

report

Отчет по 3 этапу проекта "Использование Hydra"

Подъярова Ксения Витальевна

Цель работы

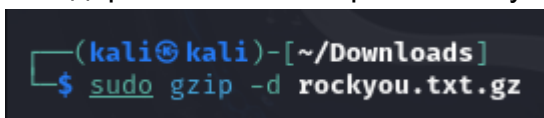
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

Задание

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

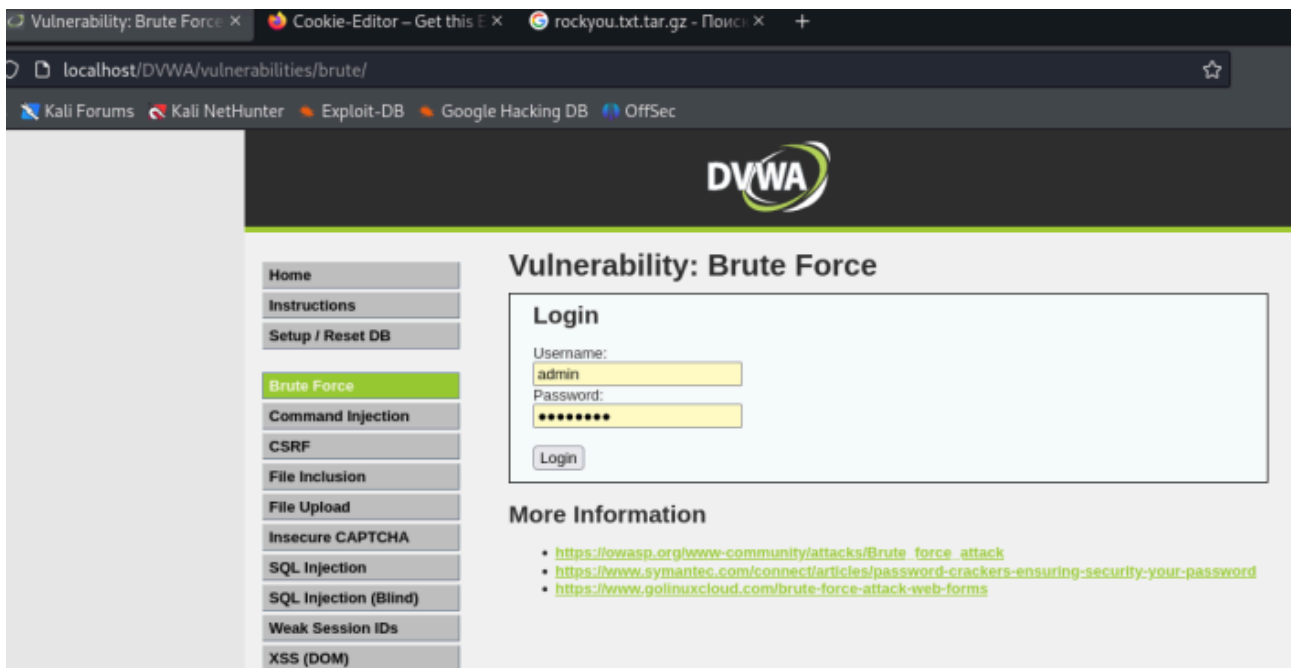
Выполнение лабораторной работы

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).

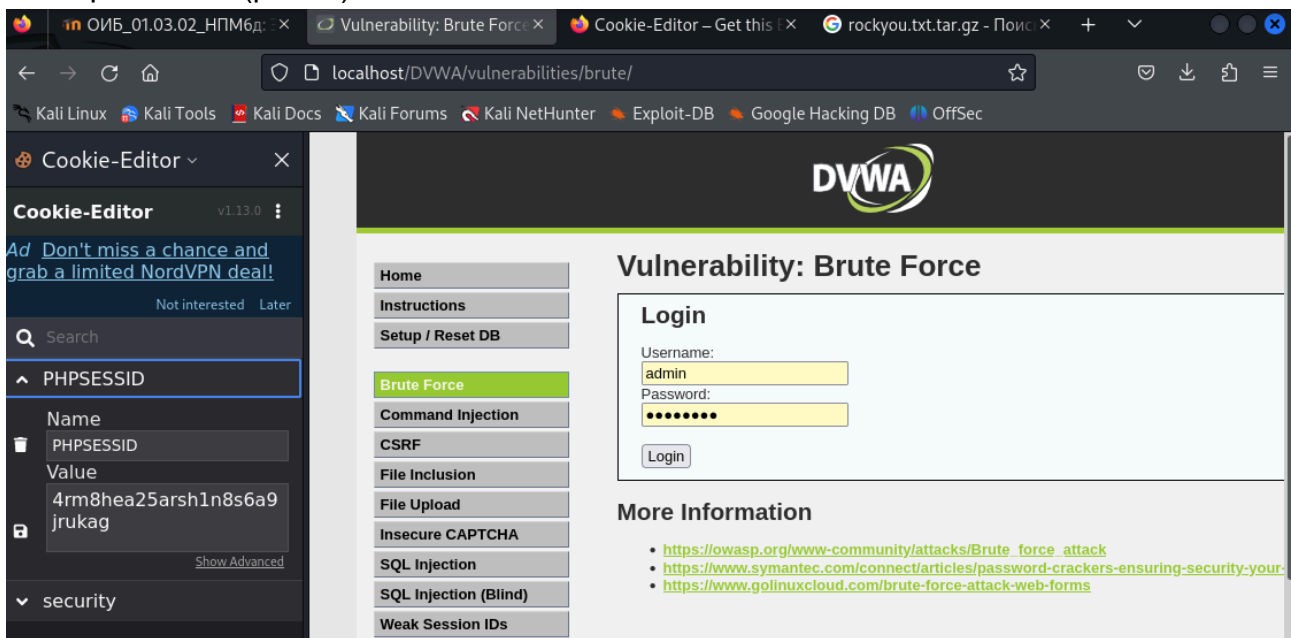


```
(kali@kali)-[~/Downloads]  
$ sudo gzip -d rockyou.txt.gz
```

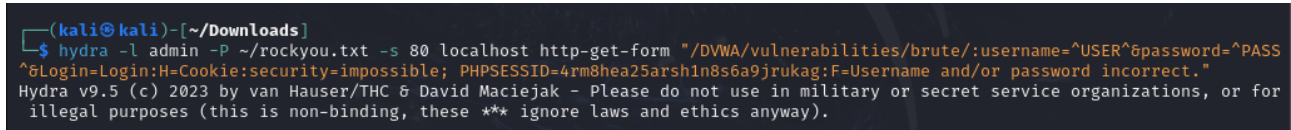
2. Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта (рис. 2).



- 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).



- 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.



- Спустя некоторое время в результат запроса появится результат с подходящим паролем.

6. Вводим полученные данные на сайт для проверки (рис. 6).

Vulnerability: Brute Force

Login

Username:

Password:

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>

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


Vulnerability: Brute Force

Login

Username:

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>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

Выводы

Приобрела практические навыки по использованию инструмента Нудра для брутфорса паролей.