. 4.4: Открытие DVWA через Burp-браузер

Затем в той же вкладке тапнем на кнопку “Intercepr is off”, переведя ее в активное состояние “Intercepr is on” (рис. 4.5), и перезагрузим открытый веб-сайт (сайт не перезагрузится, пока мы не пустим запрос дальше). Видим, что мы перехватили http-запрос и теперь можем посмотреть всю информацию о нем (рис. 4.6). Здесь можно увидеть информацию о методе запроса, адресе запроса, имени хоста, уровне бзопасности сайта, данные cookie.

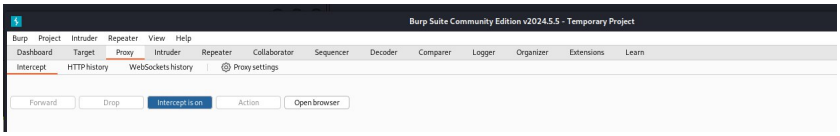

Рис. 4.5: Запуск перехвата

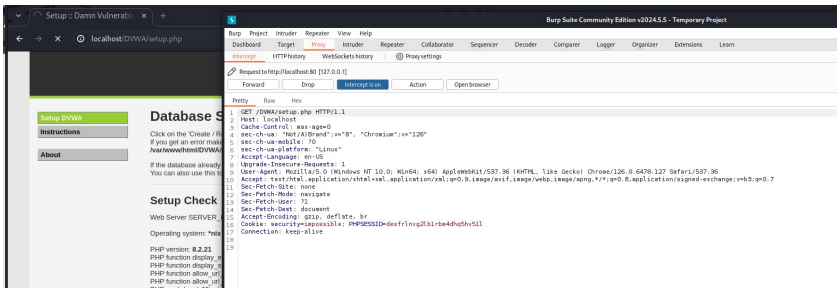

Рис. 4.6: Перехваченный запрос

Попробуем авторизоваться, перехватив этот запрос и данные для авторизации соответственно. Видим, что помимо уже знакомых нам данных (метод запроса на

этот раз POST), мы перехватили также пароль и логин (рис. 4.7). Во вкладке HTTP History можно посмотреть полную историю запросов, найдем там наш запрос и увидим еще более подробную информацию + ответ от сервера на наш запрос в правой стороне и данные о нем. (рис. 4.8)

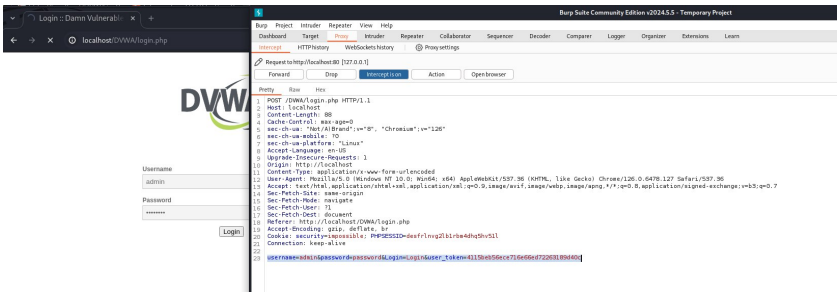

Рис. 4.7: Перехваченный запрос авторизации

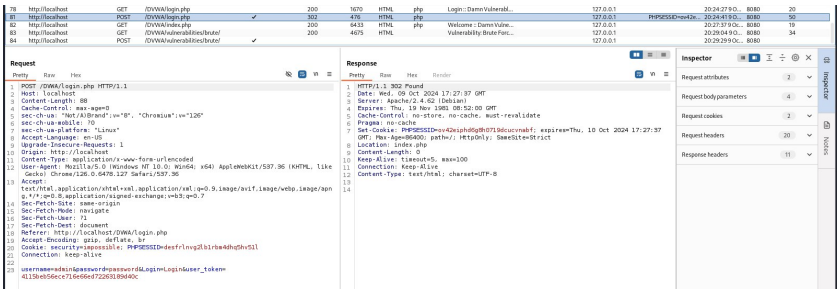

Рис. 4.8: Данные о запросе в истории запросов

Попробуем перехватить данные об авторизации и изменить их. Для этого зайдем в уже знакомую нам вкладку Brute Force и попробуем ввести данные авторизации там, попутно перехватывая этот запрос через Burp Suite. Видим, что в перехваченном запросе все также есть логин и пароль (рис. 4.9). Попробуем заменить пароль на pasw в перехваченном запросе и отправим его дальше, на сервер. Увидим ответ о неудачной авторизации на страничке DVWA. Это значит, что мы успешно изменили перехваченные данные и нарушили процесс авторизации (рис. 4.10). Так выполненный запрос измененными данными выглядит в истории запросов (рис. 4.11).

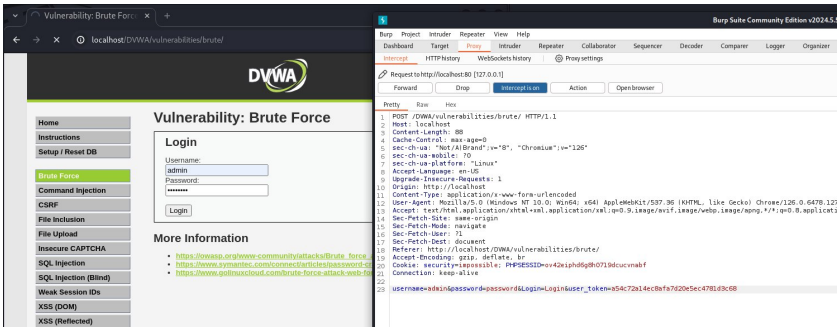

Рис. 4.9: Перехват логина и пароля с Brute Force

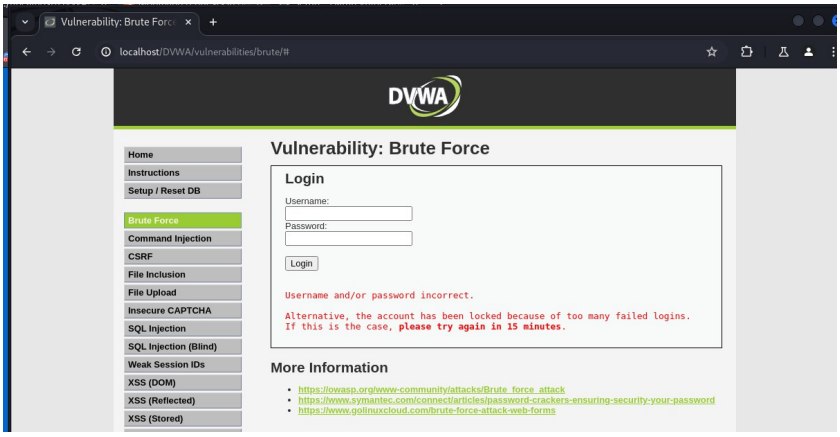

Рис. 4.10: Неудачная из-за измененных данных авторизация

Рис. 4.11: Запись об авторизации в истории запросов

5 Выводы

Мы обрели практические навыки использования Burp Suite, осуществив перехват запроса для веб-сервера DVWA и перехватив запрос аутентификации с изменением его данных

Список литературы

1. Burp Suite: швейцарский армейский нож для тестирования веб-приложений [Электронный ресурс]. © 2006–2024, Habr, 2017. URL: https://habr.com/ru/articles/328382/.