Основы информационной безопасности

Индивидуальный проект. Этап № 3. Использование Hydra

Демидова Екатерина Алексеевна

Содержание

Список иллюстраций

1 Постановка задачи

Целью данной работы является использование Hydra для подбора пароля.

2 Теоретические сведения

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо[~ 1]. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

Цель DVWA – отработать некоторые из наиболее распространенных веб-уязвимостей различного уровня сложности с помощью простого и понятного интерфейса. В этом программном обеспечении существуют как задокументированные, так и недокументированные уязвимости.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
- Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел

неудачу.

- Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

В этом этапе будет рассмотрена атака типа брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.

Hydra – это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов[~ 2]. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак. Пользователь быстро и с легкостью может добавить новые модули. Hydra предоставляет специалистам в сфере ИБ возможность узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства.

3 Выполнение лабораторной работы

Установим самый низкий уровень защиты DVWA(рис. 3.1)

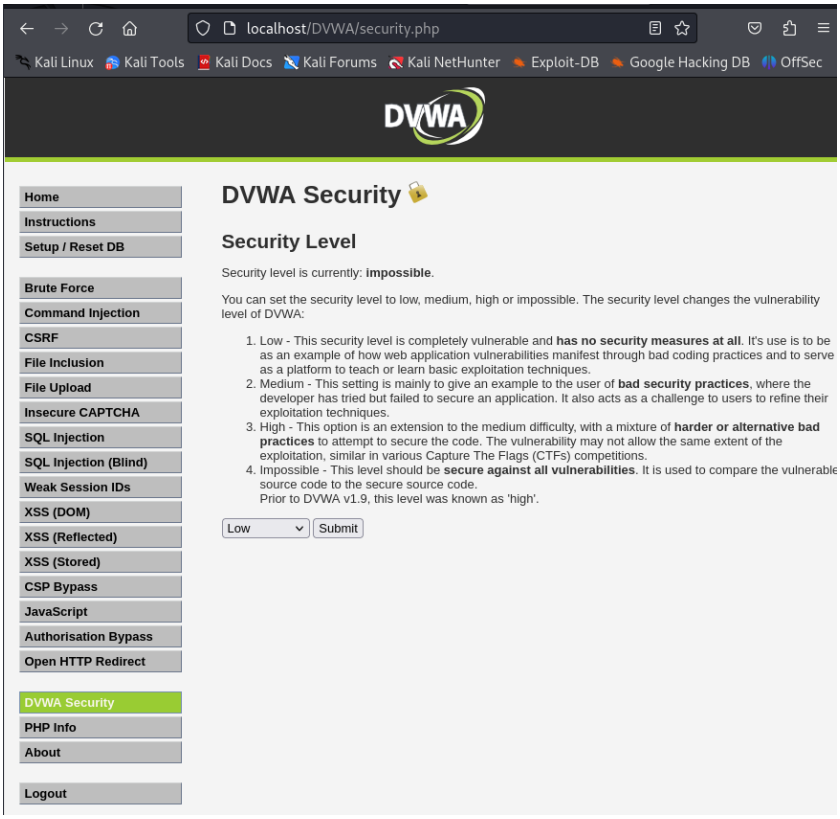

Рис. 3.1: Уровень защиты DVWA

Откроем страницу для проведения атаки brute force, которая представляет собой простейшую уязвимую форму с паролем(рис. 3.2).

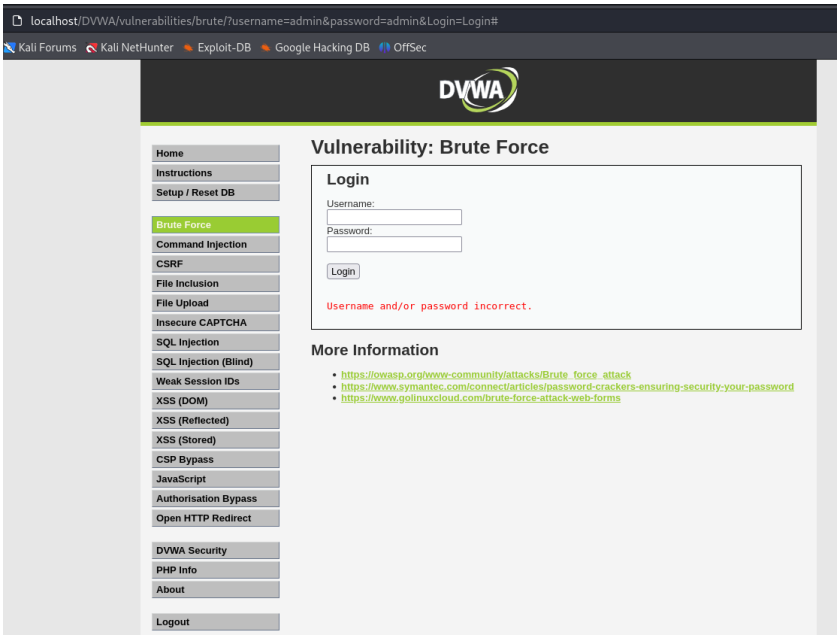

Рис. 3.2: Уязвимая форма для ввода пароля

В Kali лежит файл с наиболее популярными паролями, который мы распакуем(рис. 3.3).

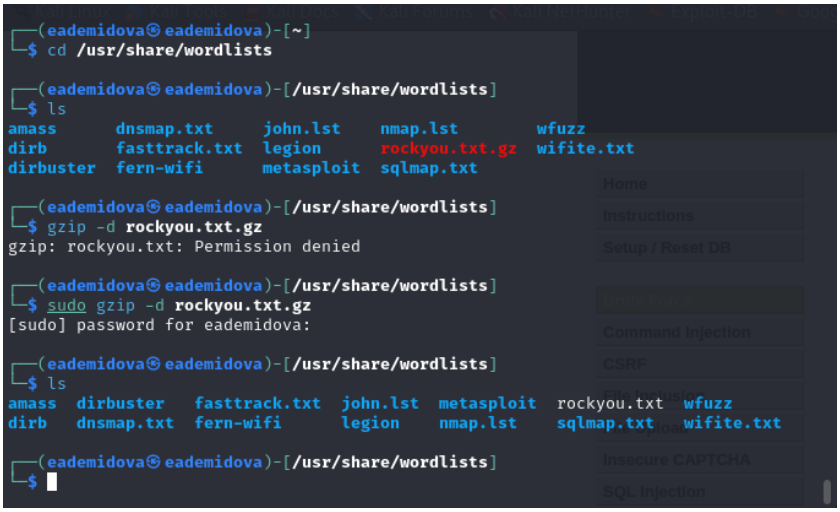

Рис. 3.3: Распаковка rockyou.txt.gz

Можно увидеть, что уже в начале есть пароль, который установлен по умолчанию для нашего аккаунта(рис. 3.4, 3.5).

Рис. 3.4: Файл rockyou.txt с наиболее популярными паролями

Рассмотрим данные о запросе на вход(рис. 3.5).

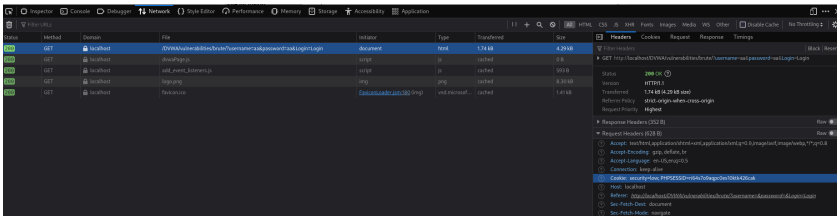

Рис. 3.5: Данные о запросе на вход

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. 3.6):

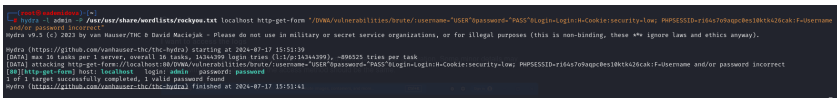

Рис. 3.6: Запрос к Hydra

В результате получим нужный пароль(рис. 3.7):

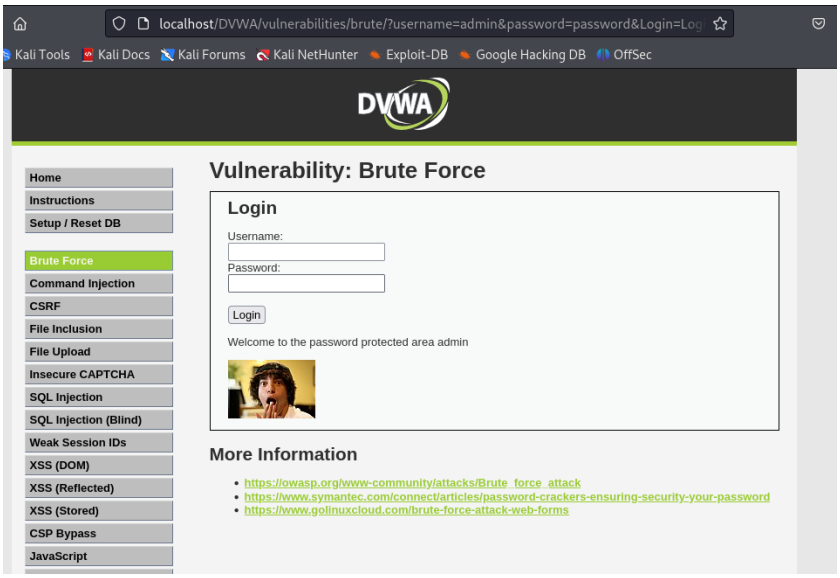

Рис. 3.7: Проверка полученного пароля

4 Выводы

В результате выполнения работы была использована Hydra для атаки типа brute force.

Список литературы

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: https://github.com/digininja/DVWA.
2. Подробное руководство по Hydra [Электронный ресурс]. CISOCLUB, 2024. URL: https://cisoclub.ru/podrobnoe-rukovodstvo-po-hydra/.