# Основы информационной безопасности

**Индивидуальный проект. Этап № 3. Использование Hydra**

Подлесный Иван Сергеевич

# Содержание

# Список иллюстраций

# 1 Цель работы

Целью данной работы является установка DVWA на Kali Linux.

# 2 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.

# 3 Ход работы

Установим низкий уровень защиты DVWA(рис. fig. 3.1)

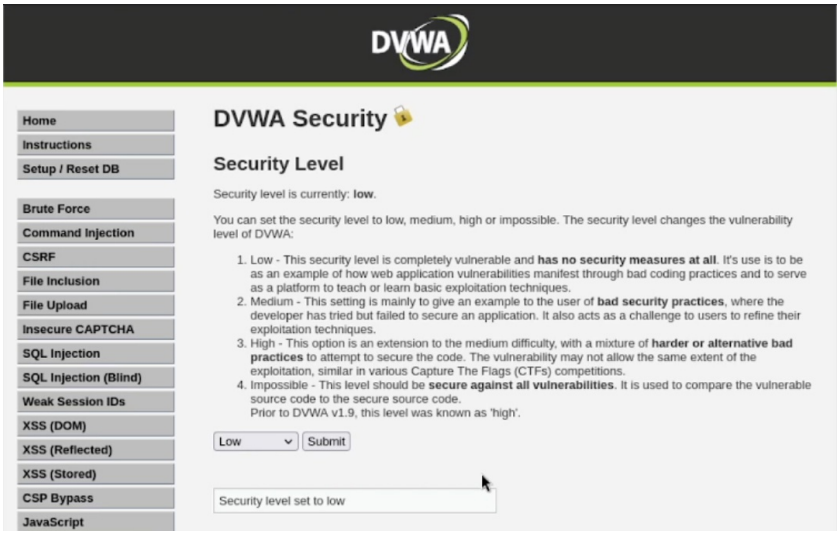


Рис. 3.1: Уровень защиты DVWA

Откроем страницу для проведения атаки brute force(рис. fig. 3.2).

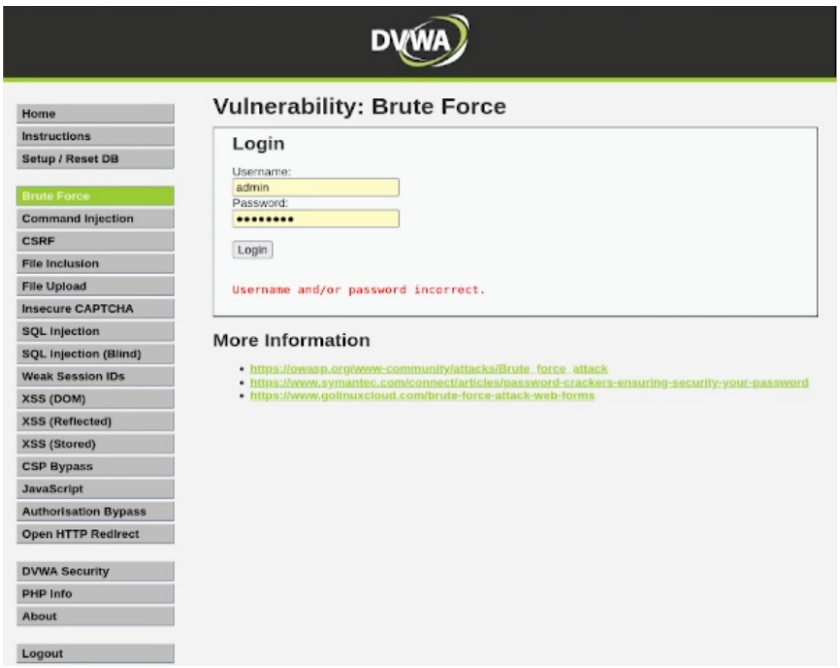


Рис. 3.2: Форма для ввода пароля

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. 3.3, fig. 3.4).

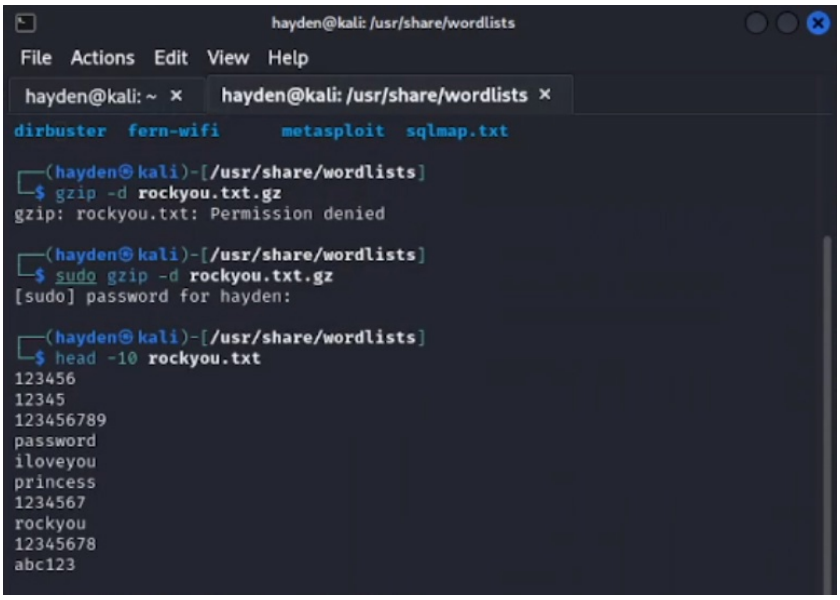


Рис. 3.3: Вывод из файла rockyou.txt 10 наиболее популярных паролей

Рассмотрим данные о запросе на вход(рис. fig. 3.4).

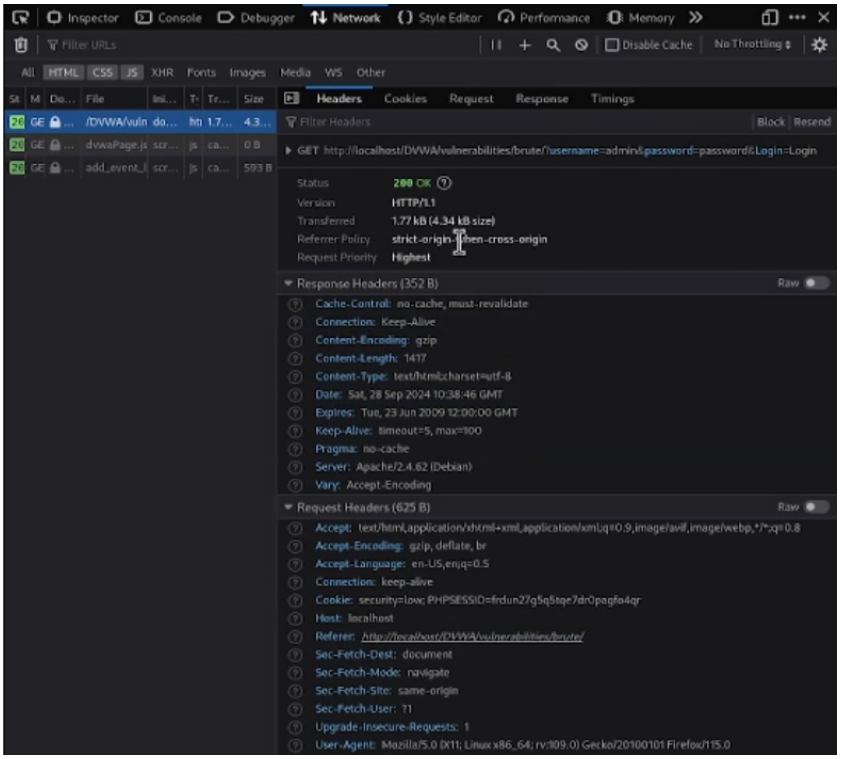


Рис. 3.4: Данные о запросе на вход

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. 3.5):

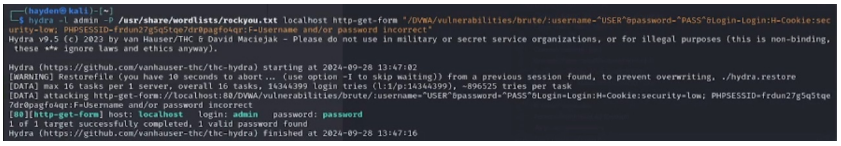


Рис. 3.5: Запрос к Hydra

В результате получим нужный пароль(рис. fig. 3.6):


Рис. 3.6: Проверка полученного пароля

# 4 Выводы

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