Основы информационной безопасности

Индивидуальный проект. Этап № 3. Использование Hydra

Подлесный Иван Сергеевич

Содержание

# Цель работы

Целью данной работы является установка DVWA на Kali Linux.

# Теоретические сведения

Damn Vulnerable Web Application (DVWA) — это намеренно уязвимое веб-приложение на PHP/MySQL. Цель проекта — помочь этичным хакерам и специалистам ИБ отточить свои навыки и протестировать инструменты.

DVWA также может помочь веб-разработчикам и изучающим ИБ, лучше понять процесс безопасности веб-приложений.

# Ход работы

Установим низкий уровень защиты DVWA(рис. fig. 1)



Рис. 1: Уровень защиты DVWA

Откроем страницу для проведения атаки brute force(рис. fig. 2).

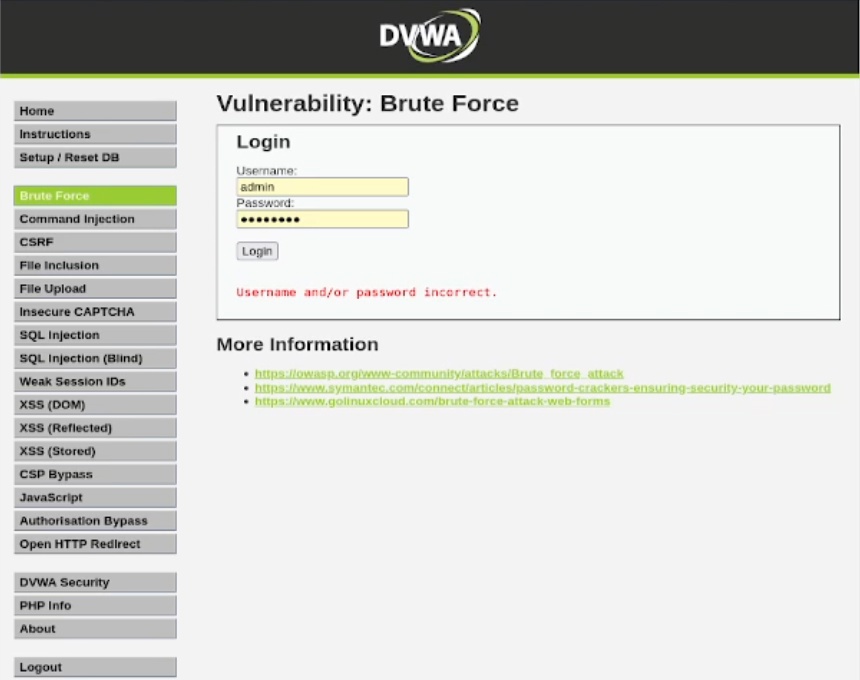


Рис. 2: Форма для ввода пароля

В Kali лежит файл с наиболее популярными паролями, распакуем его и увидим, что уже в начале есть пароль, который установлен по умолчанию для нашего аккаунта(рис. fig. 3, fig. 4).

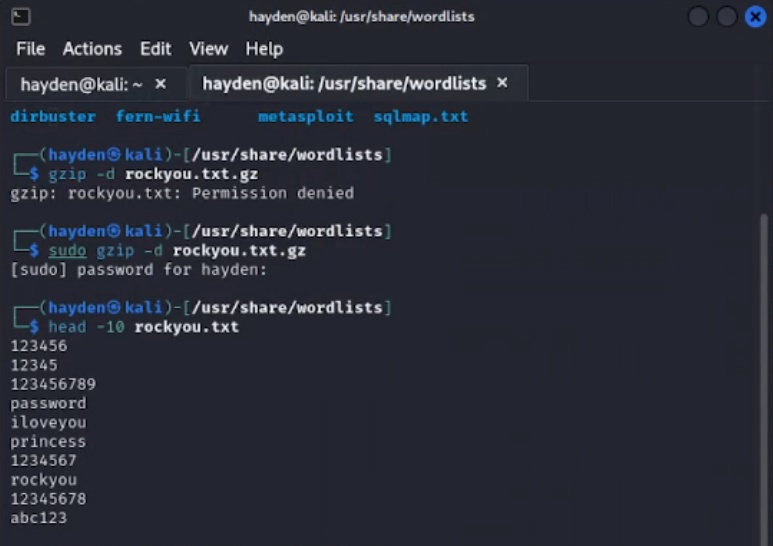


Рис. 3: Вывод из файла rockyou.txt 10 наиболее популярных паролей

Рассмотрим данные о запросе на вход(рис. fig. 4).

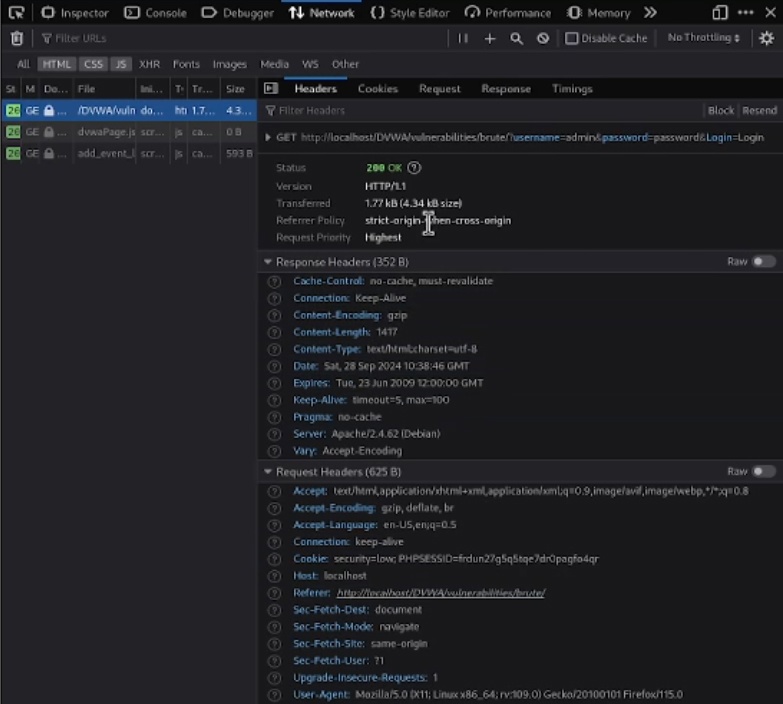


Рис. 4: Данные о запросе на вход

Исходные данные:

* IP сервера 127.0.0.1(localhost);
* Для авторизации используется html форма, которая отправляет по адресу http://localhost/DVWA/vulnerabilities/brute методом GET запрос вида username=admin&password=test\_password;
* В случае неудачной аутентификации пользователь наблюдает сообщение Username and/or password incorrect.

Запрос к Hydra будет следующим образом(рис. fig. 5):

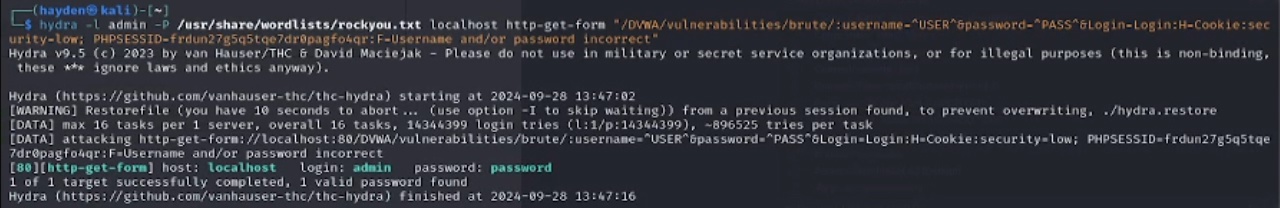


Рис. 5: Запрос к Hydra

В результате получим нужный пароль(рис. fig. 6):



Рис. 6: Проверка полученного пароля

# Выводы

В результате выполнения была успешно проведена brute-force атака на приложение DVWA.