Отчет по 3 этапу индивидуального проекта

Использование Hydra

Неустроева Ирина Николаевна

Содержание

# 1 Теоретическое введение

-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"

Используется http-post-form потому, что авторизация происходит по http методом post.

После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:Invalid username, у которой через двоеточие (:) указывается:

-путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);  
   
 -строка, которая передаётся методом POST, в которой логин и пароль заменены на ^USER^ и ^PASS^ соответственно (username=^USER^&password=^PASS^);  
   
 -строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

# 2 Цель работы

Приобретение практических навыков по использованию инструмаента Hydra взлома и подбора пороля

# 3 Выполнение

Чтобы взломать пароль, нужно сначала скачать большой список часто используемых паролей, его нужно найти в открытых источниках, установила стандартный список паролей “rockyou.txt” для Kali linux и распокавала скаченный файл

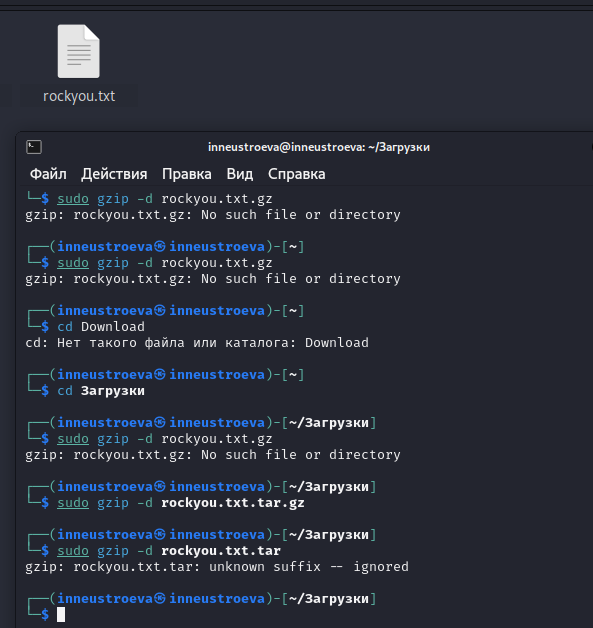


Рис. 1: Распаковка архива со списком паролей

Захажу на сайт DVWA, полученный в ходе 2 этапа индивидуального проекта. Для запроса hydra, мне понадобяться параметры Cookie c сайта

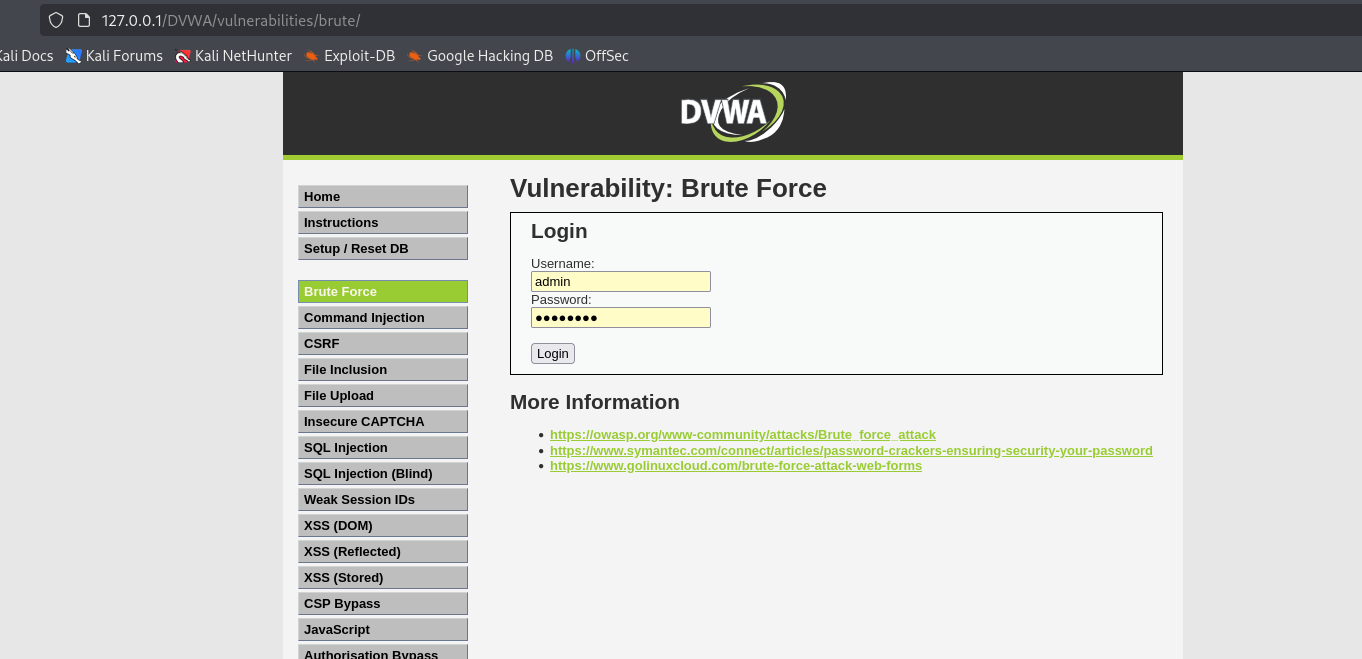


Рис. 2: Сайта DVWA для Cookie

Чтобы получить информацию о о параметрах Cookies я установила расширение для браузера, теперь мы можем увидеть и скопировать параметры Cookie

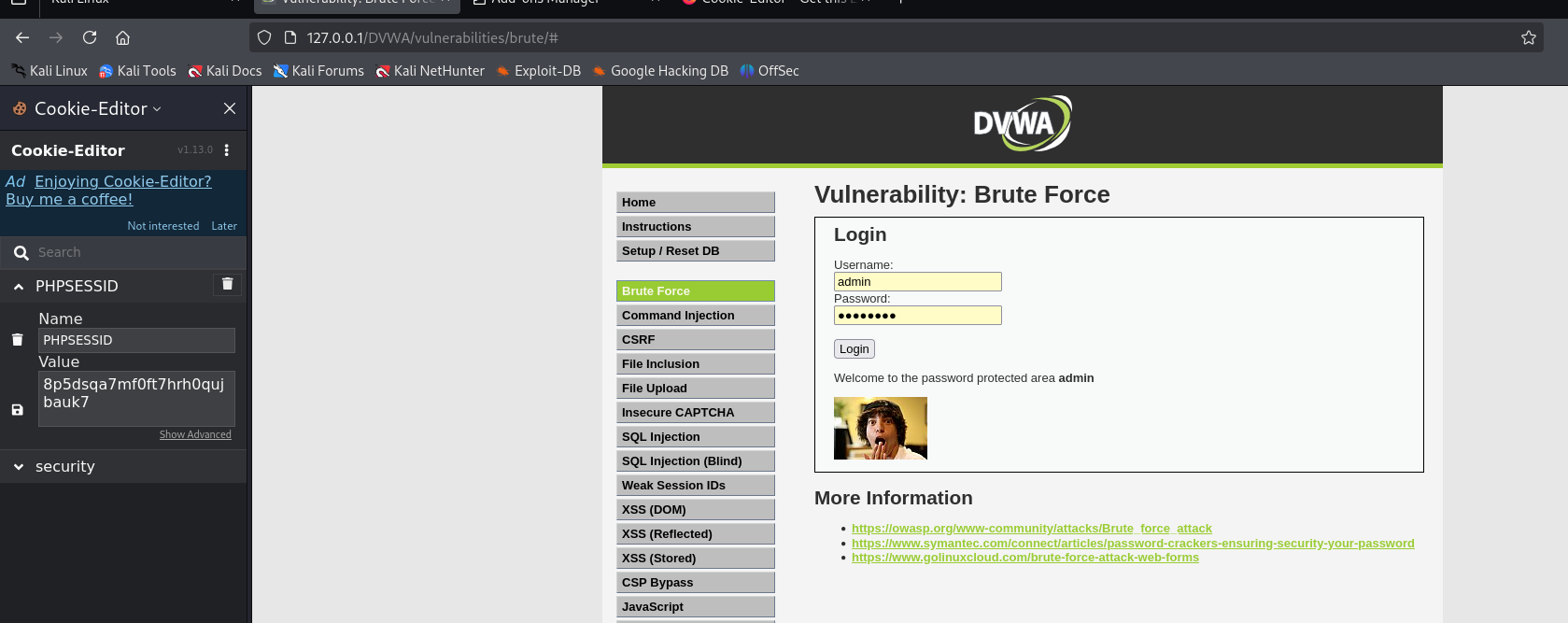


Рис. 3: Информация о параметрах Cookie

Ввожу в Hydra запрос с нужной нам информацией. Пароль подбираем для пользователя admin, используя GET-запрос с двумя параметрами Cookie: безопасность и PHPSESSID, найденными в прошлом пункте. Спустя некоторое время, появиться результат с подхлдящим паролем.

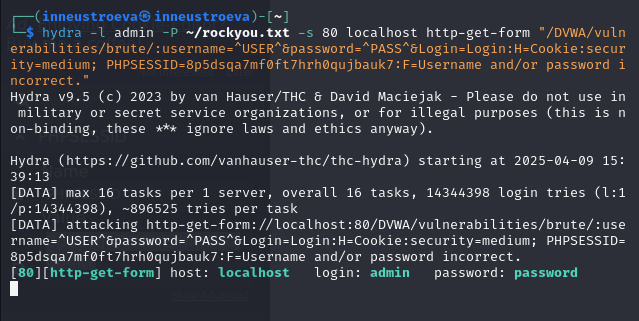


Рис. 4: Результат на запрос в Hydra

Вводим полученные данные на сайт для проверки пароля и получаем положительный результат. Все сделано верно

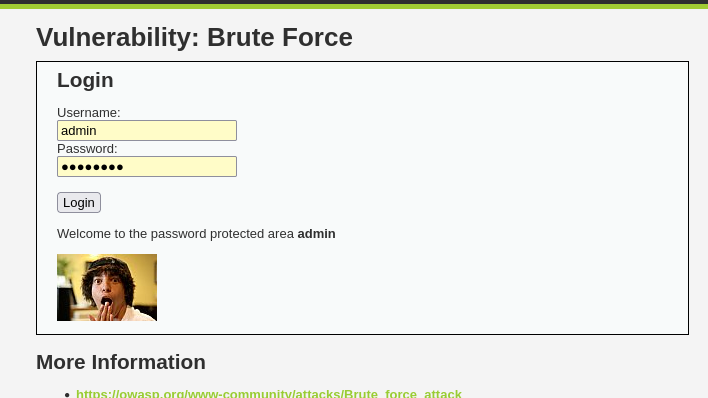


Рис. 5: проверка пароля

# 4 Выводы

В ходе нашей работы, приобрела практические навыки по использованию инструманта Hydra для подбора паролей.