Третий этап индивидуального проекта

Использование Hydra

Беличева Дарья Михайловна

Содержание

# 1 Цель работы

Научиться использовать Hydra для подбора пароля (брутфорсинга).

# 2 Теоретическое введение

Hydra – распараллеленный сетевой взломщик входа, встроенный в различные операционные системы, такие как Kali Linux, Parrot и другие основные среды тестирования на проникновение. Hydra работает, используя различные подходы для выполнения атак методом перебора, чтобы угадать правильную комбинацию имени пользователя и пароля. Hydra обычно используется тестировщиками на проникновение вместе с набором программ, таких как crunch, cupp и т.д., которые используются для генерации списков слов. Затем Hydra используется для тестирования атак с использованием списков слов, созданных этими программами[1].

* Hydra используется для подбора или взлома имени пользователя и пароля.
* Поддерживает подбор для большого набора приложений.

Пример работы:

* Исходные данные:
* IP сервера 178.72.90.181;
* Сервис http на стандартном 80 порту;
* Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test\_password;
* В случае не удачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.

Запрос к Hydra будет выглядеть примерно так:

hydra -l root -P ~/pass\_lists/dedik\_passes.txt -o ./hydra\_result.log -f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^PASS^:Invalid username"

# 3 Выполнение лабораторной работы

Запустим DVWA, перейдем к настройке уровня безопасности и выставим низкий уровень (рис. 1).

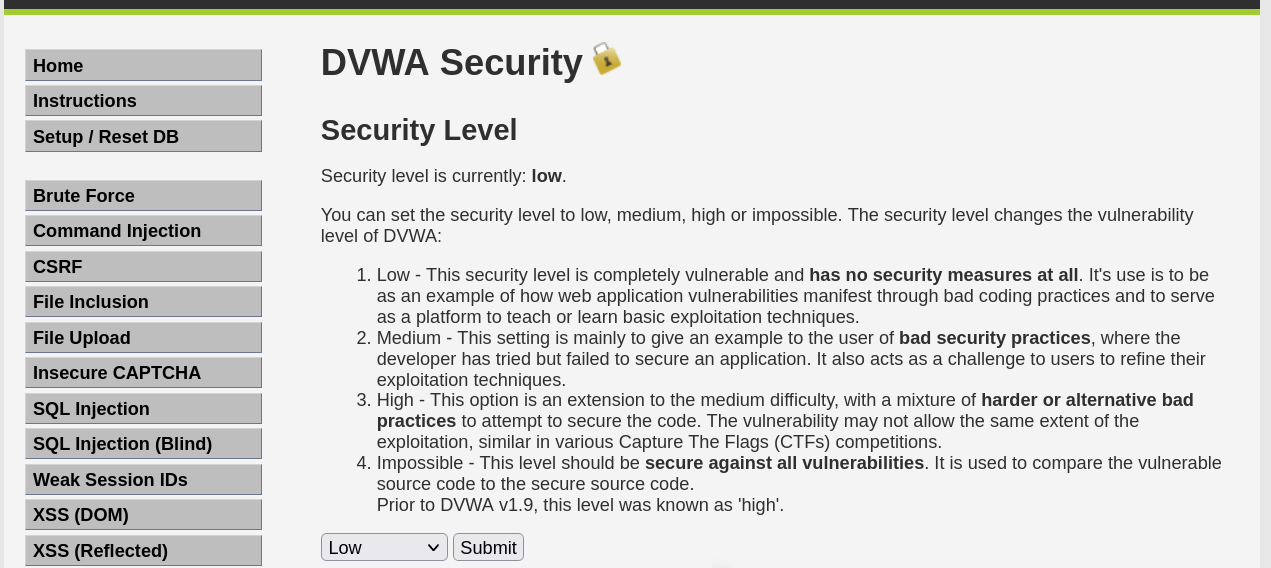


Рис. 1: Настройка уровня безопасности

Откроем страницу для проведения атаки brute force, которая представляет собой простейшую уязвимую форму с паролем (рис. 2).

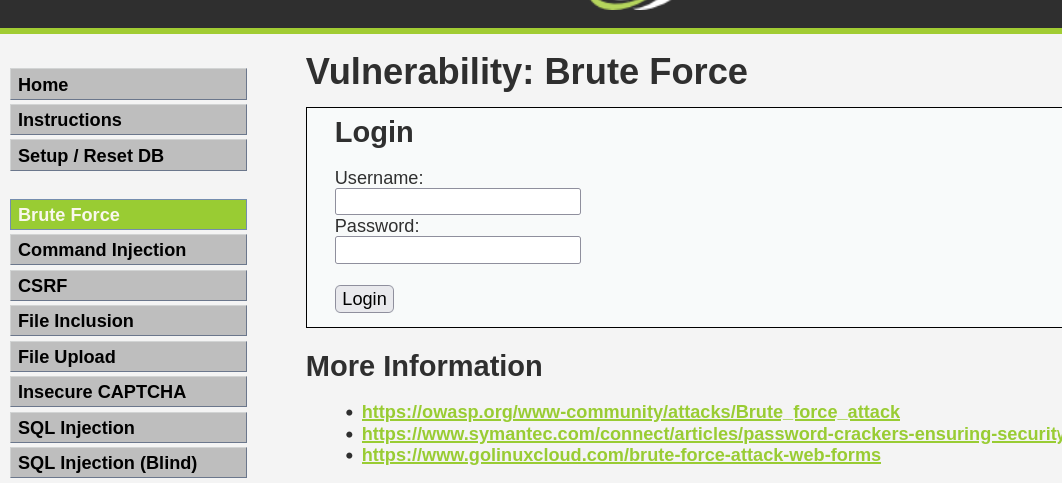


Рис. 2: Форма для ввода логина и пароля

Для работы Hydra нам нужен список паролей. В Kali есть файл со списком популярных паролей, найдем его и распакуем (рис. 3).



Рис. 3: Распаковка rockyou.txt.gz

Посмотрим содержимое первых строк этого файла (рис. 4).

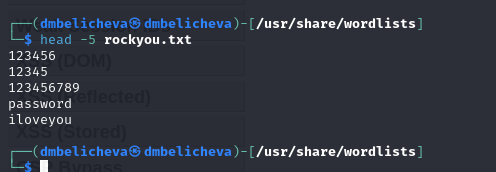


Рис. 4: Содержимое rockyou.txt.gz

С помощью горячей клавиши f12 на сайте DVWA откроем инструмент разработчика и посмотрим HTTP запросы, чтобы узнать необходимую нам информацию для атаки.

Исходные данные:

* IP сервера 127.0.0.1(localhost);
* Сервис http на стандартном 80 порту;
* 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 выглядеть так (рис. 5):

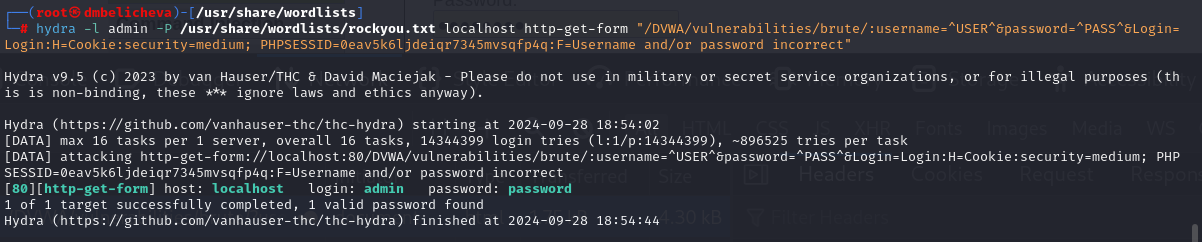


Рис. 5: Запрос к Hydra

Мы получили нужный нам пароль. Попробуем его ввести и получим успешный вход в систему (рис. 6).

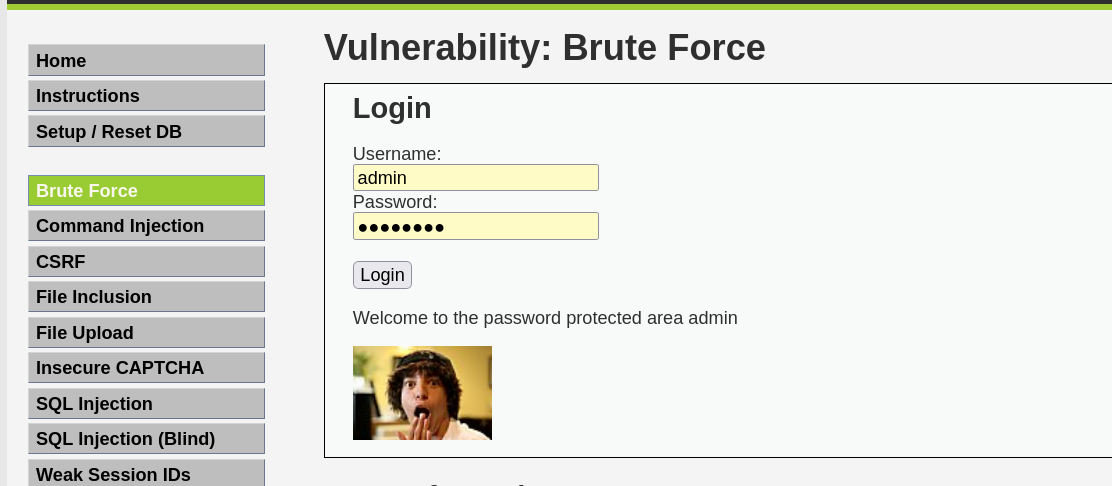


Рис. 6: Проверка полученного пароля

# 4 Выводы

В процессе выполнения данной лабораторной работы я освоила навыки использования Hydra для подбора пароля (брутфорсинга).

# Список литературы

1. Hydra (software) [Электронный ресурс]. 2024. URL: <https://en.wikipedia.org/wiki/Hydra_(software)>.