Индивидуальный проект. Этап №3

Использование Hydra для брутфорса

Кадров Виктор Максимович

Содержание

Список иллюстраций

1 Цель работы

Научиться пользоваться утилитой Hydra.

2 Задание

1. Просмотр уязвимой формы
2. Поиск словаря с паролями
3. Использование Hydra
4. Проверка результатов

3 Выполнение лабораторной работы

3.1 Просмотр уязвимой формы

Изучаем уязвимую веб-форму, чтобы узнать параметры запроса и передать в программу (рис. 3.1). Здесь мы узнаем, что выполняется GET-запрос с двумя параметрами. Также через консоль разработчика узнаем параметры cookie (ID сессии и уровень защищенности DVWA)

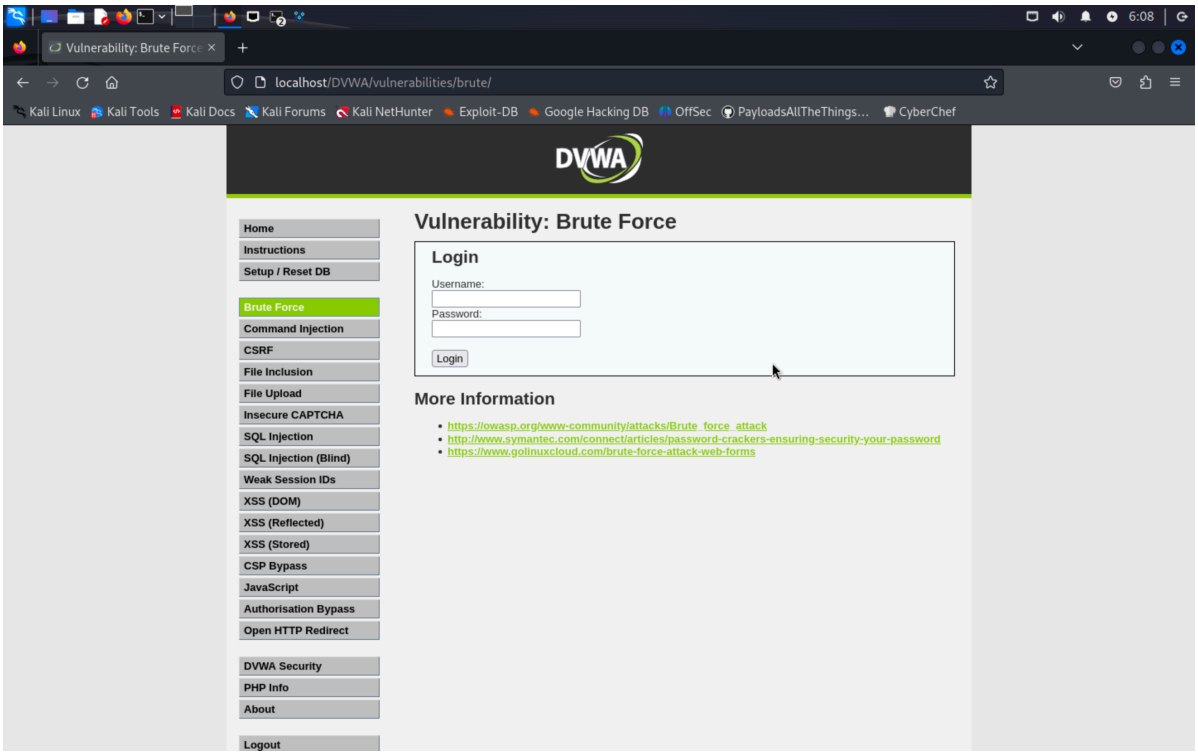

Рис. 3.1: Уязвимая форма

3.2 Поиск словаря с паролями

Выбираем один из стандартных словарей и распаковываем его (рис. 3.2).

Рис. 3.2: Словарь

3.3 Использование Hydra

Запускаем программу с нужными параметрами и после некоторого времени видим одну подходящую пару логин-пароль (рис. 3.3).

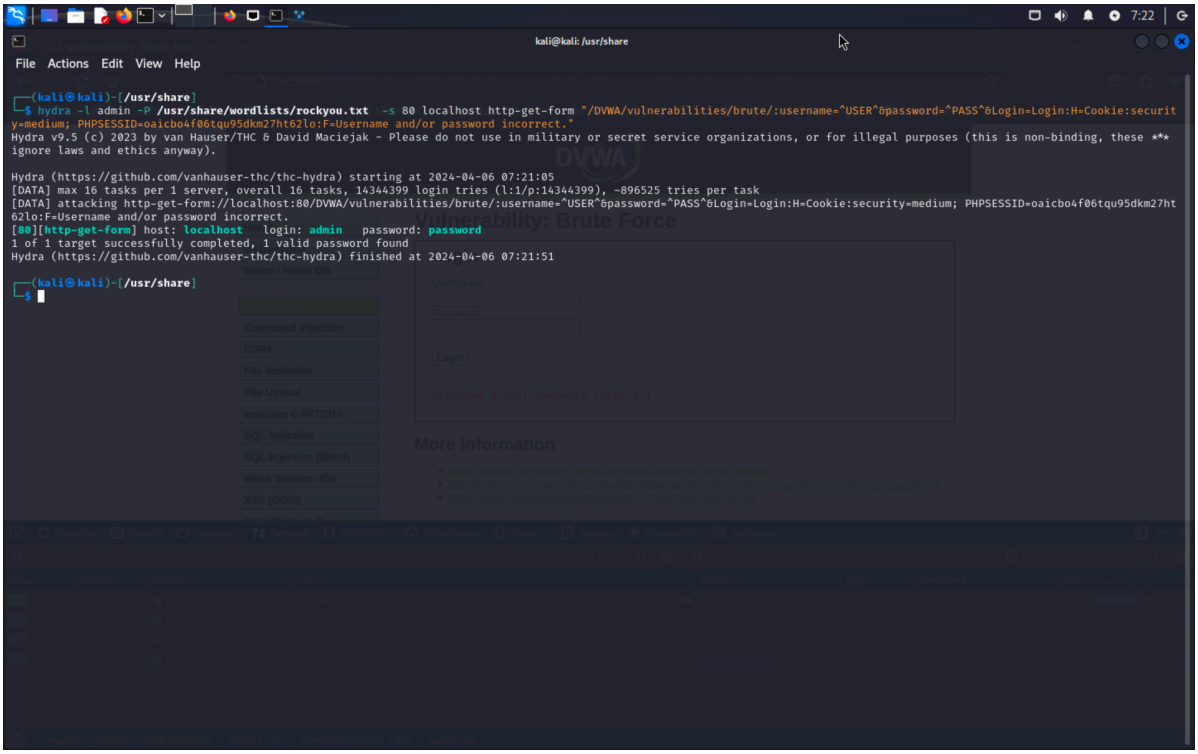

Рис. 3.3: Hydra

3.4 Проверка результатов

Проверяем, что эта пара действительно подходит (рис. 3.4).

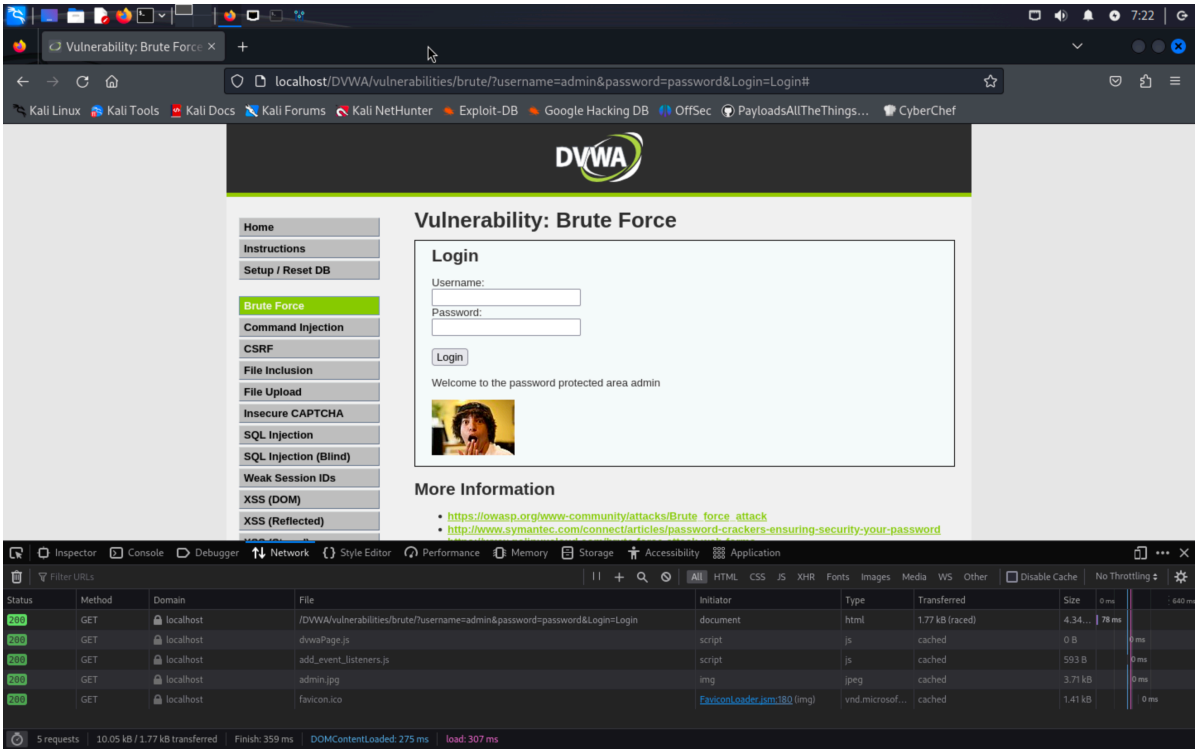

Рис. 3.4: Проверка

4 Выводы

В ходе лабораторной работы была изучена программа Hydra.