Отчет по третьему этапу индивидуального проекта

Информационная безопасность

Кармацкий Никита Сергеевич

Содержание

# 1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

# 2 Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

# 3 Теоретическое введение

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

**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 неудачной 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).

# 4 Выполнение лабораторной работы

Для того, чтоб пробрутфорсит пароль, нужно сначала найти список частоиспользуемых паролей. Он есть уже в Kali Linux, поэтому нам нужно только его найти и разархивировать каталога с ним (рис. 1).

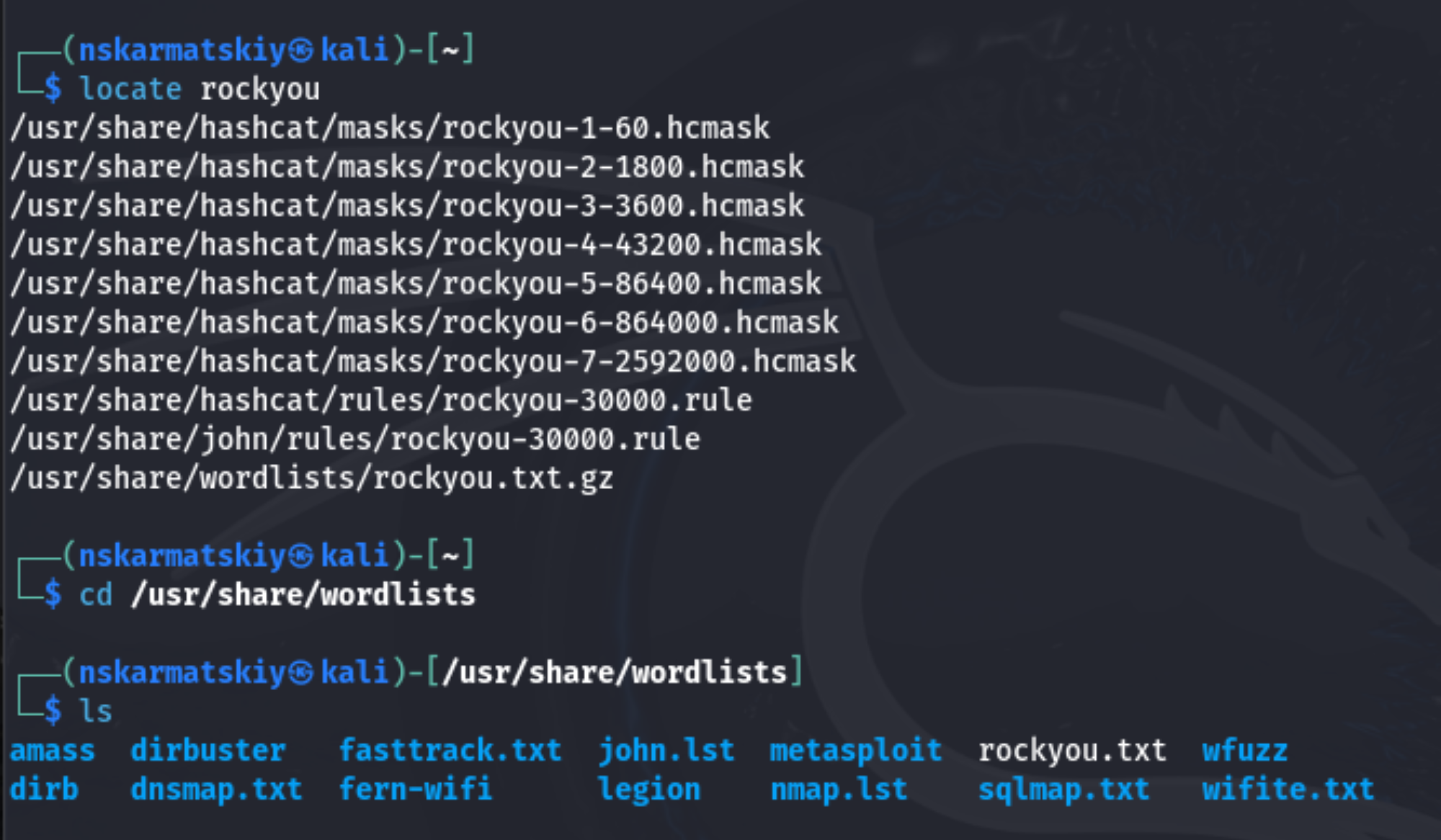


Рис. 1: Список пароле(в архиве и без)

Прочитаем файл, чтоб удостовериться что это он (рис. 2).

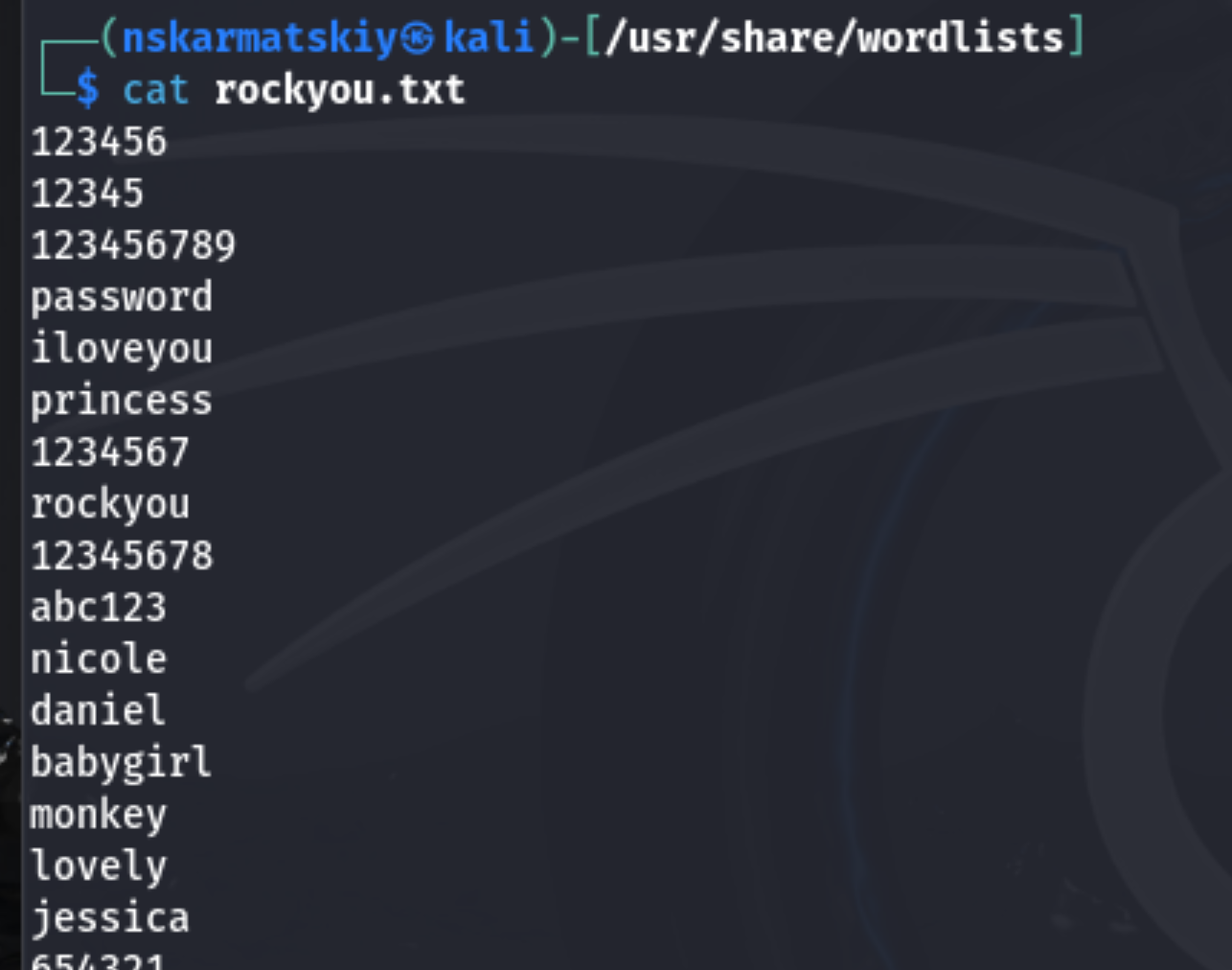


Рис. 2: Чтение файла

Заходим на сайт DVWA, в подпункт с Brute Force. Тут мы будм проверять правильность выданных данных с помощью Hydra (рис. 3).

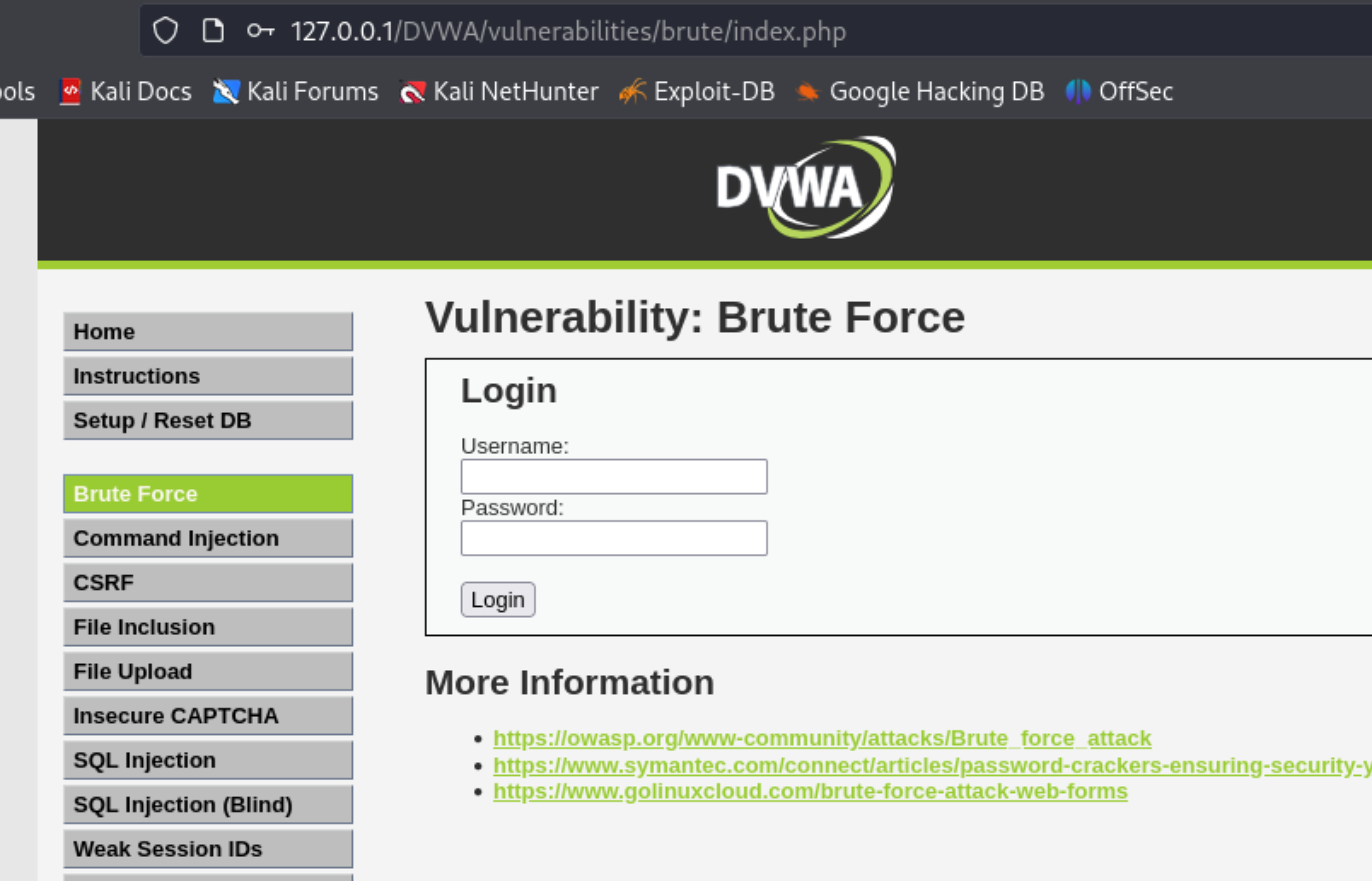


Рис. 3: Сайт DVWA

Для получения пароля и логина нам нужны файлы cookie, поэтому устанваливаем расширение, которое поможет посмотреть их параметры, а так же скопировать их (рис. 4).

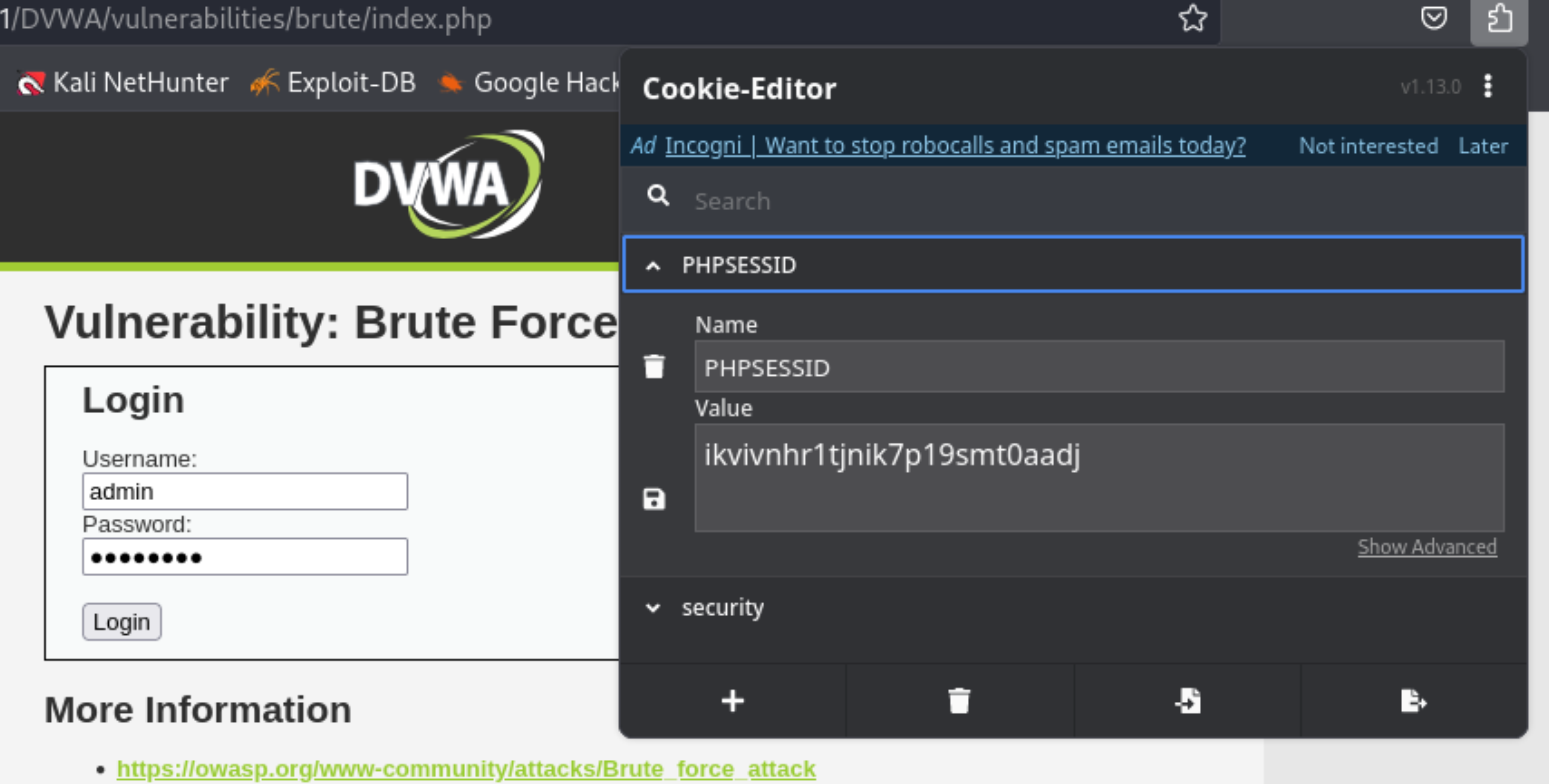


Рис. 4: Копирование параметров cookie

Вводим в Hydra нужную информацию. пароль будем подбирать для пользователя admin, используя GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID(параметры cookie) (рис. 5).

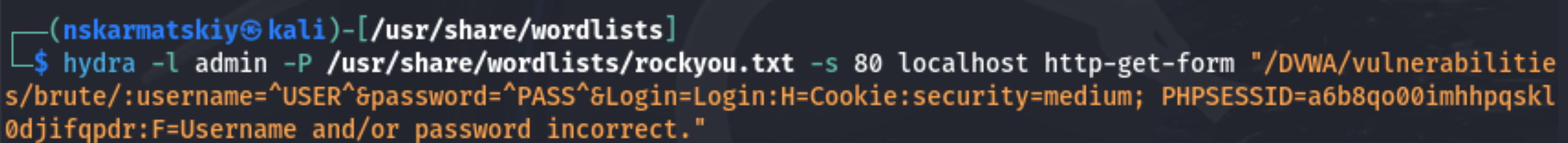


Рис. 5: Запрос Hydra

Спустя небольшое количество времени получаем результат в виде подходящий пароля и логина для конкретного юзера (рис. 6).

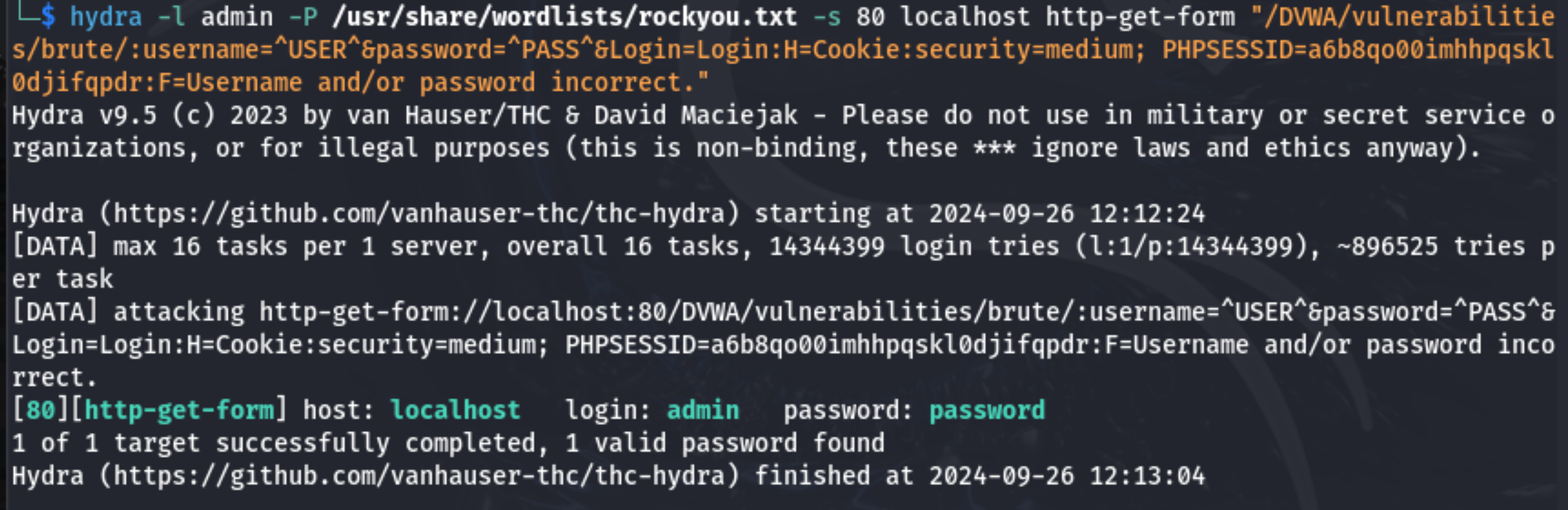


Рис. 6: Результат запроса

Вводим полученные данные на проверку (рис. 7).

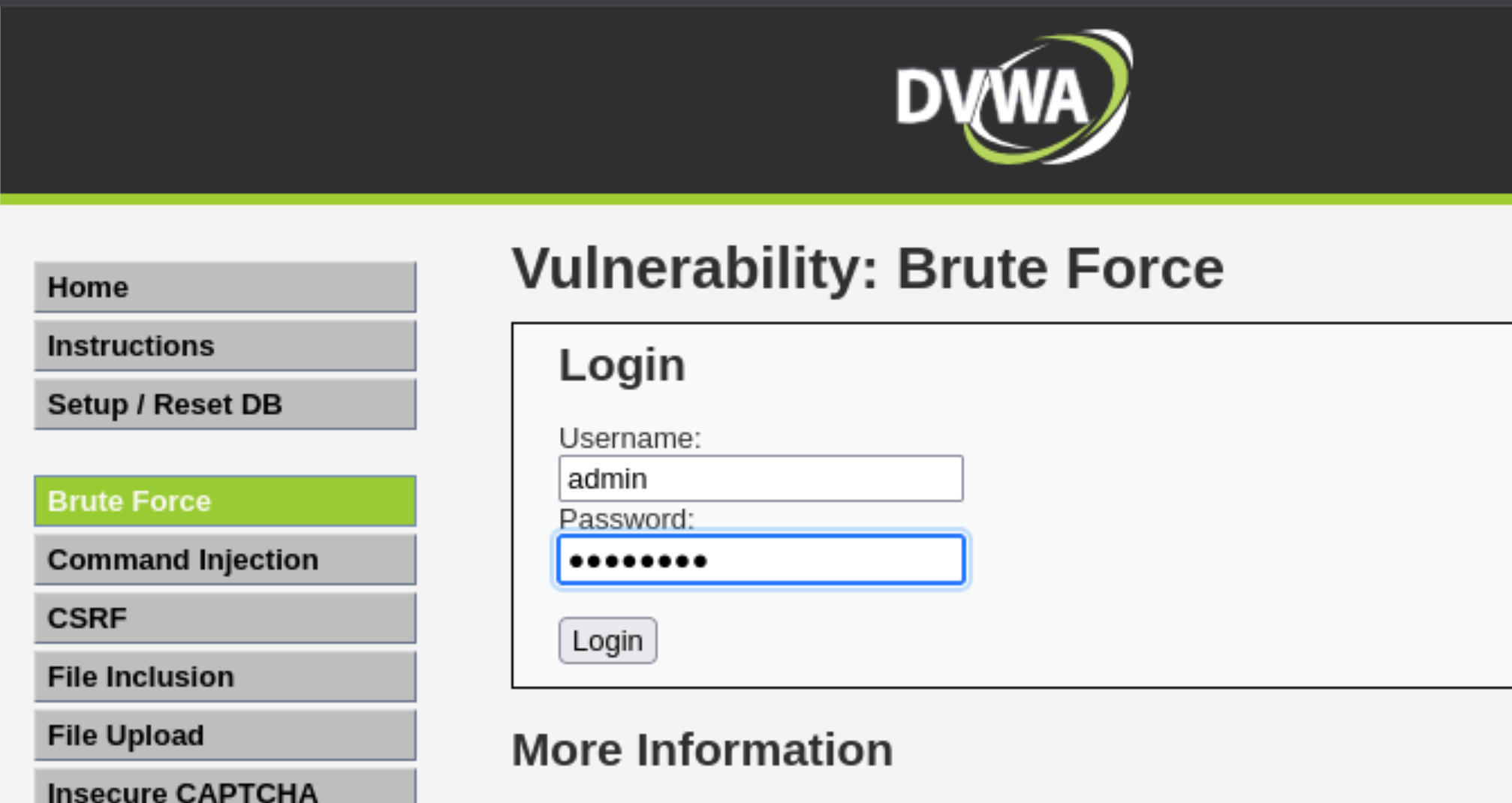


Рис. 7: Ввод данных в уязвимую форму

Получааем положительный результат проверки пароля, а это значит что все сделано верно (рис. 8)

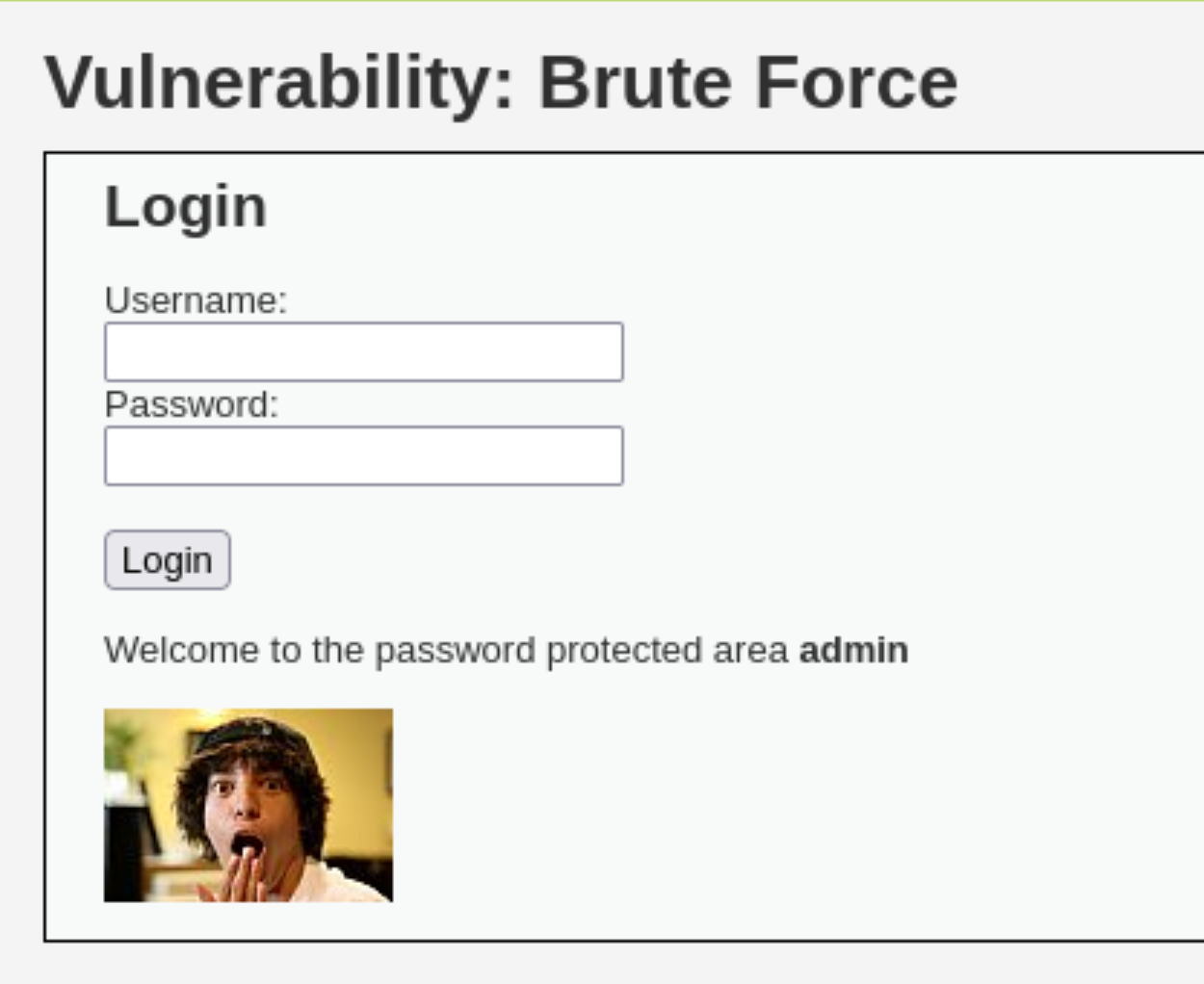


Рис. 8: Результат

# 5 Выводы

Приобрели практические навыки по использованию инструмента Hydra для брутфорса паролей.

# 6 Список литературы

[1] https://spy-soft.net/rockyou-txt/ - Словарь Rockyou.txt где находится в Kali Linux