Отчёт по этапу №3

Дисциплина: Основы информационной безопасности

Мишина Анастасия Алексеевна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Научиться использовать Hydra для подбора имени пользователя и пароля.

2 Выполнение лабораторной работы

Hydra используется для подбора или взлома имени пользователя и пароля. Поддерживает подбор для большого набора приложений. Инструмент поддерживает многочисленные сетевые протоколы, такие как HTTP, FTP, POP3 и SMB. Для работы ему нужны имя пользователя и пароль. Hydra пытается параллельно войти в сетевую службу и по умолчанию для входа использует 16 подключений к целевой машине [1].

Запсукаем mysql и DVWA (рис. 2.1).

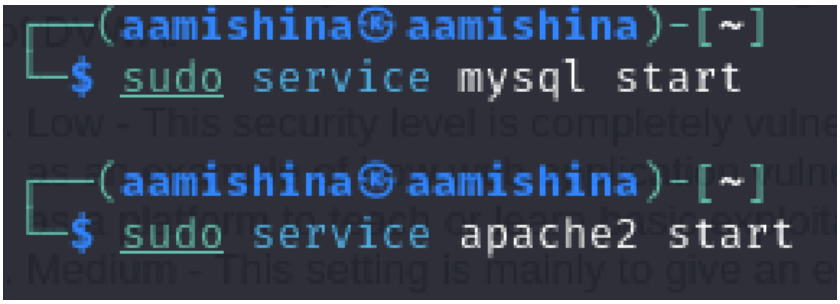

Рис. 2.1: Запуск DVWA и базы данных

Переходим в раздел DVWA Security и ставим уровень безопасности на low - низкий (рис. 2.2).

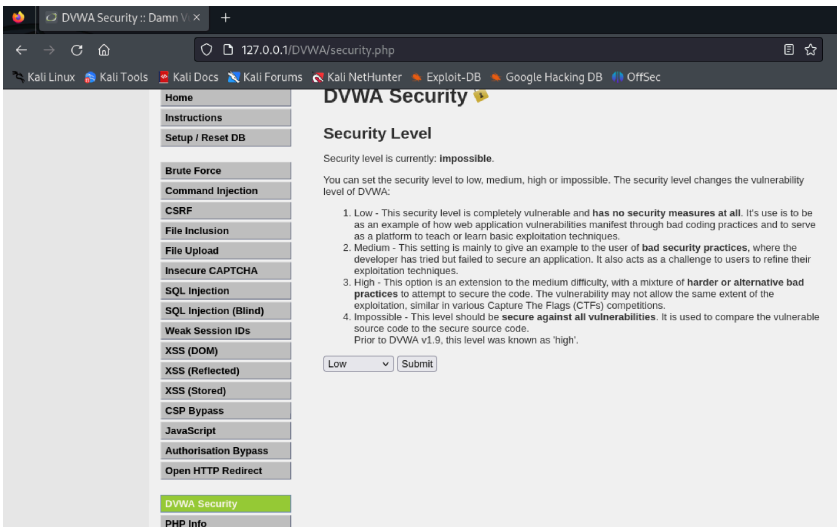

Рис. 2.2: Уровень безопасности

Создаем файл passwords.txt, где буду содержаться простые и частые пароли (рис. 2.3). Открываем его и заполняем, обязательно указываем пароль от пользователя, которого будем “взламывать” (рис. 2.4).

Рис. 2.3: Создание файла passwords.txt

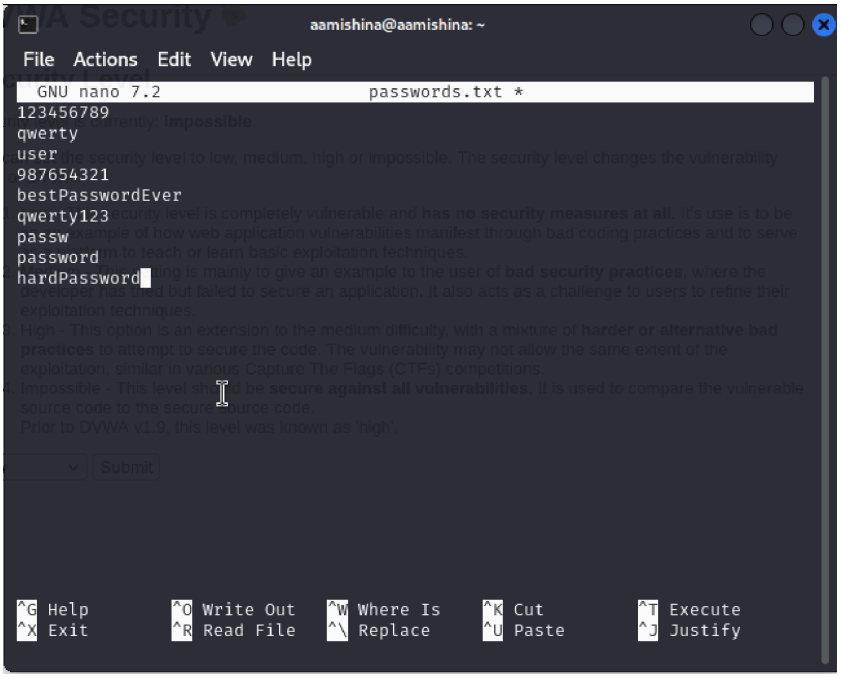

Рис. 2.4: Наполнение файла passwords.txt

Открываем на сайте раздел Brute Force, где можно пытаться подбирать пароль для формы входа. Открываем код страницы сочетанием ctrl + u, видим, что используется get метод для отправки данных, также находим названия полей ввода - username и password, кнопка для отправки имеет название Login (рис. 2.5).

Рис. 2.5: Форма входа

Для формирования запроса к Hydra нам необходимо узнать PHPSESSID. Нажимаем правой кнопкой мыши в любом месте на странице, выбираем режим Inspect, далее во вкладках Storage, Cookies находим нужный PHPSESSID [2] (рис. 2.6).

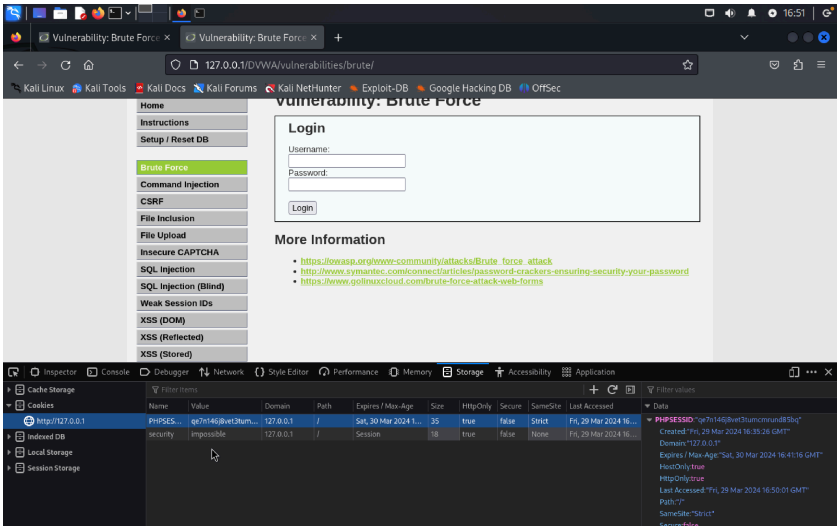

Рис. 2.6: Просмотр кода страницы, PHPSESSID

Тепер у нас есть все необходимые данные для запроса к Hydra. Создаем запрос из имеющихся данных (рис. 2.7).

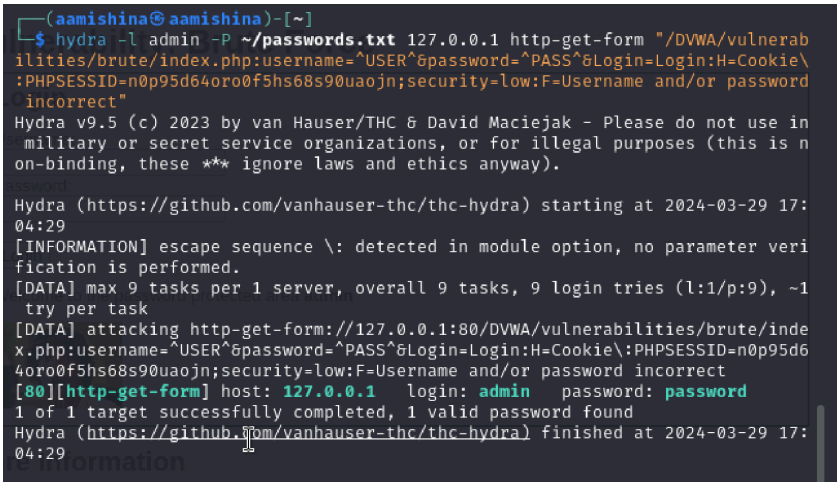

Рис. 2.7: Запрос к Hydra, подбор пароля

В результате подбирается пароль password, вводим его в форму и убеждаемся, что он подходит (рис. 2.8).

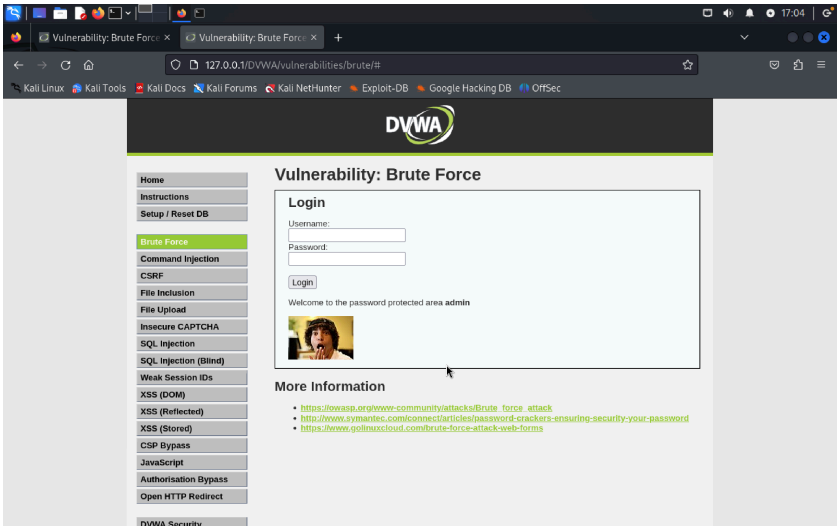

Рис. 2.8: Проверка пароля

Затем создаем файл users.txt, где буду содержаться простые и частые логины (рис. 2.9). Заполняем его, обязательно указываем наш логин - admin (рис. 2.10).

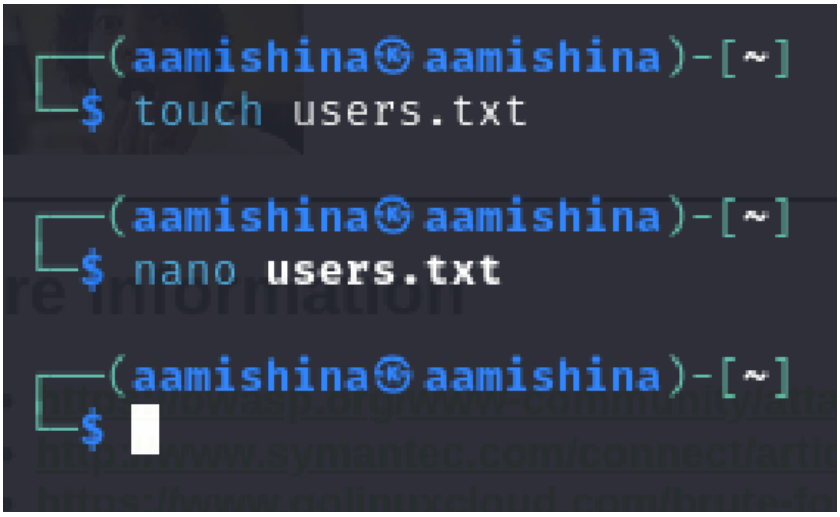

Рис. 2.9: Создание файла users.txt

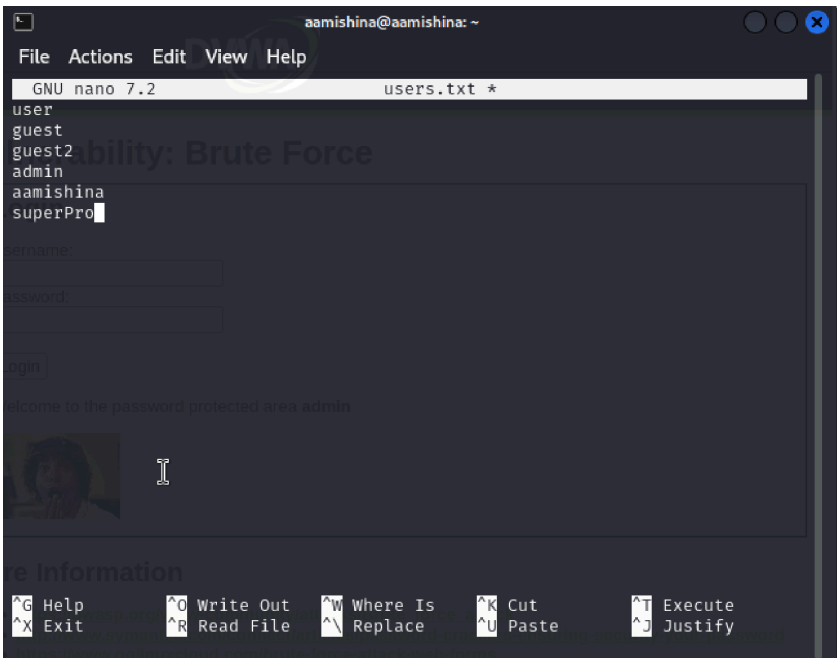

Рис. 2.10: Наполнение файла users.txt

Заново выполняем команду для Hydra. Видим, что подобралась необходимая пара: логин - пароль, а именно admin - password [3] (рис. 2.11).

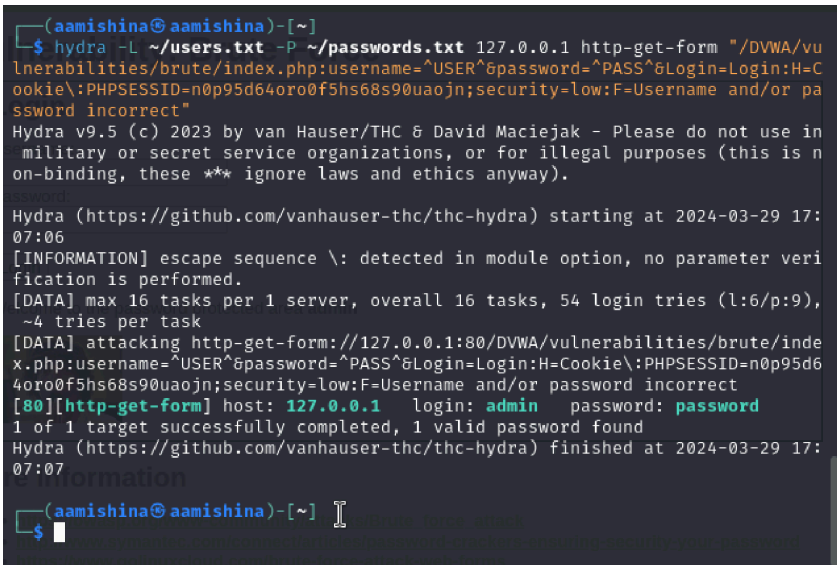

Рис. 2.11: Подбор логина и пароля

3 Выводы

В ходе выполнения данной лабораторной работы, я научилас использовать Hydra для подбора имени пользователя и пароля.

Список литературы

1. Парасрам Ш. и др. Kali Linux: Тестирование на проникновение и безопасность. 4-е изд. Санкт-Петербург: Питер, 2022. 448 с.
2. 1 - Brute Force (low/med/high) - Damn Vulnerable Web Application (DVWA). [Электронный ресурс].
3. Уязвимость DVWA. Brute Force (Уровень Low). [Электронный ресурс].