

presentation

Презентация по 3 этапу проекта "Использование Hydra"

Подъярова Ксения Витальевна

Цель работы

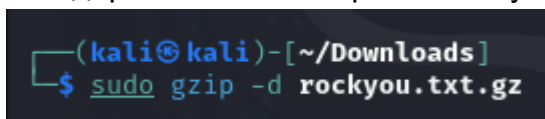
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Задание

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

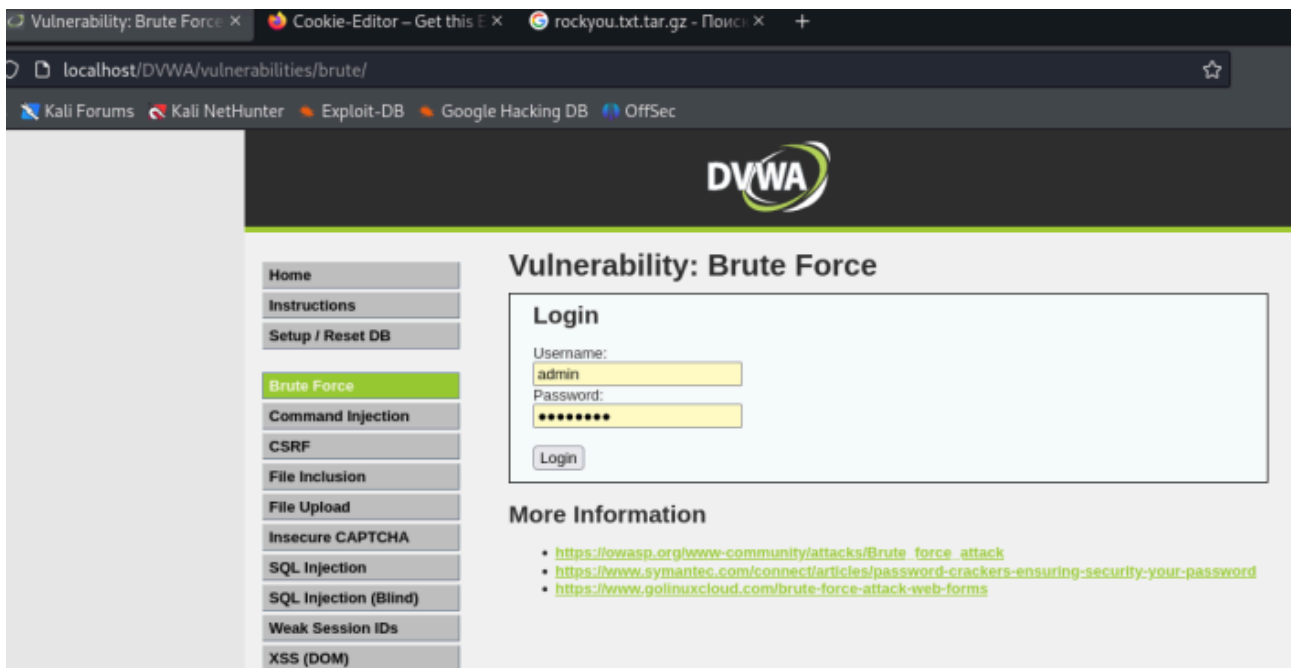
Выполнение лабораторной работы

1. Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей rockyou.txt для kali linux (рис. 1).



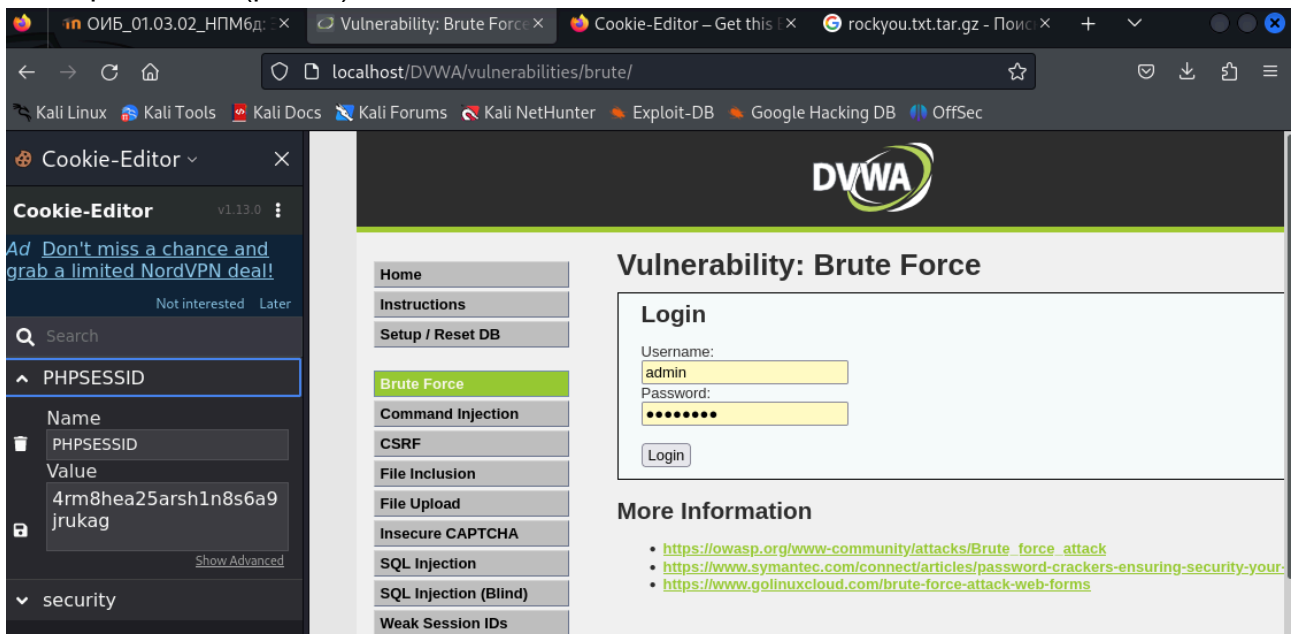
Выполнение лабораторной работы

2. Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта (рис. 2).



Выполнение лабораторной работы

- Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера, теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).



Выполнение лабораторной работы

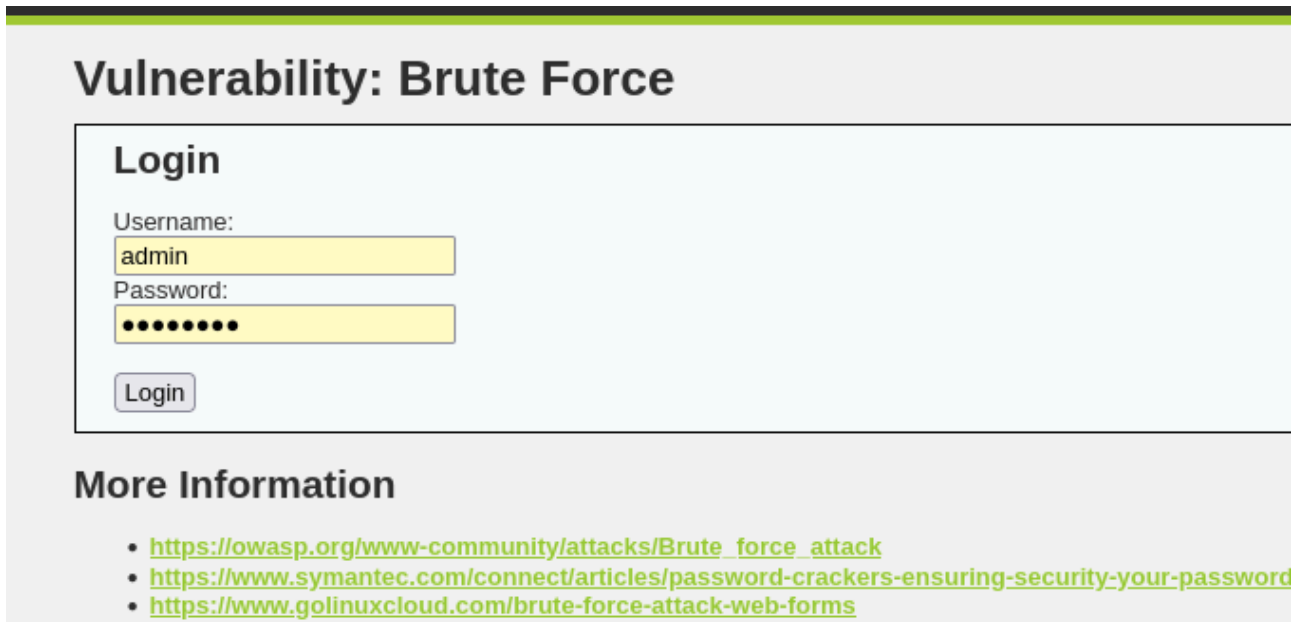
- Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie:

безопасность и PHPSESSID, найденными в прошлом пункте.

```
(kali@kali)-[~/Downloads]
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login;H=Cookie;security-impossible; PHPSESSID=4rm8hea25arsh1n8s6a9jrukag: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).
```

Выполнение лабораторной работы

5. Спустя некоторое время в результат запроса появится результат с подходящим паролем.
6. Вводим полученные данные на сайт для проверки (рис. 6).



The screenshot shows the 'Vulnerability: Brute Force' page of the DVWA. It features a 'Login' form with two input fields: 'Username' containing 'admin' and 'Password' containing a series of dots. A 'Login' button is positioned below the password field. Below the form, there is a 'More Information' section with 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>.

Выполнение лабораторной работы

7. Получаем положительный результат проверки пароля. Все сделано верно (рис. 7).

The screenshot displays the Hydra web application interface. On the left is a sidebar menu with various attack modules: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored). The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' section. In this section, the 'Username' field is filled with 'admin' and the 'Password' field is filled with ten dots. A 'Login' button is present. Below the button, a message reads 'Welcome to the password protected area admin'. Underneath the message is a small image of a person with a surprised expression. At the bottom of the main area, there is a 'More Information' section with three links: https://owasp.org/www-community/attacks/Brute_force_attack, <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your->, and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

Выводы

Приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей.